HANDBOOK OF BLOCKCHAIN, DIGITAL FINANCE, AND INCLUSION VOLUME 2

ChinaTech, Mobile Security, and Distributed Ledger



Edited by **David LEE Kuo Chuen**
and **Robert H. DENG**

Материал защищенный авторским правом

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2

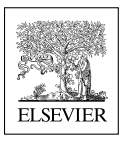
Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2

ChinaTech, Mobile Security, Distributed Ledger, and Blockchain

Edited by

David LEE Kuo Chuen
Robert Deng

Singapore University of Social Sciences, Singapore





ACADEMIC PRESS
An imprint of Elsevier

Academic Press is an imprint of Elsevier
125 London Wall, London EC2Y 5AS, United Kingdom
525 B Street, Suite 1800, San Diego, CA 92101-4495, United States
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom

Copyright © 2018 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-812282-2

For information on all Academic Press publications
visit our website at https://www.elsevier.com/books-and-journals



Publisher: Nikki Levy
Acquisition Editor: Scott Bentley
Editorial Project Manager: Susan Ikeda
Production Project Manager: Susan Li
Designer: Greg Harris

Typeset by VTeX

Dedicated To
All those who care for the needy

In Memory Of
The late Sim Kee Boon
and
The late Professor Harry Rowen

List of Contributors

Hu Anzi
CreditEase, China

Douglas W. Arner
Faculty of Law, University of Hong Kong, China

Ross P. Buckley
UNSW, Australia

Rosanna Chan
The World Bank, Washington DC, USA

Yanxiao Cheng
Xidian University, Xi'an, China

Michelle Chia
TBOP Pte. Ltd., Singapore

Liu Dawei
CreditEase, China

Robert H. Deng
Singapore Management University, Singapore

Jacob C. Donnelly
Founder, Distributed Studios, USA

Jeff Garzik
Bloq, USA

Li Gen
CreditEase, China

Cao Duy Ha
Singapore Management University, Singapore

Yuwa Hedrick-Wong
MasterCard Inc., USA

Griffin Hotchkiss
Boulder CO, USA

Alyse Killeen
StillMark Co., USA

Francis Koh
Singapore Management University, Singapore

Andras Kristof
Yojee, Singapore

Su Mon Kywe
Singapore Management University, Singapore

Holly LaCount
Polsinelli PC, USA

Roy Lai
Founder, InfoCorp Technologies, Singapore

David LEE Kuo Chuen
Left Coast, USA
Singapore University of Social Sciences, Singapore

Richard B. Levin
Polsinelli PC, USA

Yingjiu Li
Singapore Management University, Singapore

Anne-Laure Mention
RMIT University, Melbourne VIC, Australia

Abhijit Patwardhan
The 3rd Dimension Pte. Ltd., Singapore

Gareth W. Peters
University College London, London, UK
Oxford Mann Institute, Oxford University, Oxford, UK
London School of Economics, London, UK

Kok Fai Phoon
Singapore University of Social Sciences, Singapore

Dimitrios Salampasis
Swinburne University of Technology, Hawthorn VIC, Australia

Vrajlal Sapovadia
Techno Consult, Ahmedabad, India

Paul Schulte
Schulte Research, Hong Kong, China

Roland Schwinn
Eurex, Singapore

Tao Sun
Ant Financial, China

Roland Tan
TBOP Pte. Ltd., Singapore

Ernie G.S. Teo
IBM, Singapore

Guy R. Vishnia
University College London, London, UK
ITG, London, UK

Angela Walch
St. Mary's University School of Law, USA
University College London, UK

Peter Waltz
Polsinelli PC, USA

Ping Yan
Xidian University, Xi'an, China

Zheng Yan
Xidian University, Xi'an, China
Aalto University, Espoo, Finland

Adrian Yeow
Singapore University of Social Sciences, Singapore

Xingjie Yu
Singapore Management University, Singapore

Weihuan Zhou
UNSW, Australia

Preface

"Each of us has a vision of good and of evil. We have to encourage people to move towards what they think is good... Everyone has his own idea of good and evil and must choose to follow the good and fight evil as he conceives them. That would be enough to make the world a better place."

– Pope Francis as said to Cultura Oct. 1, 2013.

"To my knowledge, no society has ever existed in which ownership of capital can reasonably be described as "mildly" inegalitarian, by which I mean a distribution in which the poorest half of society would own a significant share (say, one-fifth to one-quarter) of total wealth."

– Thomas Piketty, Capital in the Twenty-First Century, 2014.

Background

Financial inclusion and impact investment are not viewed as main stream activities. Recent exodus of senior bankers and financial practitioners to inclusive FinTech companies has changed that perception somewhat. But perhaps it is still not enough to influence the stakeholders in the incumbents due to the lack of understanding of what these companies do, or a lack of good cases that demonstrate a good Returns on Investment (ROI). Increased awareness of "good" disruptive opportunities in digital banking and Internet finance is important for policy makers and investors alike, so that regulation and investment are appropriately aligned to ensure sustainable world growth.

Many are beginning to view the ***sustainability and success*** of both digital banking and Internet finance businesses as closely linked to the degree of financial inclusion and impact investing. Those at the lower end of the wealth pyramid almost always pay higher charges for services, especially financial services. However, businesses are prevented to take advantage of the higher rates because costs remain high to meet the diverse demand at the bottom. This is so until the emergence of FinTech. FinTech has the advantage of lowering cost and being an enabler for new and profitable business models. More recently, ***Blockchain, a technology that***

originated from cryptocurrency, is seen as an innovation that may propel financial inclusion to new heights. Blockchain has known to lower business costs, but more importantly, it has the potential to change the way business is conducted. It gives rise to new governance structure and how governance is being executed. It enables transparency in digital business models and may help to generate sustainable new revenue streams.

Besides the awareness and interest in new inclusive financial technology, the mindset of investors is also changing because of the slowdown of the offline economy. This is especially true for businesses that are not fully plugged into the digital economy. They are finding it difficult to grow and are faced with profit margin squeezed. Financial institutions are at the frontline of being disrupted.

Declining Returns on Equity (ROE) of financial institutions have pressured many financial institutions into rethinking their own business models and the ways they engage customers. There is now an increase in willingness to fund technology companies and to search for new business models that are data and computing power intensive. The listing of a peer-to-peer platform Lending Club that raised US$870 million in 2014 has heightened concerns that the use of smart data will further threaten profit margins. The increase in the assets under management of Robo-Advisors such as Wealthfront, Bettlement, and Sigfig have also alerted the wealth managers that some of these services are charged at 10% of current practices. However, what really threatens the financial institutions is not the start-ups that ***unbundled*** these silo services of the institutions. The real threat is coming from the large technology companies.

Alibaba's Ants Financial (Alipay) and Safaricom's M-PESA, started off as trust agents for the Alibaba e-commerce platform and telecom service provider respectively, have begun to ***re-bundle*** financial services in a way that no one has done before. They have used data and computing technology to enhance the scope of services with a focus on customers' needs and user experience. They have embraced business models that provide not only financial services originally provided by incumbents, but beyond that into social media, entertainment, crowdfunding, credit rating, insurance, taxi services, delivery services, and other mass market services.

It is important to note that with the new digital business models, not only being scalable is necessary, but the speed of scaling is even more important. Typically, it takes seven years for a tech company to break even. Sustainability is provided mainly by additional funding while building a large Hinternet consisting of hundreds of millions of customers. ***Hinternet is a large online or digital platform with a huge number of sticky customers***. World's top FinTech companies are those with the ability to scale fast in large sparsely populated countries. It is not surprising that Ant Financial (Financial Services), Qudian (Qufenqi, Micro Students Loan), Lufax (P2P and Financial Services), Zhong An (Online Insurance), and JD Finance

(Supply Chain Financing) are all originally located in China and among the top ten FinTech Companies in the world. Many of them are serving the underserved micro enterprises, underserved individuals and the unbanked in remote areas via Internet or digital devices. Many successful companies possess the ***LASIC characteristics, i.e., Low profit margin, Asset light, Scalable, Innovative, and Compliance easy***. Their strategy was not plainly to take advantage of economies of scales, but also to take advantage of economies of scopes.

Because of QE and after the steep run-up of equities, fixed income, real estate, and commodity prices, investors have also been searching for asset classes that exhibit negative correlation with the market. Digital banking and Internet finance that incorporate financial inclusion and impact investing will be an area worthy of attention. Ant Financial, with USD60b market valuation, is larger than American Express Bank, Morgan Stanley, and Bank of New York. The revenue of Ant Financial was RMB10.2b with a net profit of RMB2.6b in 2016. Profit margin of 26% was higher than Goldman, JP Morgan, Wells Fargo, Bank of America, Citigroup, and Morgan Staley that registered between 18% and 25.6% as at third quarter of 2016. Ant Financial has an annual profit growth rate of 64% from 2015 to 2017. Similar statistics are registered for M-PESA that has 24 million registered customers served by a network of over 100 thousand agents spread over Kenya. There are more M-PESA accounts than formal bank accounts of just over 5 million. M-PESA revenue continues to grow at over 20%.

It is worth taking note of the ***4Ds: Digitization, Disintermediation, Democratization, and Decentralization*** (see David LEE Kuo Chuen, The 4Ds: Digitization, Disintermediation, Democratization, and Decentralization, 2017, https://www.slideshare.net/DavidLee215/the-deep-skill-of-blockchain-david-lee-27april2017-final, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2998093). The transformation of the traditional economies will go through the four stages and we are possibly into the second and third stage. Investors and financial institutions seeking for-profit opportunities and higher ROI/ROE in a low-growth environment flushed with liquidity will do well to take advantage of the digital revolution. Both Ant Financial and M-PESA provide good case studies of how businesses are taking a view on combining digitization and inclusion.

Throughout the two volumes, prominent authors will share their technical knowledge, accumulated experiences, business views, political perspectives, and future scenarios. Many of them need no introduction as they are well known academics, practitioners and government officials that were and are still personally involved in the areas that they have written. Topics that are covered are FinTech, Digital Finance, Cryptocurrency, Digital Banking and InsurTech, FinTech Regulation, China FinTech, Security, Blockchain, Inclusion and Innovation, and Emerging Technology.

The last few Chapters focus on the 3rd and 4th D: Democratization and Decentralization. The issues of mobile devices and digital identity are crucial to bring on democratization of

technology and blockchain is potentially the driver for decentralization. For scalability and sustainability, financial inclusion is key as there are still more than 60% of world population that are still underserved or unserved by the financial system, and excluded from the economic, social, and financial system.

It is therefore the editors' view that it is a right time to publish this two-volume handbook explaining and exploring the important concepts and opportunities in financial inclusion, impact investing, and decentralized consensus ledger.

Purpose

Despite rapid development, few technical papers have been written about blockchain, digital finance and inclusion. It will be interesting to analyze the latest technology and product development in these two areas and their implications. The time seems ripe to bring together economic analysis, financial evaluation, methodological contributions, technology explorations, and findings in the three areas.

This two-volume Handbook will provide a collection of papers by pioneers, academics, and practitioners. The authors are carefully chosen from a pool of established experts in their respective fields. The two volumes will deliver first-hand knowledge about the latest developments, the theoretical underpinnings, and empirical investigations. They bridge the gap between the practical usability and the academic perspective, written in a language assessable to practitioners and graduate students. They will appeal to an international audience that wants to learn not only about their own fields of specialization but also fields related to theirs. Each chapter will review, synthesize, and analyze the topic at hand, acknowledge areas where there are gaps between theory and practice, and suggest directions for future research when appropriate.

Themes

The Handbook has three main themes. The first theme is digital finance, and in specific topics such as the disruption, the function, the evolution, and the regulatory environment (or the lack of it) of digital finance. The idea is to discuss the origins and backgrounds of the digital revolution.

The second theme is financial inclusion. Some explore the sustainability of social enterprises, and examine the potential of e-commerce/telecom companies as future digital entities providing services beyond finance.

The third theme centers on decentralized consensus ledgers and the potential of the blockchain in alternative finance. These chapters will explain the technology while speculating about its

use in the future of finance and beyond. The division into three themes is not intended to be hermetic: we expect overlap and links among the chapters of the various parts.

We expect this Handbook to enrich the understanding of the world of blockchain, digital finance and inclusion and be an excellent guide for future work especially in financial inclusion that may bring about sustainable growth. We end the preface with the following quote from Evangelii Gaudium, Apostolic Exhortation by Pope Francis, 2013:

> *"In this context, some people continue to defend trickle-down theories which assume that economic growth, encouraged by a free market, will inevitably succeed in bringing about greater justice and inclusiveness in the world. This opinion, which has never been confirmed by the facts, expresses a crude and naïve trust in the goodness of those wielding economic power and in the sacralized workings of the prevailing economic system. Meanwhile, the excluded are still waiting."*

Hopefully, with a better understanding of how technology can substantially lower operation cost and can create new scalable business models with big data, artificial intelligence, Internet of Things, and computing power, the excluded need not wait too long with technology serving the entire pyramid! With new technology giving hope to achieve a "mildly" inegalitarian distribution in which the poorest half of society would own a significant share (say, one-fifth to one-quarter) of total wealth.

Acknowledgment by David LEE Kuo Chuen

This two-volume Handbook is a project of more than a year dating back to 2015 and two conferences with Stanford University as the beginning and the link. This work would not have been possible if not for the support of the US Treasury for the 2015 Fulbright Visiting Fellowship at Shorenstein Asia–Pacific Research Center at Stanford University. Much of the initial research and understanding of FinTech and inclusion started when the first editor David LEE Kuo Chuen was in Palo Alto researching the Silicon Valley eco system. The mission of the fellowship was to harness Silicon Valley technology to serve the underserved in Asean to be mentored by the late Harry Rowen.

The "SKBI-BFI Smart Nation, Silicon Valley Technology and Connectivity Inclusion Conference" was held on 17th November 2015 at the Bechtel Conference Center, Stanford, California, United States (https://skbi.smu.edu.sg/conference/131141?itemid=611). The late Professor Harry Rowen, who served four US Presidents, was the mentor for the Fulbright Fellowship and scheduled as the first speaker for the conference. Unfortunately, he passed away a

few days before the conference. These two volumes are published in memory of both the late Sim Kee Boon and the late Professor Harry Rowen without whom this project would not have started.

> *The late Sim Kee Boon was one of Singapore's pioneer civil servants – men who worked closely with the Old Guard political leaders and played a key role in the success of Changi Airport and turned the fortunes of Keppel Shipyard around. He is among the most versatile of Singapore public servants. He spent all his working life making invaluable contributions in his various roles in Government, particularly in the areas of economic development, trade and investment matters. Mr. Sim dedicated himself fully to serving the country.*
>
> *The late Henry Rowen was a professor emeritus of Stanford University affiliated with the Graduate School of Business, the Hoover Institution and the Asia/Pacific Research Center of the Freeman–Spogli Institute for International Studies. His non-academic jobs included heading a major non-profit research company (the RAND Corporation) and serving in several Washington agencies under four presidents (two Democratic and two Republican). They have been Assistant Director of the Bureau of the Budget, Chairman of the National Intelligence Council and Assistant Secretary of Defense for International Security Affairs. He published "The Silicon Valley Edge: A Habitat for Innovation and Entrepreneurship" and "Making IT: The Rise of Asia in High Tech" with several other authors, way before the interest in FinTech.*

Special appreciation goes to Prof Tan Chin Tiong and Prof David Montgomery for connection to Stanford as well as the guidance of Acting Director of APARC Prof Takeo Hoshi and Director Professor Gi Wook Shin. Associate Director Huma Shaikh, Center Event Coordinator Debbie Warren, and Executive Assistant Kristen Lee and others at Stanford were most helpful during the initial period of research and the first conference.

I would like to thank Noreen and Herman Harrow for allowing me to stay with them to write some of the chapters while in Monterey; Erika Enos for introducing me to various start-ups and design studios; David Schwartz for going out of his way to assist me in organizing the Smart Nation Conference at Stanford; Ron and Pat Miller, and Barbara Gross for their company and allowing us to play with their dogs.

The following up conference entitled "FinTech and Financial Inclusion: Nascent financial technologies for enhancing access to finance" (https://skbi.smu.edu.sg/conference/142741) was jointly organized with SKBI, IMF, Stanford University, India School of Business, Singapore University of Social Sciences (Formerly UniSIM), Humboldt – Universität zu Berlin,

and supported by the Monetary Authority of Singapore and UOB. Other supporting organizations were ChainB.com and Idea Ink, Association of Cryptocurrency Enterprises and Start-ups (ACCESS), Chartered Alternative Investment Analyst Association (both the San Francisco and Singapore Chapters), Economic Society of Singapore, Financial Planning Association of Singapore, iGlobe Partners, Internal Consulting Group, Plug and Play and Singapore Accountancy Commission. Many papers are drawn from this conference.

The Board of Advisors and staff at Sim Kee Boon Institute for Financial Economics (SKBI) are most helpful and the editors are heavily indebted to them. Without the then Provost Rajendra Srivastava and Dean Howard Thomas for "twisting" David Lee's arm to become both the Academic and Executive Director for the Institute, the research would not have taken shape for the two volumes.

Stephen Riady, Chairman of OUE and Lim Chee Oon, ex-Chairman of SKBI, are always great mentors. Special appreciation goes to Jacqueline Loh, Leong Sing Chiong, Mohanty Sopnendu, Roy Teo, Bernard Wee, Stanley Yong and Tan Yeow Seng from the MAS; Auback Kam, Tan Kok Yam, Lee Chor Pharn, Derrick Cham and Jacqueline Poh from the Civil Service, Philip Foo, Priscilla Cheng, and Elaine Goh from SKBI. My special thanks to President Arnoud De Meyer, Provost Lily Kong, Dean Gerry George, Annie Koh, Steve Wyatt, Phil Zerrillo, Christopher Dula, Ernie Teo, Wan Zhi Guo, Yan Li, Pei Sai Fan, Lim Kian Guan, Fock Siew Tong, Francis Koh, Benedict Koh Seng Kee, Chan Soon Huat and others that have helped in many ways. Thanks to those colleagues at Singapore University of Social Sciences, especially Provost Tsui Kai Chong, President Cheong Hee Kiat, Chancellor Aline Wong, Dean Lee Pui Mun, Phoon Kok Fai, Joseph Lim, Linda Low, Ding Ding, Yu Yin Hui, Calvin Chan, Guan Chong, Jason Chiam, and Rubini Nyana. Appreciation also to the support of CAIA, especially William Kelly, Peter Douglas, Joanne Murphy, Scott Nance, Hossein Kazemi, Nelson Lacey, and Wendy Leung. The President of CFA Paul Smith is generous to comment on these two volumes. Without the hard work of Susan Ikeda, Susan Li and the encouragement of Scott Bentley, this project would have been impossible.

My research assistants have been most helpful in collating and preparing the tables and figures, especially Zoey Phee, Yu Xiaoyi, and Dian Fu Research Team consisting of Zhang Han, Chang Su, Chi Ying, and Lin JingXian; the Blockchain Research Team consisting of Wu Yuting, Zhang Mengyu, Sun Ming, Chen Wanfeng, Huang Yiya, Lee Yinhao; the FinTech Research Team consisting of Ng Jing Ying, Kelvin Lim Jia Hui, Abraham Albert Putihrai and Ian Chong Wei Ming; and the Silicon Valley Research Team consisting of Natasha Singhal and Guo Zongren. Many more from my MAF, MWM and GMF classes have helped and I apologize for omitting anyone and not explicitly thanking them.

My family, who always bear with me for spending many nights away in my study room finishing the work, are a force behind these two volumes. Much of the inspiration of this work

came from Evangelii Gaudium by Pope Francis and the work of Thomas Piketti. I thank God for guiding me towards a direction of research to serve the entire pyramid that I continue to enjoy. May this book be used in a way to benefit the needy, the excluded and the neglected of this world!

Acknowledgment by Robert Deng

I am very grateful to David LEE Kuo Chuen for initiating this project and for having me as his co-editor. I would like to thank all the authors and everyone else who have contributed to this Handbook and made it possible. My utmost gratitude goes to my family for their unconditional love and support.

17 March 2017

David LEE Kuo Chuen

Robert Deng ed.

CHAPTER 1

The Game of Dian Fu: The Rise of Chinese Finance

David LEE Kuo Chuen, Ernie G.S. Teo

Contents

1.1 Introduction: What Is Dianfu 颠覆? 2

1.2 Dian Fu One: Dian Fu in the Equity Market 3

1.2.1 Rise of China's GDP 3

1.2.2 Rise of China's Stock Market 4

1.2.3 Market Capitalization of the World's Top Stock Exchanges 4

1.2.4 National Equities Exchange and Quotations (NEEQ) 5

1.2.5 Private Equity and Venture Capital 8

1.2.6 Variable Interest Entity (VIE) 12

1.2.7 Investment Abroad 14

1.3 Dian Fu Two: Dian Fu in China's Peer-to-Peer Lending 15

1.4 Dian Fu Three: Dian Fu in Crowdfunding 21

1.5 Dian Fu Four: Dian Fu in the People's Currency 25

1.6 Dian Fu Five: Dian Fu in Banking 27

1.7 Conclusion 30

1.7.1 Financial Inclusion and Fintech 30

1.7.2 Expanding to the ASEAN Region 32

Appendix: Acquisitions of Alibaba 33

Acknowledgments 34

References 34

Notes 36

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00001-2
Copyright © 2018 Elsevier Inc. All rights reserved.

1.1 Introduction: What Is Dianfu 颠覆?

In tandem with the meteoric rise of the Chinese economy, financial institutions in China have grown very large in a short time. This is achieved through innovation not only in technology but through products and services. Industrial and Commercial Bank of China (ICBC) is now the largest bank in the world, UnionPay is the largest credit card issuer, and AliPay is the largest third-party payment company. In the Peer-to-Peer (P2P) lending sector, CreditEase has come to dominate the world, Lend Academy (2013 December 03).

The rise in the number of Chinese FinTech is an interesting factor contributing to the growth of China's finance market. These fintech firms may not originate from traditional financial institutions but instead come from industries such as e-commerce. E-Commerce firms, such as Alibaba (阿里巴巴) and its Tao Bao ((淘宝) platform, have been experiencing rapid growth compared to American's platforms like eBay and Amazon (Morgan Stanley Blue Paper, 2014). E-commerce, with a combination of online and offline (OAO) operations, will be a potential key driver of the finance market in the future (Dahlman and Aubert, 2001). By creating stickiness to its users, platforms that offer third-part payments, e-commerce, logistic, trade, supply chain services will fuel growth of financial services such as insurance, lending, financing, wealth management, crowdfunding, credit rating, and other banking services. Given the market potential, it is hardly surprising that the number of incubators and accelerators has increased exponentially over the years. There were 1,600 incubators in China as of June 2015 (Johnston and Zhang, 2015). Out of these 1,600 incubators, over 600 of them were incubators of national level. Fintech and Blockchain companies are drawing increased attention from these incubators and venture capital in China.

With language as a barrier, it may be difficult to follow developments in China. For instance, online financial services such as Yu'E Bao (余额宝), Zhao Cai Bao (招财宝), Yu Le Bao (娱乐宝), Zhima Credit (芝麻信用), Qudian (趣店), ZhongAn (众安), JD (京东), Rong360 (融 360), Zhongtuobang (众托邦) are well-known in China, but may not be familiar to those from outside China. This chapter aims to bridge some of the knowledge gaps of Chinese finance.

There are a few interesting questions we hope to address: What are the potentials and pitfalls of the future developments of China, Asia and the world at large? Will the Chinese financial giants disrupt the global financial industry just as the Chinese industrial upsurge has disrupted other areas such as manufacturing, logistics and shipping? To understand the rise of Chinese finance, it is important to understand the concept of Dian Fu.

Dian Fu (颠覆) in Chinese means to disrupt, overturn, subvert and overthrow. In particular, the growth of Alibaba to a dominant position in the e-commerce world with its associated company Ant Financial is dominating the payments industry in China. When Alibaba first

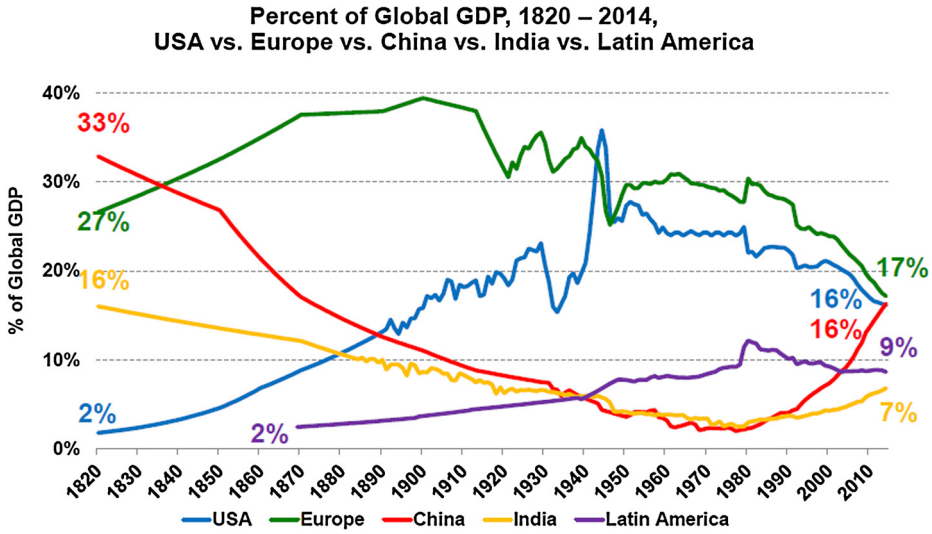


Figure 1.1: Percent of global GDP, 1820–2014.
(Source: Angus Maddison, University of Groningen, OECD, 2014)

started, eBay had 60% of the market share in China. However, within a short period of time, eBay had to exit from the Chinese market.[1]

Five categories of Dian Fu will be presented in this paper. We explain how the change in the Chinese environment has brought about great progress in its financial sector, by examining each category of Dian Fu. Next, we discuss possible scenarios of the future of Chinese finance. Finally, we conclude with a discussion of the strategies deployed by the Chinese government, such as employing the Bi-Lateral Swap Agreement for Renminbi (RMB), the setting up of Asia Infrastructure Investment Bank, adoption of "One Belt, One Road" (OBOR) policy and other related policies aimed at transforming the Chinese financial sector.

1.2 Dian Fu One: Dian Fu in the Equity Market

1.2.1 Rise of China's GDP

China has been experiencing a rise in its GDP since the 1970s, and has been growing exponentially since then. The share of Chinese GDP to world GDP has increased to 16% in recent years (see Fig. 1.1). China's GDP share is predicted to overtake the US in 2016. Several policies will be implemented in the coming years, such "One Belt, One Road" and internationalization of blockchain-based e-RMB, to position China as an attractive partner for foreign

www.elsevierdirect.com



Figure 1.2: China stock value 1992–2015.
(Source: Lu, 2014)

investors (Acutus, 2015), as well as a major infrastructure investor into regions of high economic growth.

1.2.2 Rise of China's Stock Market

The great economic growth of the Chinese market in the past could be observed through the changes in its stock market. The stock market in China has been growing steadily since 2001 in market capitalization, number of listings and trading volume. China had 2613 listed companies, and they are valued at a market cap of ¥37.24 trillion as at 2015 (as depicted in Fig. 1.2).

1.2.3 Market Capitalization of the World's Top Stock Exchanges

The total market capitalization of the Shanghai Stock Exchange (SSE) and Shenzhen Stock Exchange (SZSE), excluding Hong Kong Stock Exchange (SEHK), amounted to the US$9.6 trillion as at end June 2015. The exchanges' market capitalization increased by more than 65% over first six months of 2015. With 2613 companies in 2014 and a combined market capitalization of USD5.8 trillion, the SSE and SZSE is a staggering ten times that of 2002. There is still much room for expansion in the Chinese securities market as China is projected to grow at an average 6% per annum. Based on the GDP to market capitalization, China market is predicted to catch up with the larger stock exchanges, such as the New York Stock Exchange (NYSE) and the National Association of Securities Dealers Automated Quotations (NASDAQ) (as reflected in Fig. 1.3). However, what is more interesting to observers is the development of Chinese finance, especially the rise of the National Equities Exchange and Quotations (NEEQ) that fuels the growth of innovative start-ups.

www.elsevierdirect.com

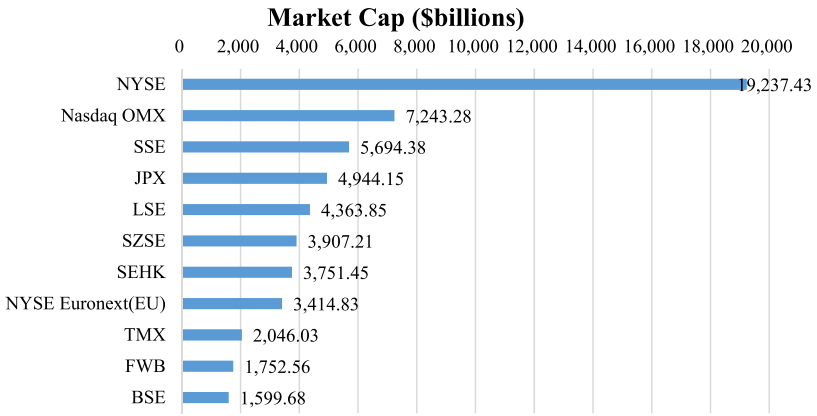


Figure 1.3: Market cap ($ billion).
(Source: World Federation of Exchanges – Bloomberg, 2015)

1.2.4 National Equities Exchange and Quotations (NEEQ)

The National Equities Exchange and Quotations (NEEQ) is China's newest stock market and the third board. It is an alternative to the Shenzhen and Shanghai stock exchanges set up primarily for advanced production and technology companies. NEEQ is an over-the-counter (OTC) market that provides greater financing opportunities for small companies with less stringent listing requirements. The third board is also the only OTC market regulated by the China Securities Regulatory Commission (CSRC). Recently, CSRC has relaxed regulations to allow qualified foreign institutional investors (QFII) and RMB Qualified Foreign Institutional Investors (RQFII) to invest in NEEQ. Individual investors with ¥500,000 instead of ¥ 5m can now participate in the market – a move that is likely to attract more liquidity to NEEQ.

NEEQ was started in 2006 in Beijing, expanded nationwide in 2013, and took off in 2014. As at 2015, there are over 2800 listed firms on NEEQ (see Fig. 1.4). Investors are mostly local private-equity firms and individuals. Shares in NEEQ can be transferred in three ways: 1) Equity-transfer agreements, which is the main method, representing over 60% of transfers; 2) The market-maker (dealer) system, which grew rapidly in 2014 and now accounts for about 30% of transfers; 3) A bidding system, which is same as those of the main exchanges. The last accounts for less than 10% of transfers because of the lack of liquidity in NEEQ, but is expected to grow.

Listing on NEEQ is sought after by technology and media companies and the number has increased due to the low listing requirements. Companies with continuous earnings will qualify for listing on NEEQ. There are no requirements on cash flows, net assets, and total capital stock. As illustrated in Fig. 1.5, the NEEQ listed entity can be upgraded to Second Board,[2]

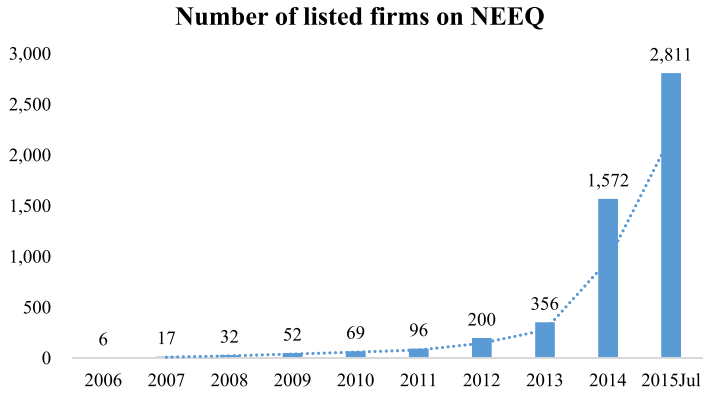


Figure 1.4: Number of listed firms on NEEQ, 2006–2015.
(Source: Business Sohu (搜狐财经), 2015)

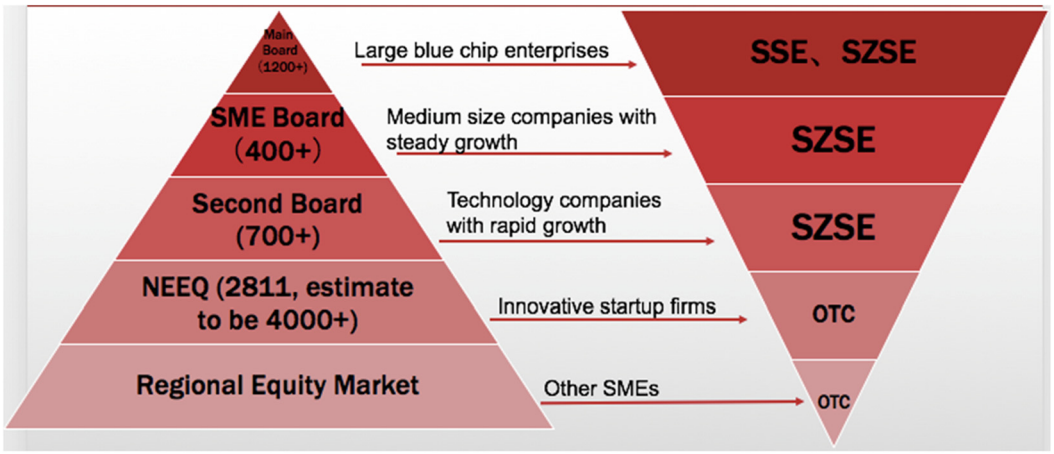


Figure 1.5: China securities exchange's structure.
(Source: Lee and Teo, 2015)

Small Medium Enterprise Board,[3] as well as the Main Board if it meets certain minimum requirements in profit margin and market value. NEEQ listed entities are known to be acquired by big firms at high P/E ratios.

With the positive outlook and high returns of the Chinese stock market, over 100 NASDAQ listed Chinese companies were planning to delist from NASDAQ and relist in China. This phenomenon of delisting and relisting indicates the success of the exchanges as platforms to encourage investment in start-ups that are innovative. Majority of these firms are Technology, Media, and Telecommunications (TMT) companies, as observed in Fig. 1.6.

www.elsevierdirect.com

S/N	Companies	Industries	Ticker	Current Market CAP/ Pre-Delist Market CAP ('100 million USD)	Privatisation announced on	Privatisation Completed on	Status
1	Momo Inc.	Technology	MOMO.O	32.15	2015.6.23	--	In Progress
2	Vimicro Corporation	Technology	VIMC.O	3.38	2015.6.22	--	In Progress
3	China Info Tech	Technology	CNIT.O	1.28	2015.6.22	--	In Progress
4	AirMedia Group Inc	Mobile Communications Operator	AMCN.O	3	2015.6.19	--	In Progress
5	Qihoo 360 Technology Co Ltd	Technology	QIHU.N	87.16	2015.6.17	--	In Progress
6	iDreamSky Technology Ltd	Technology	DSKY.O	5.59	2015.6.13	--	In Progress
7	Bona Film Group Ltd	Service Industry	BONA.O	7.98	2015.6.12	--	In Progress
8	Homeinns Hotel Group	Service Industry	HMIN.O	15.29	2015.6.11	--	In Progress
9	21Vianet Group Inc	Technology	VNET.O	17.77	2015.6.10	--	In Progress
10	Renren Inc	Technology	RENN.N	14.62	2015.6.10	--	In Progress
11	E-House (China) Holdings Limited	Finance	EJ.N	9.26	2015.6.9	--	In Progress
12	JA Solar Holdings Co Ltd	Finance	JASO.O	3.9	2015.6.5	--	In Progress
13	Mindray Medical International Ltd	Health Care	MR.N	33.89	2015.6.4	--	In Progress
14	Taomee Holdings Ltd	Technology	TAOM.N	1.24	2015.5.30	--	In Progress
15	China Mobile Games and Entertainment Group Limited	Technology	CMGE.N	6.58	2015.5.18	--	In Progress
16	WuXi AppTec	Health Care	WX.N	30.77	2015.4.29	--	In Progress
17	China Cord Blood Corporation	Biotechnology	CO.N	5.16	2015.4.27	--	In Progress
18	Xueda Education Group	Service Industry	XUE.N	2.51	2015.4.21	--	In Progress
19	Sungy Mobile Limited	Technology	GOMO .N	1.54	2015.4.13	--	In Progress
20	Jiayuan.com International Ltd	Technology	DATE.N	2.4	2015.3.17	--	In Progress
21	Shanda Games Limited	Technology	GAME.O	18.66	2015.1.27	--	In Progress
22	Perfect World Co., Ltd	Technology	PWRD.N	9.66	2014.12.31	--	In Progress
23	GIANT INTERACTIVE GROUP INC	Technology	GA.N	28.57	2013.12.19	2014.7.18	Completed
24	ChinaEdu Corporation	Education	CEDU.N	0.6	2013.6.21	2014.1.1	Completed
25	FOCUS MEDIA HOLDING LTD	Service Industry	FMCN.O	36.21	2012.8.13	2013.5.24	Completed

Figure 1.6: Privatization of the Chinese stocks listed in the U.S.
(Source: Careerin.cn, 2015, http://www.nasdaq.com (2015/6/24) and chinadaily.com)

In June 2015, there was a major correction in the China stock market. It resulted in a huge negative spillover effect to the rest of the world (Institute of Chinese Studies, 2015). Despite the crash, firms that were listed on NEEQ ended in positive returns towards the end of the

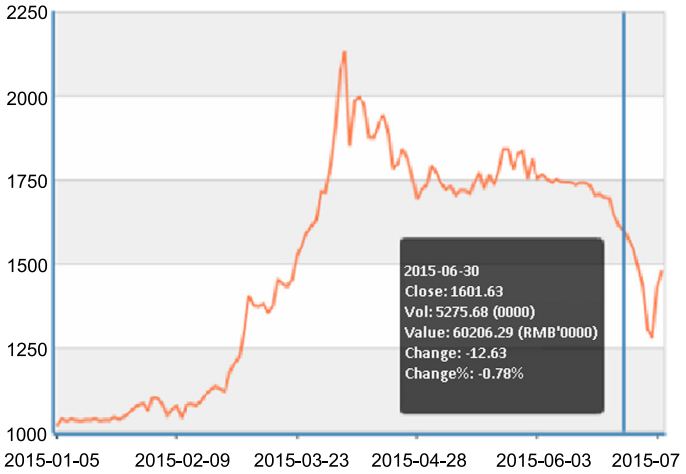


Figure 1.7: Market value of NEEQ, Jan. to Jul. 2015.
(Source: Lee and Teo, 2015 and Careerin.cn)

year and outperformed the S&P Composite Index. The rapid rise in the China Stock Market has caused the delisting from other offshore markets besides NASDAQ and this trend will continue as long as there is more liquidity in China. This rapid flow of funds into the stock exchanges has stimulated great interest in investment in start-ups and micro-, small, and medium enterprises via private equity and venture capital. The lighter touch approach of the exchanges, with the encouragement from the Government for start-ups, has played a major role in attracting technology companies to list on NEEQ, fueling interest in smaller companies that seek offshore listing previously. This Dian Fu impact by the exchanges, especially NEEQ, has been positive for the development of Internet, Finance, Media and Technological start-ups.

However, ever since the correction of the stock market, China Government and CSRC (China Securities Regulatory Commission) took many immediate measures to stabilize the securities market and tightened regulation. The stock market was much more stable in the third quarter of 2015. The volatility of securities' indexes has since reduced (as shown in Fig. 1.7).

1.2.5 Private Equity and Venture Capital

Within the last 10 years, there is a significant increase in private equity in China. The number has increased from 10 firms in 1995 to more than 8000 firms in 2015, managing over US$620 billion (Deloitte, 2014). The private equity sector in China has been on an exponential rise since 2008 and the investable amount has crossed a high figure of US$147 billion during the

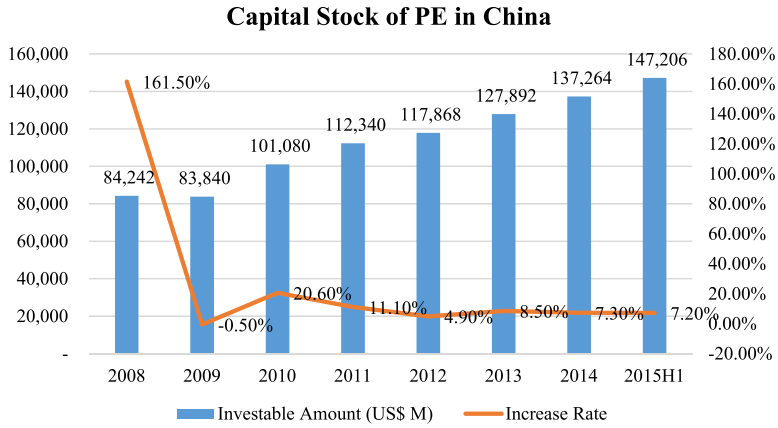


Figure 1.8: Capital stock of PE investable amount in China, 2008–2015.
(Source: Qingke Data, 2015; Lee and Teo, 2015)

first half of 2015 (as shown in Fig. 1.8) (Qingke Data, 2015). A growth of 7.2% was experienced in 2015. The top five highly invested industries are the Internet, Finance, Media, IT and Biotechnology industries.

Rise of wealth in China and its changing demographics have resulted in large amount of funds being injected into PE firms, VCs, NEEQ and P2P platforms. Those listed on the NEEQ include both high-tech enterprises and investment agencies. Examples of investment agencies are Jiu Ding Investment (九鼎投资) and Silicon Valley Paradise (硅谷天堂). The NEEQ is set up to support the Government's objectives of developing and reforming the capital market, so as to support innovation and encourage corporate restructuring. In line with the policy, more NEEQ funds are expected to set up in the coming years to serve as a new source of funding for start-ups. The number of NEEQ funds has grown from 13 in 2013 to 640 in June 2015 with an investable amount of more than USD147b, while this can also be viewed as an earlier exit route for PE and VC investments. Figs. 1.9 and 1.10 list the top 10 PE firms and top 10 VC firms in China, respectively. The regulator's initial hands-off approach to the development of this sector has resulted in exponential growth.

The growth of PE/VC sector has an impact on the State-Owned Enterprises (SOEs) that are heavily in debt. The PE/VCs are playing an important role of restructuring the SOEs. There was a shift from self-governance to a deepening of restructuring exercise of the SOEs. In the mid July report by Standard & Poor's (S&P), China was holding an estimated amount of US$14.2 trillion of Chinese Corporate Debt in 2013.[4] In a sector that employs a large number of workers, China has to find ways to restructure its debts. SOE plays a very crucial role in the Chinese economy. It contributes 2/5 of the country's gross domestic product (GDP) and 1/5 of employment.

www.elsevierdirect.com

Rank	Chinese Name	English Name
1	鼎晖投资基金管理公司	CDH Investment Fund Management Company
2	高瓴资本管理有限公司	Hillhouse Capital Management
3	老虎环球基金	Tiger Global Fund
4	腾讯产业共赢基金	Tencent Collaboration Fund
5	上海云锋投资管理有限公司	Shanghai Yunfeng Investment Management Co. Ltd
6	复星资本	Fosun International
7	中信产业投资基金管理有限公司	Citic Industrial Investment Fund Management Co. Ltd
8	昆吾九鼎投资管理有限公司	Kunwu Jiuding Investment Management Co. Ltd
9	博裕投资顾问有限公司	Boyu Capital Advisory
10	DST	DST

Figure 1.9: Top 10 PE firms in China.
(Source: PE Daily, 2015)

Rank	Chinese Name	English Name
1	IDG 资本	IDG Capital
2	红杉资本中国基金	Sequoia Capital China
3	深圳市创新投资集团有限公司	Shenzhen Innovation Investment Group Co. Ltd
4	江苏高科技投资集团	Jiangsu Venture Capital Co. Ltd
5	DCM 戴盛资本	Delta Capital Markets Ltd
6	达晨创业投资有限公司	Dachen Venture Investment Co. Ltd
7	赛富亚洲投资基金之管理公司	SAIF Partners
8	启明维创创业投资管理（上海）有限公司	Qiming Venture Partners (Shanghai)
9	深圳市同创伟业创业投资有限公司	Cowin Capital
10	北京金沙江创业投资管理有限公司	GSR Ventures

Figure 1.10: Top 10 VC firms in China.
(Source: PE Daily, 2015)

www.elsevierdirect.com

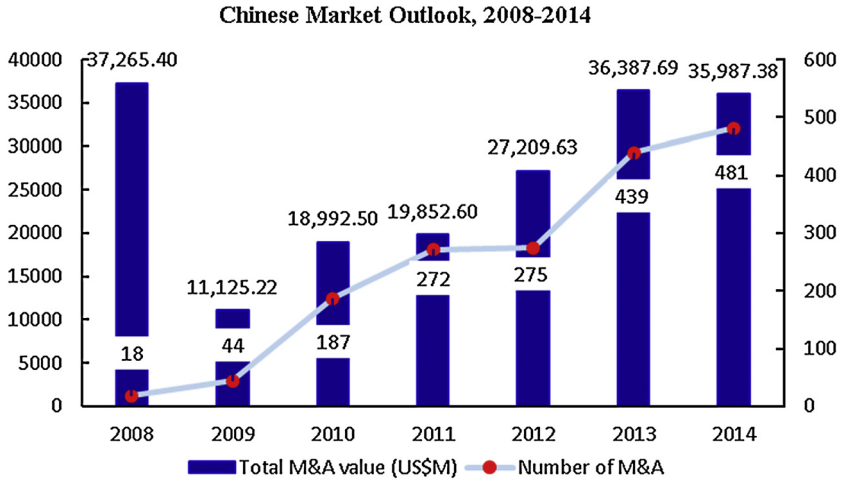


Figure 1.11: Chinese market outlook, 2008–2014.
(Source: National Bureau of Statistics of China, 2014)

According to Fig. 1.11, there were 481 cases of mergers and acquisitions (M&A) valued at US$35 billion in China in 2014. Standard Chartered Bank China (SCB) estimated the overall debt of China to have increased from 150% to 245% of its GDP from 2008 to 2014. The total debt value of China in 2014 was estimated to be US$22.8 trillion.

From Fig. 1.12 it can be observed that there were 62 investments in 2014 and the VC/PE investment has amounted to US$8.9 billion. This is due mainly to the relaxation of Government law and regulations. The various local governments in China are now allowed to issue market-directed debt instruments on top of the existing State-directed debt swap resulting in lower borrowing cost. There were also promotions of Public-Private-Partnerships (PPPs). China has been attempting to pursue its strategy of promoting stock ownership from a low of single digits of 9% of the population to a larger percentage. Asset sharing via the stock market has the advantage of allowing the population to share the growth of the economy and at the same time, lowering the debt burden of the privatized SOEs. While the crash of the market in 2015 has slowed the growth of the chinese market, the strategy of increasing share ownership via public and private equity remains intact. The PE and accelerators crossed 600 in June 2015. The largest areas include Beijing with 36, Shanghai with 28, Jiangsu with 114, Zhejiang with 43, Tianjin with 30, Guandong with 43, Shandong with 54, and Liaolin with 31. In 2016, many blockchain labs were set up including Wanxiang (万向), Yunxiang (云象). In Shanghai, Chainlab was launched as an accelerator for blockchain start-ups. In September 2016, the International Blockchain Week, jointly organized by Ethereum Foundation and Wanxiang, was held in Shanghai over six days. Starting with Devcon2, a developers' conference organized by

www.elsevierdirect.com

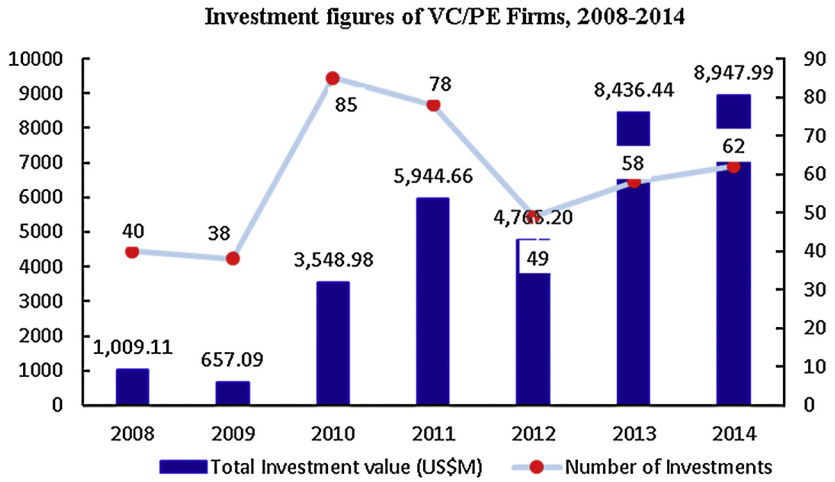


Figure 1.12: Investment figures of VC/PE firms, 2008–2014.
(Source: National Bureau of Statistics of China, 2014)

the Ethereum Foundation, the event was followed by a demo day hosted by Chainb.com and the 2nd Global Blockchain Summit hosted by Wanxiang. The event attracted close to 1000 attendees (local and international) each day. China has established itself as the blockchain center of the world with USD 30b investment in the Wanxiang blockchain smart city project in Hangzhou which covers over 83m square feet of land, using blockchain to manage Internet of Things. The project is expected to develop innovations at the intersection of transport, smart cities and blockchain. A blockchain focused fund Fenbushi with USD30m capital is also the only blockchain fund in the world with over 35 companies in its global portfolio focusing mainly on the Ethereum platform and cryptocurrency technology.

1.2.6 Variable Interest Entity (VIE)

In China, foreign direct investment has been classified into four categories: (1) encouraged; (2) permitted; (3) restricted; (4) prohibited. Different categories are subject to different levels of governmental review. As such, foreign investors must obtain certain approvals from the Government for their investments in China. It can be difficult to obtain approval to access certain industries, especially restricted industries, such as value-added telecommunication services, direct sales, mail order, and online sales.

There is an innovative way to enjoy cashflow and participation in restricted industries via the Variable Interest Entity (VIE) structure. VIE is an entity in which the investor holds a controlling interest on usage, cashflow, lease, or other arrangement without direct ownership in

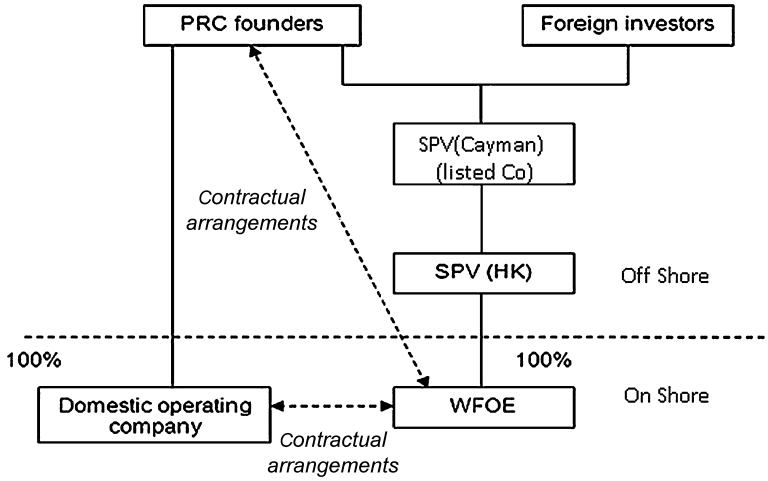


Figure 1.13: Variable interest entity model.
(Source: Charltons, 2012)

restricted industries. By using a VIE structure, foreign investors do not need the PRC Government's approval for a foreign direct investment since they do not own the equity of the Target Company nor directly participate in operation. However, they can still indirectly participate in a Target Company and receive revenues from it. It is an interesting contractual arrangement to separate ownership from revenues and/or operation control.

In a VIE structure, as Fig. 1.13 shows, foreign investors can indirectly control and derive economic benefits from a subsidiary or subsidiaries (Target Company or Group of Companies) through the ownership of a Wholly Foreign-Owned Entity (WFOE). The WFOE has certain indirect controls and benefits through the contractual agreements (VIE contracts) with the Target Company and the shareholders of the Target Company.

Four mega VIEs (Sina, Baidu, Alibaba and Tencent) have successfully ventured out of China. Sina, Baidu, and Alibaba and Tencent[5] have used similar structures to list on exchanges outside China. This structure is also commonly referred to as the Sina-model structure since it was first used by Sina in 2000. The VIE structure plays an important role in allowing foreign shareholders to participate in some of the Chinese industries, especially the Internet industry. For those VIEs seeking delisting from foreign exchanges and planning to relist on the Chinese exchanges, it is a cumbersome and time consuming exercise. To address the difficulties of unbundling the VIEs and to facilitate relisting, the Government has recently announced that Chinese stock exchanges will accept VIE structure for listing. This will shorten the lead time for VIE relisting in China and will grow the market capitalization further when market conditions stabilize.

www.elsevierdirect.com

1.2.7 Investment Abroad

In the early 1990s, those Chinese companies with assets offshore were able to conduct backdoor listing by pledging their offshore assets to banks outside China. Many established Chinese firms have ventured out of China to list abroad using offshore assets, an alternative route from the VIE structure. Some prominent examples include Cosco and China Everbright in Singapore, China Travel International Investment Hong Kong Ltd. and Tsingtao Brewery in Hong Kong. They used either backdoor listing methods or obtained special permission from the central authority. Cosco was the first company to embark on a backdoor listing with offshore assets (ships) in Singapore in 1993, followed by China Everbright. China Travel International Investment Hong Kong Ltd. was listed in Hong Kong in 1992 followed by 10 to 15 back door listings of other Chinese companies. Tsingtao Brewery H shares were listed on the Hong Kong Stock Exchange in July 1993 followed by nine other approved companies. In late 1994, another 22 companies were approved for listing in Hong Kong accelerating the growth of "H" share markets. These listed Chinese companies were collectively known as the Red Chips market.

But in 2015, the trend reversed. Instead of listing offshores for foreign capital, the Chinese listed companies are investing Chinese capital and acquiring aggressively offshore. In the earlier years, the listed companies were listed offshore and at times, reinvested into China to take advantage of tax holidays and to more flexible regulation enjoyed by foreign companies. Listed below are some activities of recent overseas ventures. In the 3rd week of Aug. 2015, ten listed Chinese companies have announced mergers and acquisitions (M&A) deals outside China. In Q2 2015, overseas M&A activities have increased 60% to US$32.55 billion, with 128 deals mainly in TMT, real estate and finance.

Shun Rong San Qi (顺荣三七) has acquired 81.25% of SNK, a Japanese games company, for US$63.5 million, Su Ning Huan Qiu (苏宁环球) has acquired 20.17% of Korea's REDROVER for ¥242 million, and Zi Jin Kuang Ye (紫金矿业) has acquired 100% of Australia's Phoenix Gold Limited for ¥200 million. The trend has now reversed and instead of reinvesting into China from offshore listed vehicles, the Chinese listed domestic entities are investing offshore. The strategy is to Zou Chu Qu (走出去) or Chu Hai (出海), which means to invest offshore in preparation of internationalization of the Chinese Yuan and rebalancing of the massive buildup of foreign reserves that has fueled asset inflation in China. Needless to say, the technology companies are aggressively investing offshore. As an interesting example, we have listed the acquisitions of Alibaba in the appendix.

Since 2007, "Dim Sum Bonds", which are RMB-nominated bonds, are issued outside mainland China. In April 2011, the first RMB Initial Public Offering (IPO) occurred in Hong

Kong, when the Chinese property investment trust Hui Xian raised ¥ 10.48 billion ($1.6 billion) in its IPO. Beijing has allowed RMB-denominated financial markets to develop in Hong Kong as part of the effort to internationalize the RMB.

1.3 Dian Fu Two: Dian Fu in China's Peer-to-Peer Lending

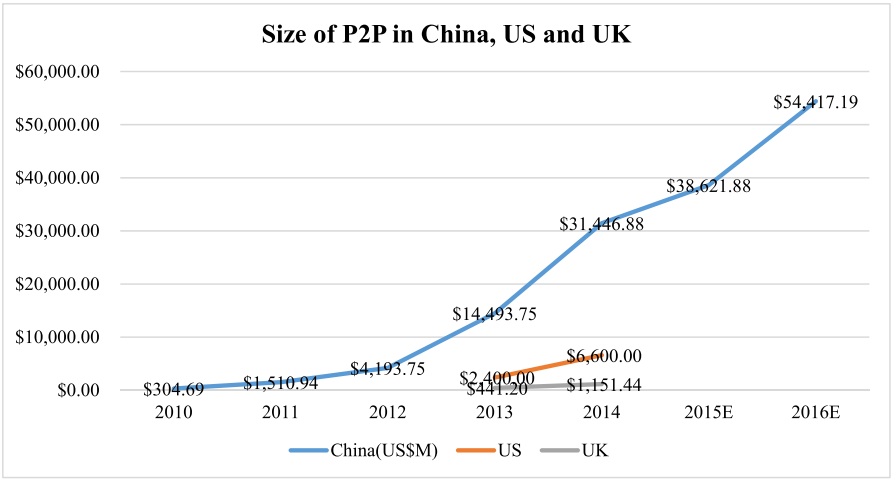
Internet finance is developing at a lightning speed in the 21st century, and many new online financial instruments such as P2P loans are surfacing in the market. P2P lending is a form of financing that allows borrowers to obtain a loan from a group of individual lenders without going through an intermediary, such as a bank. This scheme is targeted at Micro-, Small and Medium Enterprises (MSMEs) and individuals who are not covered under the traditional financial services. This online platform could be seen a form of enhancement to the current traditional financial system if proper risk management is adopted utilizing big data and artificial intelligence.

Peer-to-Peer lending platforms (P2Ps) have their origins in the US when Lending Club started in 2006. In the United States, the P2P market is dominated by two large players, Lending Club and Prosper Funding LLC. They accounted for 96% of the US P2P market (Wang et al., 2009). Transaction fees, servicing fees and management fees account for most of the revenue. In China, there were more than 2028 of such online loan companies in the first half-year of 2015 (China Daily, 2015). Some of these are only acting as platforms for borrowers and lenders to come together, while others might be involved in the financial transactions as well. The former will exhibit lower risks than the latter. Some examples are Pai Pai Dai (拍拍贷), Dian Rong Wang (点融网) and so forth.

In recent years, P2Ps have developed due to the low barriers of entry, strong liquidity and convenient procedures. Traditional financial institutions exhibit much higher capital expenditure (CAPEX) and barriers of entry. The Internet has enabled these online platforms to act as a medium to reduce CAPEX and enhance efficiency to meet the needs of lenders and borrowers. This allows SMEs that have difficulties borrowing from traditional banks to have access to capital. SMEs which are in need for financial support but are unable to obtain loans from traditional banks turn to P2P. The rise of P2P platforms has also helped to reduce the number of SMEs taking up small loans from private finance companies which are charging very high interest rate (Chen and Han, 2012).

In China, P2Ps are experiencing an exponential growth ever since the launch of the P2P unsecured online petty-sum lending platform, Pai Pai Dai (拍拍贷) in 2007. The 2028 P2Ps handled ¥ 683.5 billion loans that amounted to over ¥ 208.7 billion outstanding in the first half of 2015. In Fig. 1.14, it is shown that the size of P2P in China has grown so fast that it

www.elsevierdirect.com



(US$ M)	2010	2011	2012	2013	2014	2015E	2016E
China	$304.69	$1,510.94	$4,193.75	$14,493.75	$31,446.88	$38,621.88	$54,417.19
US				$ 2,400.00	$ 6,600.00		
UK				$ 441.20	$ 1,151.44		

Figure 1.14: Size of P2P in China, US and UK.
(Source: Research Cases of P2P Lending, 2014)

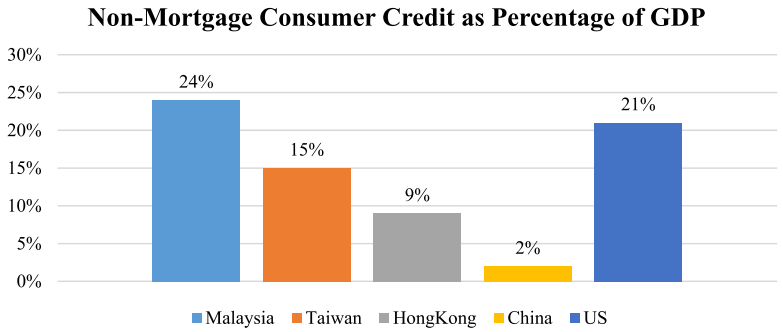


Figure 1.15: Non-mortgage consumer credit as percentage of GDP.
(Source: CreditEase Report, 2014)

overtook that of US and UK from 2013 to 2015. China's P2P market is now estimated to be 5 times larger than the US, and is worth over US$32 billion.

An area which could further enhance the growth of the P2P market in China would be its non-mortgage consumer credit market. According to the CreditEase Report, 2014 (Fig. 1.15), non-mortgage consumer credit accounts for only 2% of the country's GDP. This value is much

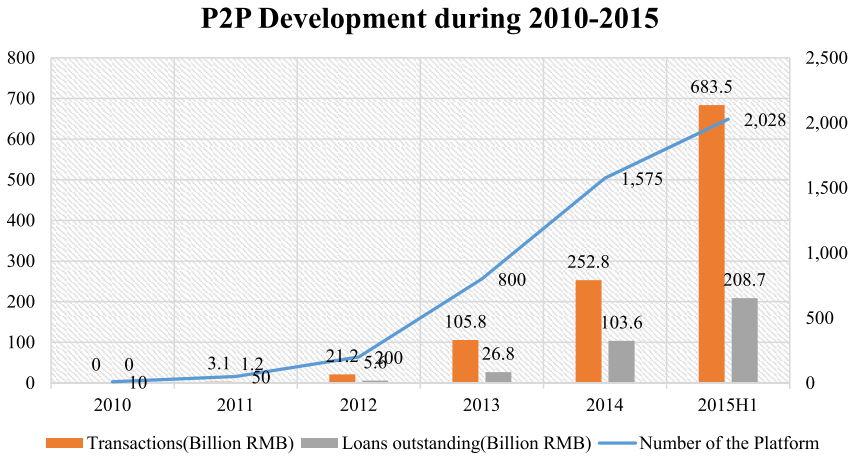


Figure 1.16: P2P development in China from 2010 to 2015.
(Source: CreditEase Report, 2014)

lower as compared to other countries with markets which are more mature. Despite the recent crackdown by the Government and tighter regulation, P2P lending in China still has much room for development if appropriate regulation is implemented. Currently, saving rates in China are high and the deposits rates are low. P2Ps were considered attractive investment until recently. But few lenders were taking on risks after the stock market correction and after news of many of the previously unregulated P2Ps were defaulting. Some platforms were discovered to be scams. A cross-reference with Figs. 1.16 and 1.17 shows that the returns of P2P have been decreasing with the longer duration of loans since 2013. This is because the P2P industry has expanded too rapidly over time and the risk of defaults has been on the rise. After accounting for the higher risk premiums associated with the lenders, the returns are considerably less attractive than a few years ago.

Before the Government intervened in the P2P market in 2016, there were large injections of funds from PE/VC. Referring to Fig. 1.17, the number of investment from PE/VC has increased dramatically from 3 cases in 2012 to 57 in 2015, along with the investment amount of US $5.7 billion. Fig. 1.18 reflects the increasingly high amount of investment into the P2Ps in China in recent years, and Fig. 1.19 lists the top ten PE investments.

The rise of P2P platforms has also brought about an increase in the employment level with the expansion of these P2P start-ups. It can be observed from Figs. 1.20 and 1.21 that within a short span of two years, the number of staff hired in P2P platforms has grew substantially for 14 out of the 17 firms. CreditEase has a total of 361,000 P2P lenders in China and the firm employed 28,000 employees (as shown in Fig. 1.22) as at July 2015.

www.elsevierdirect.com

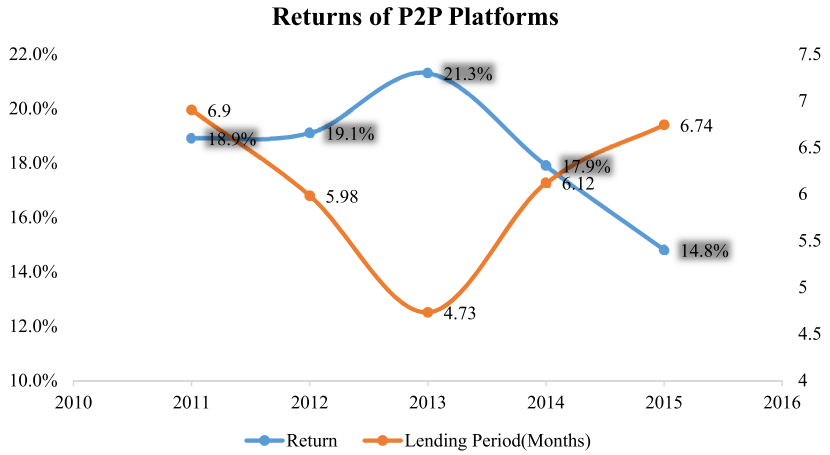


Figure 1.17: Returns of Chinese P2P platforms from 2010 to 2015.
(Source: CreditEase Report, 2014)

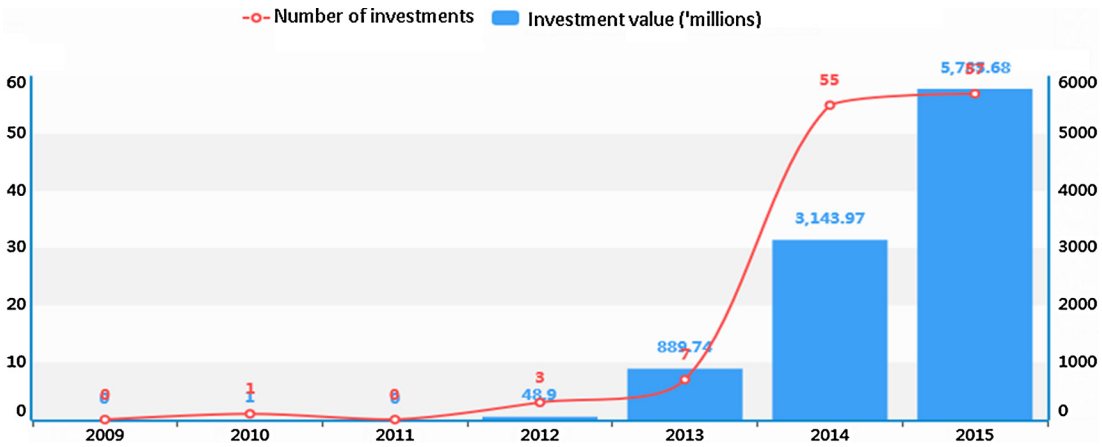


Figure 1.18: Investment into P2P in China.
(Source: CreditEase Report, 2014)

However, there was a problem in the P2P market in China. Problematic platforms started arising and more platforms are facing solvency issues, as seen in Fig. 1.23. As such, when a huge withdrawal of funds is made and if there is insufficient liquidity in the P2P firm, the company owner might flee and abandon the website. Previously, enforcement of governmental rules and regulations on the P2P market was pretty weak. Hence, the Government has revised policies and strengthened the enforcement of policies to address the issue of problematic platforms. The policy titled "An instructional guide on improving the development of Internet Finance" was released in July 2015 to better regulate the P2P industry (Office of Advocacy, 2015). The

Ranking	P2P Firms	Trading Vol ('0000/ week)	Financing Amount (USD Millions)	Investor	APP Index	Estabilshed
1	Weidai	33398.87	16.24	Shanda Group	50.44	2006/3/23
2	Yooli	20776.36	59.26	Hillhouse Capital Group,Morningside Venture Capital,SBCVC	69.12	2012/5/31
3	renrendai	17199.81	133.18	Tencent Collaboration Fund, TBP Capital,Joinhope Assets Management Limited	59.57	2010/4/28
4	touna	15816.11	0.01	GF XINDE INVESTMENT MANAGEMENT	57.98	2013/11/19
5	tuandai.com	15164.88	40.81	Jdcapital	63.41	2010/3/1
6	LuJingSuo	14365.23	485	CDH Investment, China International Capital Corp,Shikumen Capital	67.93	2011/9/29
7	Pai Pai Dai	9037.19	115.56	Sequoia Capital, Lightspeed China Partners, SIG Asia Investments LLP,VMS Investment Group Limited	50.63	2007/8/1
8	Licaifan	4587.15	22.9	Zhong Capital, Magic Stone Investment	68.39	2014/1/13
9	yindou.com	2010	0.98	Legend Star	35.23	2013/9/4
10	xyb100	1970.08	10	eGarden Ventures, SoftBank CI, SIG Asia Investments LLP	42.94	2006/12/29

Figure 1.19: Top 10 huge investment from PE in China.
(Source: Pedata, 2014)

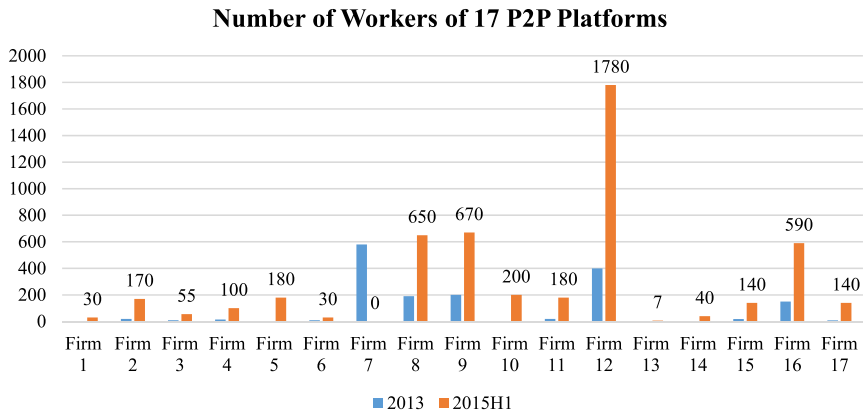


Figure 1.20: Number of workers of 17 P2P platforms.
(Source: China P2P Internet Platform Report, 2015)

policy will serve as a baseline for firms in the industry, and it will be strongly enforced upon. The policy focuses on platform definition, business scope, capital supervision and registered capital limit. The new policy would be able to effectively resolve the problem of problematic P2P platforms illegally running away with clients' investment.

Moving forward, it is believed that the P2P market in China will be of better and assured quality after the exit of problematic firms. It is estimated that interest rates would start declining even further. The new rates would not be as high as before, as the initial high interest rate was

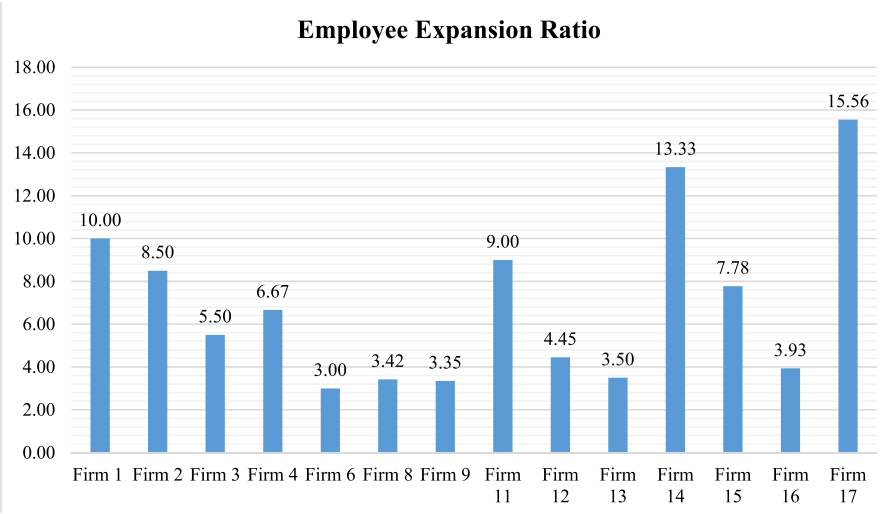


Figure 1.21: Employee expansion ratio.
(Source: China P2P Internet Platform Report, 2015)

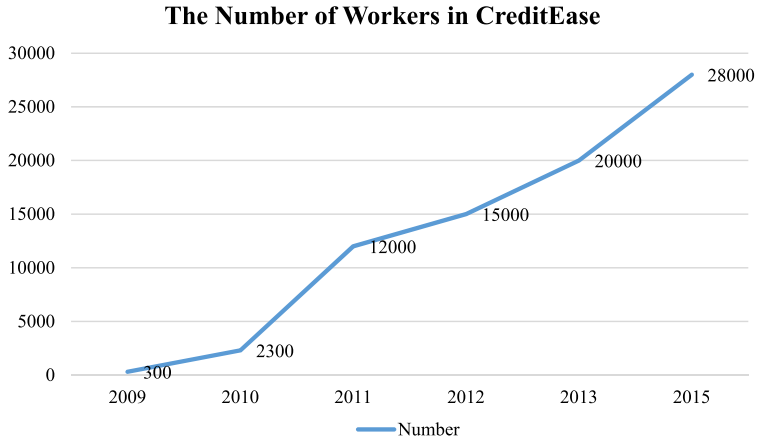


Figure 1.22: Number of workers in CreditEase.
(Source: Askci (中商情报网), 2015)

given to attract investors to help build up its investors' base. As the P2P market matures and stabilizes with time, companies are likely to upgrade their risk management and system capabilities to compete with one another. This would result in better technical systems in the P2P market and barriers to entry will rise.

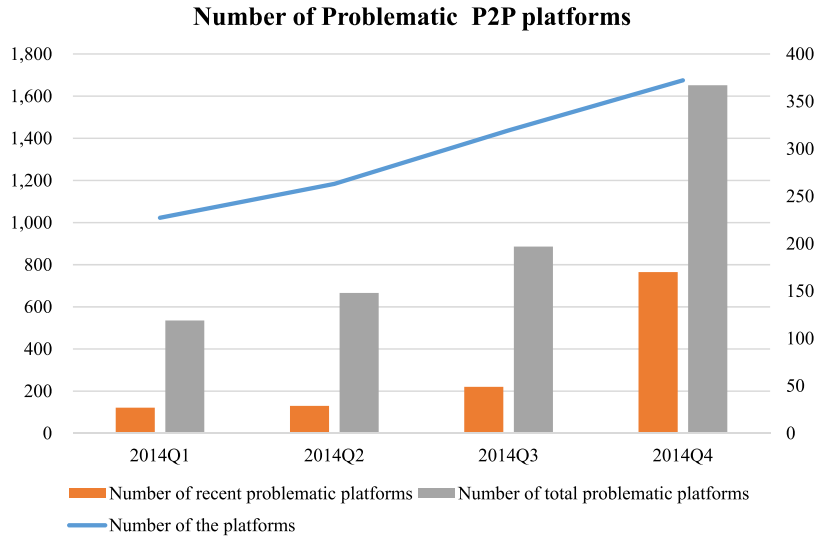


Figure 1.23: Number of problematic platforms.
(Source: Askci (中商情报网), 2015)

Over time, we believe that industry structure will change and more quality assets would be transacted over P2P online platforms. With a diverse market, we might see a trend of smaller P2P start-ups focusing on niche subsectors and strengthening their comparative advantages. Possible cooperation could occur between banks, e-commerce firms and offline business groups. It is very likely to see an extension of P2B services through industrial supply chain management programs in the future as well. Businesses can borrow via online platforms from a diverse group of investors. The use of big data analysis and artificial intelligence can lower default risks, especially for lending portfolios that are geared towards production rather than consumption lending. The trend in P2B will be towards collateralized lending, towards non-speculative lending and towards technology assisted lending.

1.4 Dian Fu Three: Dian Fu in Crowdfunding

Crowdfunding, as the name implies, allows project or ventures to raise funds from a large group of people. Each investor typically invests only a small amount. This is made possible through the widespread use of the Internet and social media. It is a new financing technique to help improve access to capital (Stanberry and Aven, 2014). Crowdfunding is common place in China; this section will discuss the development and trends of crowdfunding in the country.

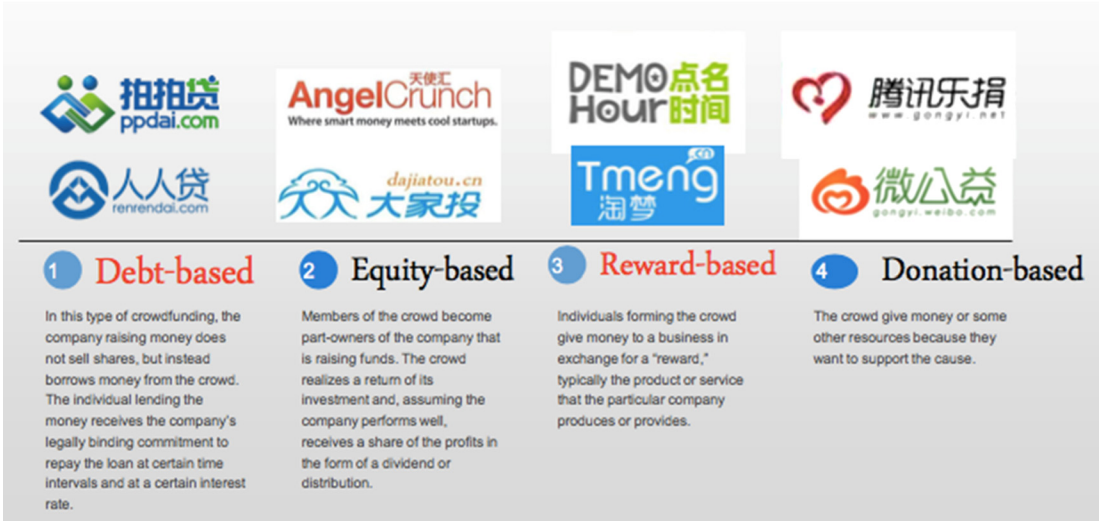


Figure 1.24: Categories of crowdfunding platforms based on type of returns.
(Source: CC Stock《2015年中国众筹行业半年报》, 2015)

The different types of crowdfunding can be categorized into the four main groups as illustrated in Fig. 1.24.

In 2014, AngelCrunch (天使汇) dominated the equity crowdfunding market with 2607 deals amounting to ¥ 769 million (AngelCrunch, 2014). As seen in Fig. 1.25, Beijing leads in the sector of crowdfunding. Crowdfunding platforms are located in all 19 provinces and cities of China (CC Stock, 2015). There are mostly located in the coastal areas with higher levels of economic development. A total of ¥ 4.6 billion was raised during the first half of 2015 (CC Stock, 2015). The distribution of funds raised is shown in Fig. 1.26.

There are various types of crowdfunding platforms. Fig. 1.27 complies a list of prominent platforms and Fig. 1.28 summarizes some statistics of these platforms including the amount of funds successfully raised.

An interesting use of crowdfunding in China that has caught much attention is the funding of Chinese movie productions. The surge in number of movie goers in China has boosted box office figures, making this a promising form of investment. Take, for example, the Chinese film entitled "Monkey King: Hero is Back"; eighty-nine investors invested a total of ¥ 7.8 million. The movie hit a total of ¥ 800 million at the box office within 24 days. Investors saw a return of ¥ 30 million of principal and interest (China Impact Fund of Dao Ventures, 2014). This is a total of 400% total returns on principle. A comparison study between the box office in China and in North America further illustrates the potential of the Chinese market. According

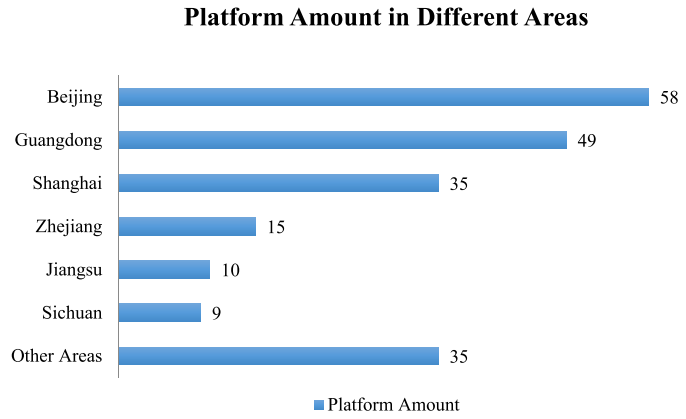


Figure 1.25: The number of platforms in the different areas of China.
(Source: CC Stock《2015年中国众筹行业半年报》, 2015)

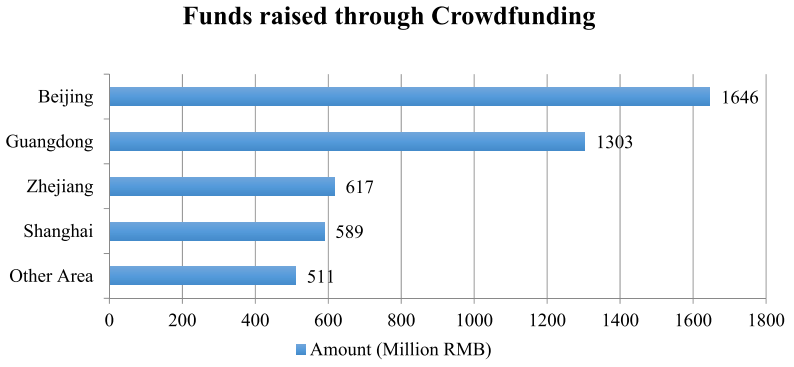


Figure 1.26: Amount raised from the different areas of China.
(Source: CC Stock《2015年中国众筹行业半年报》, 2015)

to PricewaterhouseCoopers Global Entertainment and Media Outlook 2015–2019, box office spending in China is projected to pass US$5 billion in 2015 and is expected to rise at a compounded annual growth rate of 15.5%. It is believed to reach an amount of US$8.8 billion by 2019 (PricewaterhouseCoopers, 2015). Fig. 1.29 compares growth trends in China and North America. It could be observed that China is expanding and performing much better than North America from the growth indexes.

There has been an increasing number of FinTech firms starting up in China and they turning to reward-based crowd-funding (European Commission, 2015). This sector is led by Chinese firms, Jin Dong (京东) and Tao Bao (淘宝), each holding 301 and 544 deals; with proceeds of ¥147 million and ¥63 million respectively (Lee and Teo, 2015). With the rising trend of

www.elsevierdirect.com

Company/Group	Name	Type	Date
Alibaba	Taobao Crowdfunding (淘宝众筹)	Reward-based crowd-funding Donate-based crowd-funding	2013
	Ant Dake (蚂蚁达客)	Equity-based crowd-funding	2015.6
Jingdong	Jingdong Crowdfunding (京东众筹)	Reward-based crowd-funding Donate-based crowd-funding Lending-based crowd-funding	2014
	Dongjia (东家)	Equity-based crowd-funding	2015.3
Ping An Insurance (Group)	Qianhai Crowdfunding (前海众筹)	Equity-based crowd-funding	2015.4
Suning	Suning Crowdfunding (苏宁众筹)	Donate-based crowd-funding Reward-based crowd-funding	2015.4
Baidu	Baidu Crowdfunding (百度众筹)	N/A	Is coming

Figure 1.27: Different types of crowdfunding present in China.
(Source: Ming In Wang (鸣金网), 2015)

Platform	Project(successful)	Money amount(successful) /million RMB	People support(successful)	Total project amount
Jingdong	271	206	801641	1000
Taobao	228	117	1048379	1131
Qingju	128	16	45570	160
Suning	20	7	29373	80
Angelcrunch	310	3000	2386	36954
Renrentou	162	328	8698	165
Yuanshihui	11	15	344	352
Tianshijie	13	40	5296	30
Dajiatou	55	68	700	69

Figure 1.28: Details on the various crowdfunding platforms.
(Source: Ming In Wang (鸣金网), 2015)

advanced technology deeply integrating into our daily lives, we predict that there will be more FinTech startups in crowdfunding.

The size of Chinese market is huge and, as an example, Wanda Group's commercial Wen-ZhuanYiHao pre-REIT (Real Estate Investment Trust, 万达商业地产众筹稳赚一号) ¥5b crowdfunding was completed within three days with the retail portion completed in 1.5 hours.

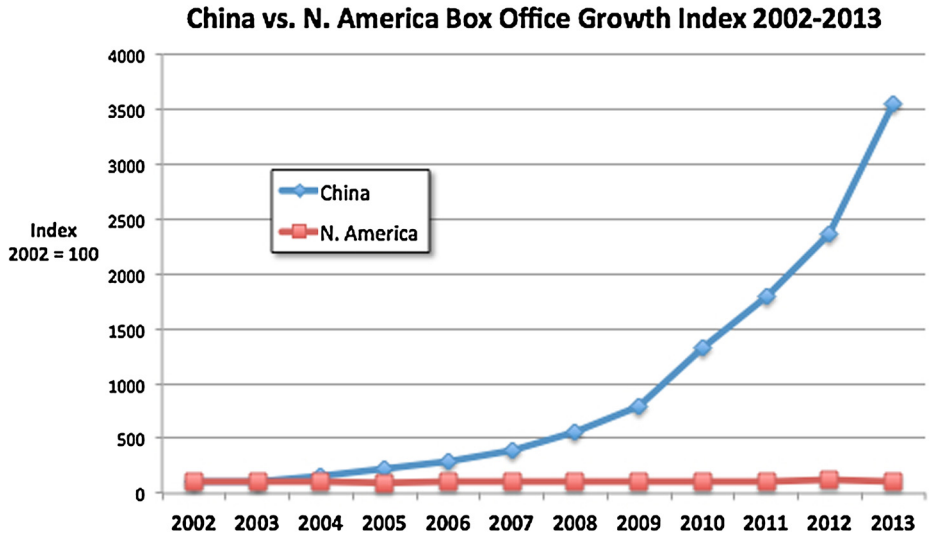


Figure 1.29: China vs North America box office growth index, 2002–2013.
(Source: The Movie Times, 2015)

That demonstrated the size and potential of China's crowdfunding market with a much larger size than a lot of IPOs!

1.5 Dian Fu Four: Dian Fu in the People's Currency

The internationalization of the RMB refers to the process of the RMB becoming a major pricing and settlement currency in international trade, a financial transaction currency and an international reserve currency. RMB was internationalized in Africa in 2000 and since then, Sino-African trade has accounted for an increasing proportion of China's total foreign trade (African Development Bank Group, 2011). This has contributed greatly to Africa's total foreign trade. A rise of 3.82% to 16.13% trading activity was experienced from 2000 to 2012.

Started in 2002, the Chinese government has also allowed (RMB Qualified Foreign Institutional Investors (QFII) to access the A-share market in the attempt to bring in more investment into the China (PricewaterhouseCoopers, 2012). The QFII program was launched by the People's Republic of China in 2002 to allow foreign investors access to its stock exchanges in Shanghai and Shenzhen. Prior to QFII, foreign investors were not able to buy or sell shares on China's stock exchanges because of China's tight capital controls. With the launch of the QFII Program, licensed investors can buy and sell yuan-denominated

www.elsevierdirect.com

RMB Clearing Bank Location	Date	Clearing bank
1. HONG KONG	2003.12	BOC
2. MACAU	2004.09	BOC
3. VIENTIANE	2012.06	ICBC
4. TAIPEI	2012.12	BOC
5. SINGAPORE	2013.02	ICBC
6. PHNOM PENH	2014.03	ICBC
7. LONDON	2014.06	CCB
8. FRANKFURT	2014.06	BOC
9. SEOUL	2014.07	BOCM (BANK OF COMMUNICATIONS)
10. PARIS	2014.09	BOC
11. LUXEMBOURG	2014.09	ICBC
12. QATAR	2014.11	ICBC
13. TORONTO	2014.11	ICBC
14. SYDNEY	2014.11	BOC
15. KUALA LUMPUR	2015.01	BOC
16. BANGKOK	2015.01	ICBC
17. CHILE	2015.05	CCB
18. JOHANNEBURG	2015.07	BOC

Figure 1.30: Internationalization of RMB in the world.
(Source: International Monetary Institute, 2015)

"A" shares. This includes bonds, index futures, warrants, open/closed-end funds, and exchange-traded funds (ETFS). RQFII participants could invest in the same range of investment products as QFIIs. The only key difference between a RQFII participant and a QFII participant is that a RQFII used RMB while a QFII used their foreign home currency to purchase securities. Fig. 1.30 shows the list of countries that RMB has internationalized in.

In 2015, the Chinese Government announced its plan to expand its international trade through its Silk Road Economic Belt (as shown in Fig. 1.31). Also named "One Road, One Belt" (一带一路 or Yi Dai Yi Lu), it is estimated that over 70 projects, with an annual output of US$20 billion, will be carried out along the Silk Road, and helping to create over 200,000 new jobs (Bloomberg Brief, 2015a, 2015b). Currently, the number of box offices in China is increasing and this might suggest a promising idea of investment in Chinese movie made through crowdfunding platforms. A US$40 billion Silk Road Infrastructure Fund would be used to provide funding to carry out infrastructure, resources, industrial cooperation, financial cooperation and other projects related to Yi Dai Yi Lu (Bloomberg Brief, 2015a, 2015b). The

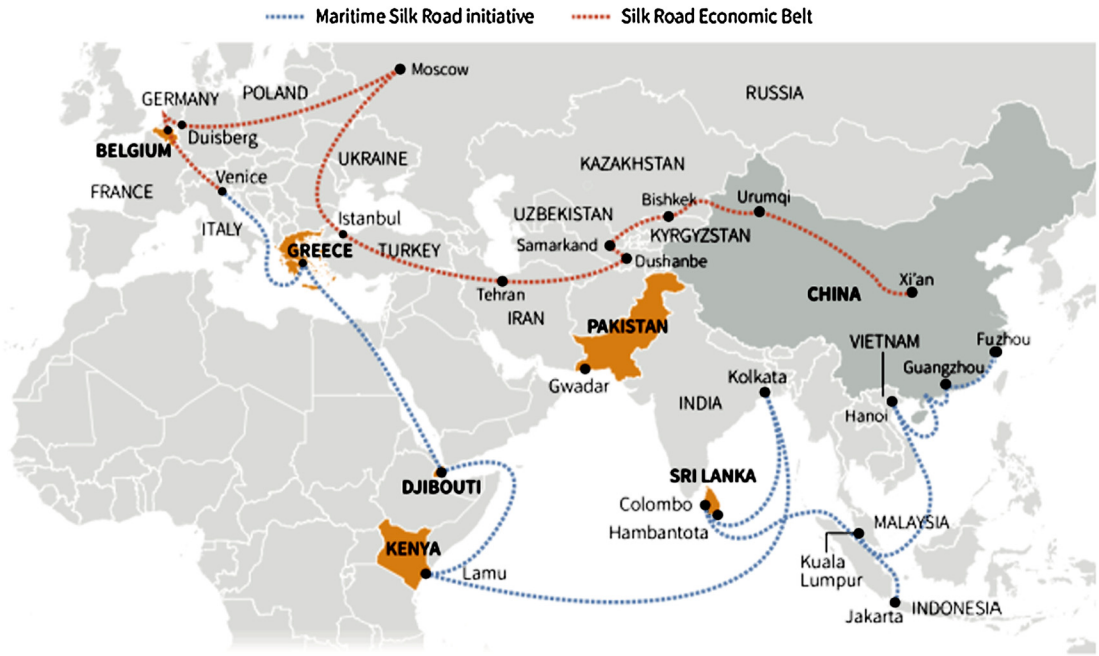


Figure 1.31: Map of the Maritime Silk Road Initiative and the Silk Road Economic Belt.
(Source: The Citizen Daily, 2015)

company that manages the fund, The Silk Road Fund Co. Ltd., is strongly backed by China's foreign exchange reserves, China Investment Corp, Export-Import Bank of China, and China Development Bank. The fund started operation in February 2015 with US$10 billion in capital. It was 65% contributed by China's State Administration of Foreign Exchange, which manages China's Foreign Reserve. The fund is chaired by Jin Qi, the assistant governor of People's Bank of China.[6] With many future plans ahead, the economic outlook of China looks promising. Besides accounting for close to 10.92% component of the SDR (Special Drawing Rights) basket, China is also planning a Blockchain-based electronic RMB. Having an eRMB may increase the transparency of the flow of offshore RMB and allowed for financing, structured products, and other functions that will aid the Chinese enterprises in their quest for offshore investment and operations.

1.6 Dian Fu Five: Dian Fu in Banking

Digital banking is set to overtake physical branches as the preferred access channel for customers to interact with their bank (PricewaterhouseCoopers, 2015). PwC's research found that

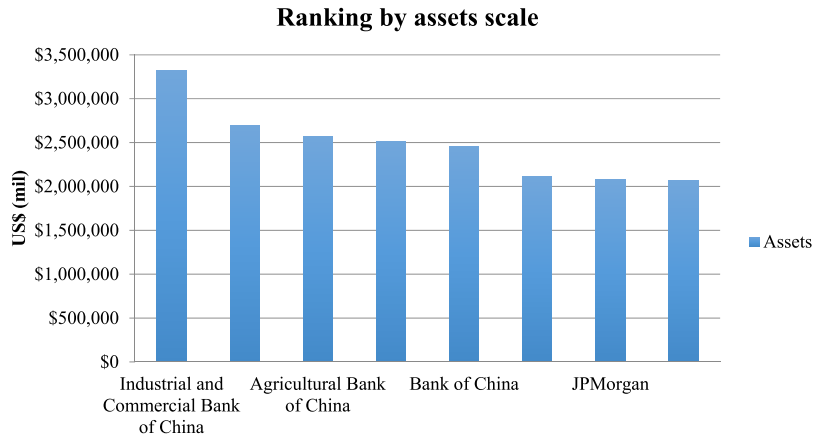


Figure 1.32: Banks ranking by assets scale.
(Source: Accuity, 2015)

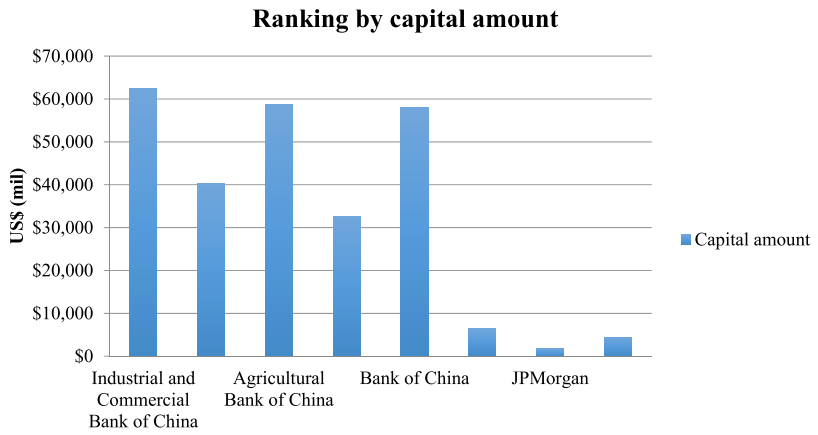


Figure 1.33: Banks ranking by capital amount.
(Source: Accuity, 2015)

customers are willing to pay for digital banking as they believe it can bring convenience and value.

The Industrial and Commercial Bank of China (ICBC) is the biggest bank in the world. As at June 2015, ICBC has the largest asset size of US$3.3 trillion and greatest capital of US$62.5 billion as compared to other megabanks (as shown in Figs. 1.32 and 1.33). The bank has footprints all around the world, over 6 continents and more than 42 countries. It has approximately 17,122 domestic branches and 400 overseas branches. ICBC serves around 456 million individual customers and 5.09 million corporate clients (ICBC Annual Report, 2014).

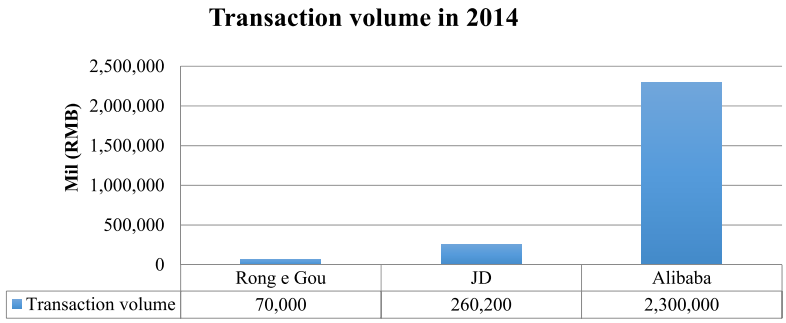


Figure 1.34a: Transaction volume in 2014.
(Source: People China, 2014)

The Internet business is on the rise and banks are being disrupted. However, Chinese banks have their own plans to withstand the challenge. This section will discuss the relative attempt of e-ICBC to respond to the challenges and the development of their Internet finance. There are three platforms, namely the e-Commerce Rong e Gou (融 e 购), instant message platform Rong e Lian (融 e 联), and the direct online platform Rong e Hang (融 e 行). There are also the different product lines, ICBC e-payment and e-charging for transaction banking, ICBC e-investment for investment banking, Yi-Dai as a credit product for personal client, and Wang Dai Tong (网贷通) as a B2B credit product for small and micro businesses. These e-commerce platforms have been well-received by the market and Fig. 1.34a and 1.34b reflect the high transaction volume that was experienced by the various platforms. A record high volume of ¥ 2.3 million transactions was done over at Alibaba (阿里巴巴). In 2014. Alibaba (阿里巴巴) is the largest e-commerce platform in China. From Fig. 1.34a, a significant difference in transaction volume could be observed between Rong e Gou (融 e 购), Jin Dong (JD, 京东), and Alibaba (阿里巴巴). As seen in Fig. 1.34b, in June 2015, Rong e Gou has overtaken JD to be the second largest e-commerce platform in China even though the number of users are fewer than in both Alibaba and JD.

In response to lending to smaller and medium enterprises, various banks have also structured loan and wealth management products to compete with Ant Financial. In the Internet finance sector, three forms of development models are being adopted. They are the independent, cooperation, and diversification models. The independent model refers to banks that operate on their own entity, with no partners involved. Some examples could be seen in Fig. 1.35. Banks could also corporate with partners and some examples are shown in Fig. 1.36. Lastly, banks could also perform diversification whereby a single bank partner with various other firms to produce different streams of products. This could be illustrated by Ping An Bank (平安银行), as shown in Fig. 1.37. Ping An Bank (平安银行) has partnered with multiple partners to create different financial products.

www.elsevierdirect.com

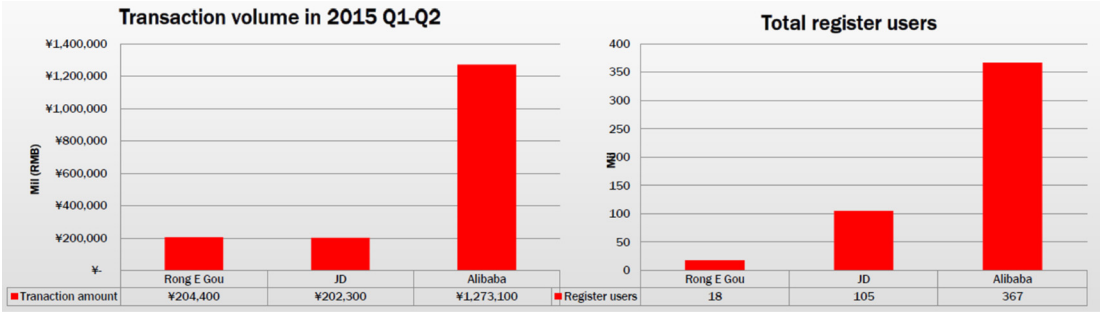


Figure 1.34b: Transaction volume in 2014.

Banks	Partner	Product	Nature of Business	Founded time
Agricultural Bank of China	N/A	Mobile Banking	Mobile App: E-payment, E-business, E-social	Mar-14
China Minsheng Banking	N/A	RuYiBao, DingHuoBao, MinShengJin etc.	Direct banking	Feb-14
Baoshang Bank	N/A	XiaoMa Bank: QianLi Ma, MaBaoBao	Online Wealth management product(bond and Money market fund)	Jun-14
ICBC	N/A	e-ICBC	Internet Finance Platform	Mar-15
Bank of Communications	N/A	HaoShengYi (MobileApp)	Small an Micro Finance "O2O"	May-15

Figure 1.35: Developmental model-independent banks.
(Source: SINA Corporation, 2013)

It is evident that the Internet finance is growing very rapidly in China and people are responding very positively towards it. Many banks are in the process of expanding their e-business sector and increasing the value of their e-commerce platforms. This whole new phenomenon is expected to bring about greater benefits to consumers. Consumers will now have more product choices that are of higher quality to choose from.

1.7 Conclusion

1.7.1 Financial Inclusion and Fintech

With the growth of mobile payment and mobile phone penetration, China has been one of the most successful countries in the world in their financial inclusion programs. Ant

www.elsevierdirect.com

Banks	Partner	Product	Nature of Business	Founded time
Beijing Bank	ING Group	N/A	Internet + Direct Banking (the first one)	Sep-13
Beijing Bank	Tencent	Beijing Yee Tong	Internet + Medical, Third party payment and retail selling	Apr-15
Bank of China	Baidu	N/A	O2O, Data + risk management, clients+ costs, consumer credit services	Jun-16
Industrial and commercial bank	Ant-Financial services	N/A	strategy corporation in payment, financial services, financial inclusion	Jun-15
Huaxia Bank	Webank	"Jielidai"	strategy corporation in resource sharing, credit card, wealth management, interbank business etc.	Feb-15

Figure 1.36: Developmental model-banks with partners.
(Source: SINA Corporation, 2013)

Banks	Partner	Product	Nature of Business	Founded time
Ping An Bank	Webank	<business corporation agreement>	strategy corporation	May-15
	Shopex	"big data credit" platform	Internet funding based on Big data	May-15
	He Bang corporation	N/A	Internet + agriculture service	Jun-15
	GuangQi corporation	photon pay	A new Mobile payment technology– tap to pay, don't need card	Jun-15
	N/A	Orange e startup	support star-up companies	Jun-15
	N/A	Orange Bank: Ding HuoTong, PingAn	Direct banking	Aug-14
	N/A	Orange E net	E-commence	Jun-14

Figure 1.37: Ping An Bank with its partners.
(Source: SINA Corporation, 2013)

www.elsevierdirect.com

Financial has come to dominate the payment industry because of its ability to serve the underserved and unbanked. Acting as a trust agent for buyers and sellers for Alibaba, Alipay has developed into international payment companies with both economies of scale and economies of scope, bringing services such as insurance, lending, crowdfunding, wealth management, credit rating, and monetization of casual jobs such as Daowei (到位) to micro enterprises and individual users. This is all possible because of mobile penetration as the apps play an important part in providing the services online.

1.7.2 Expanding to the ASEAN Region

The five categories of Dian Fu presented in this paper reflect the great potential of the Chinese market and the rise of Chinese finance in this era. Chinese companies are set to dominate the business world, especially digital finance with its advantage in financial inclusion, scalable technology, and innovative low margin-asset light business models. The Internet Plus policy, One Belt One Road strategy, China International Payments Cross Border eRMB strategy, Big Data policy, Supply Chain policy, and Blockchain Development policy will enable China to dominate the old financial world with new business models.

Given that a large number of countries in ASEAN are agriculture-based with sparsely populated areas, China will be able to use its connectivity inclusion policy of high speed rail, balloon and drone WiFi, solar and renewable energy cell phone towers, LiFi and other scalable technologies to connect the underserved and unbanked. Many of these countries will borrow China's experience to connect using both hardware and software manufactured by China, thus alleviating some of the excess capacity and unemployment problems of China. With cheap data plans, China will be able to connect the 600m population with the help of its willing neighbors. Having set the standard of Blockchain with its experiment on smart cities, blockchain will be a key enabler for digital asset ownership for the masses, especially in the low-income high-growth areas. ASEAN with six countries growing at above 5.5% and RMB480.4b, total trade will be the growth areas for both China and ASEAN. It is interesting to see that the national policies of China combined with technology and innovation will disrupt traditional industries not only in China, but will also enable its neighbors to grow with the Middle Kingdom!

Appendix: Acquisitions of Alibaba

Time	Firm Name	Name	Amount (US$ M)
2005-08	中国雅虎	Yahoo China	NA
2006-10	口碑网	KouBei	600
2008-05	phpwind	phpwind	NA
2009-09	万网	WanWang	540
2010-03	星辰急便	Stars Express	4.6
2010-06	Vendio	Vendio	NA
2010-08	易图通	EMG	35
2010-08	Auctiva	Auctiva	NA
2010-10	搜狗	Sogou	15
2010-11	一达通	OneTouch	NA
2011-05	CNZZ	CNZZ	NA
2011-07	美团	MeiTuan	50
2012-11	丁丁网	ddmap	NA
2013-03	虾米网	XiaMi	NA
2013-04	新浪微博	Sina Corp	568
2013-05	高德	AutoNavi	234
2013-03	友盟网	Umeng	80
2013-07	穷游网	Qyer	NA
2013-08	UC优视	UC	NA
2013-09	酷盘	Kanbox	NA
2013-10	天弘基金	Tianhong Asset Management Co	4
2013-10	ShopRunner	ShopRunner	NA
2013-12	日日顺物流	RRS	233
2014-01	中信21世纪	CITIC 21CN	207
2014-02	TutorGroup	TutorGroup	NA
2014-03	文化中国传播集团	ChinaVision Media Group	804
2014-03	TangoMe Inc.	TangoMe Inc.	215
2014-03	银泰商业集团	Intime Retail Group	692

www.elsevierdirect.com

Time	Firm Name	Name	Amount (US$ M)
2014-03	魅族	Meizu	1050
2014-04	恒生电子	Hundsun Technologies Inc.	515
2014-04	华数传媒	Wasu Media Holding	1050
2014-04	优酷土豆	Youku	1080
2014-05	阿斯兰	ASLAN	NA
2014-05	新加坡邮政	Singapore Post Ltd.	223
2014-06	恒大	Evergrande	187
2014-09	石基信息	Shiji Information Technology Co	439
2014	快的	Kuaidi	NA
2014	陌陌	Momo	NA
2014	茵曼	Inman	NA
2015-03	光线传媒	Enlight Media Group	375
2015-06	上海文化广播影视公司	SMG	187
2015-07	魅力惠	Mei.com	100
2015-08	苏宁云商	Suning Appliance Co	4.4

Acknowledgments

Special appreciation to the members of the SKBI Dian Fu Research Team Zhang Han, Chang Su, Chi Ying Ying, Lin-JingXian, and Zoey Phee.

References

Accuity, 2015. Bank Rankings – Top Banks in the World. Retrieved November 23, 2015, from http://www.accuity.com/useful-links/bank-rankings/.

Acutus, 2015. The Chinese Dream: One Belt, One Road. Retrieved November 23, 2015, from http://www.acutus-ca.com/wp-content/uploads/2015/11/The-Chinese-Dream.pdf.

African Development Bank Group, 2011. Annual Report 2011. Retrieved on August 27, 2015, from http://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/AfDB%20Group%20Annual%20Report%202011.pdf.

Askci, 2015. 中商情报网 (2015) Retrieved November 23, 2015, from http://www.askci.com/news/2015/08/03/101936qzad.shtml.

Bloomberg Brief, 2015a. One Belt, One Road. Assessing the Economic Impact of China's New Silk Road. Retrieved on November 23, 2015, from http://www.bloombergbriefs.com/content/uploads/sites/2/2015/07/SC_062615-OBOR.pdf.

Bloomberg Brief, 2015b. One Belt, One Road, Assessing the Economic Impact of China's New Silk Road. Retrieved on August 27, 2015, from http://www.bloombergbriefs.com/content/uploads/sites/2/2015/07/SC_062615-OBOR.pdf.

Business Sohu, 2015. Retrieved on August 27, 2015, from http://mp.weixin.qq.com/s?__biz=MjM5NjUxNDgzMw==&mid=205267509&idx=2&sn=d6efe71bc0a0c0b33ea8eb258355ded3&scene=5#rd.

Career In, 2015. Retrieved on August 13, 2015, from http://mp.weixin.qq.com/s?__biz=MjM5OTkzODQ0Mg==&mid=207435837&idx=5&sn=bfeddf34dc5149d1984c9f8daa0dd0aa&scene=5#rd.

CC Stock, 2015. 《2015 年中国众筹行业半年报》. Retrieved on November 23, 2015, from http://www.ccstock.cn/money/licai/2015-11-20/A1447952840790.html.

Charltons, 2012. China Laws and Regulations for PRC Companies Seeking a Listing on the HKEx. Retrieved November 23, 2015, from http://www.charltonslaw.com/hong-kong-law/china-laws-and-regulations-for-prc-companies-seeking-a-listing-on-hkex/.

Chen, D., Han, C., 2012. A comparative study of online P2P lending in USA and China. Journal of Internet Banking and Commerce 2012. Retrieved November 23, 2015, from http://www.icommercecentral.com/articles/a-comparative-study-of-online-pp-lending-in-the-usa-and-china.pdf.

China Daily, 2015. Retrieved on August 27, 2015 from http://en.citizendaily.net/chinas-belt-and-road-strategy-ignores-indias-concerns/.

China Impact Fund of Dao Ventures, 2014. China Crowdfunding Report. Retrieved on August 27, 2015 from http://www.ied.cn/sites/default/files/CIF%20China%20Crowdfunding%20Report_Final.pdf.

China P2P Internet Platform Report, 2015. Retrieved November 23, 2015, from http://www.askci.com/news/2015/08/03/101936qzad.shtml.

CreditEase Report, 2014. Retrieved on November 23, 2015, from http://english.creditease.cn/pressroom/PressRelease/2014/0421/95.html.

Dahlman, Carl J., Aubert, Jean-Eric, 2001. China and the Knowledge Economy. World Bank Institute Development Studies.

Deloitte, 2014. Art and Finance Report 2014. Retrieved on August 27, 2015, from https://www2.deloitte.com/content/dam/Deloitte/es/Documents/acerca-de-deloitte/Deloitte-ES-Opera_Europa_Deloitte_Art_Finance_Report2014.pdf.

European Commission, 2015. Crowdfunding Explained. Retrieved November 23, 2015, from http://www.investhorizon.eu/resources/documents/3/CrowdfundingExplained_EN.pdf.

ICBC Annual Report, 2014. Retrieved on August 27, 2015, from http://v.icbc.com.cn/userfiles/Resources/ICBCLTD/download/2015/22014AnnualReport_20150421.pdf.

Institute of Chinese Study, 2015. Deconstructing the Shanghai Stock Exchange Crash. Retrieved November 23, 2015, from http://www.icsin.org/uploads/2015/07/16/e025b3de71db00e894353d06c9b6cfdc.pdf.

International Monetary Institute, 2015. RMB Internationalization Report 2015. Retrieved on August 18, 2015, from http://files.clickdimensions.com/golddiscoveryfundcom-avren/files/rmbinternationalizationreport2015forrelease.pdf?_cldee=d2lsbGVtQGNkZnVuZC5jb20%3D&urlid=3.

Johnston, M., Zhang, M., 2015. China's Innovations: Platforms for Partnerships. Retrieved on August 27, 2015 from https://www.asiapacific.ca/sites/default/files/filefield/apfc_report_incubators-pd05.pdf.

Lee, D., Teo, E., 2015. The Game of Dian Fu. Retrieved on August 18, 2015, from http://www.smu.edu.sg/sites/default/files/skbife/pdf/The%20Rise%20of%20Chinese%20Finance%20颠覆.pdf.

Lend Academy, 2013. The World's Largest P2P Lending Company That You Have Never Heard of-. Retrieved November 10, 2016, from http://www.lendacademy.com/the-worlds-largest-p2p-lending-company-that-you-have-never-heard-of/.

Lu, F., 2014. The Real Value of China's Stock Market by Fangzhou Lu, Shanghai Stock Exchange and Shenzhen Stock Exchange. Retrieved October 13, 2015 from http://www.stern.nyu.edu/sites/default/files/assets/documents/Fangzhou%20Lu_Thesis_Honors%202014.pdf.

Ming In Wang, 2015. (鸣金网) (2015). Retrieved November 23, 2015, from http://www.28zhongchou.com/zixun/zhishi/778.html.

Morgan Stanley, 2014. China Internet eCommerce: China's Consumption Growth Engine. Morgan Stanley Blue Paper.

National Bureau of Statistics of China, 2014. Retrieved on August 13, 2015, from http://mp.weixin.qq.com/s?_biz=MzI1MTAxNDE0Ng%3D%3D&mid=211919834&idx=1&sn=87b8dfd794da30c48a6f24e58eb53448&scene=2&from=timeline&isa%20ppinstalled=0#rd.

Office of Advocacy, 2015. Peer-to-Peer Lending: A Financing Alternative for Small Businesses. Retrieved on August 27, 2015, from https://www.sba.gov/sites/default/files/advocacy/Issue-Brief-10-P2P-Lending_0.pdf.

PE Daily, 2015. Retrieved on November 23, 2015 from http://pe.pedaily.cn/201412/20141204374638.shtml.
People China, 2014. Retrieved on November 23, 2015 from http://finance.people.com.cn/money/n/2015/0112/c218900-26369498.html.
PricewaterhouseCoopers, 2015. PricewaterhouseCoopers's Global Entertainment and Media Outlook 2015–2019. Retrieved November 23, 2015, from http://www.pwc.com/gx/en/industries/entertainment-media/outlook/overview.html.
PricewaterhouseCoopers, 2012. Qualified Foreign Institutional Investors (QFII) Brochure. Retrieved November 23, 2015, from https://www.pwc.de/de/kapitalmarktorientierte-unternehmen/assets/fuer-qualified-foreign-institutional-investors-oeffnet-sich-die-tuer-zu-chinas-kapitalmarkt-allmaehlich.pdf.
Qingke Data, 2015. Retrieved on August 27, 2015, from https://qke.github.io.
Research Cases of P2P Lending, 2014. Retrieved on November 23, 2015, from http://www.guancha.cn/economy/2015_01_25_307435.shtml.
SINA Corporation, 2013. Retrieved on November 23, 2015, from http://finance.sina.com.cn/money/bank/ywycp/20130918/141716800000.shtml.
Stanberry and Aven 2014. Crowdfunding and Expansion of Access to Startup Capital.
The Movie Times, 2015. Retrieved on August 18, 2015, from http://www.the-movie-times.com/thrsdir/Yearly.cgi.
Wang, Greiner, Aronson, 2009. The Role of Social Capital in People-to-People Lending Marketplaces. Retrieved on November 23, 2015, from https://www.researchgate.net/publication/221598231_The_Role_of_Social_Capital_in_People-to-People_Lending_Marketplaces.
World Federation of Exchanges – Bloomberg, 2015. Retrieved on November 25, 2015, from http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=117213136.

Notes

1. For an interesting documentary on this episode, watch Crocodile in the Yantze River: The Alibaba Story (http://www.crocodileintheyangtze.com/buynow.html).

2. The Second Board is also called the Growth Enterprise Market. It was started in 2009 by the Shenzhen Stock Exchange to mark the creation of the long-awaited market for venture businesses.

3. The launch of the SME Board was a major step towards the establishment of a multi-tier capital market system and paved the way for a second board market.

4. However, economists estimated this figure should be reduced by 25% as the figure included the component on those local Government financial vehicles (LGFVs). With the necessary adjustments made, the debt figure would be approximately US$11.4 trillion instead.

5. These four companies are commonly referred to as BATS.

6. Jin Qi said in March 2015 that the fund will be invested in projects with reasonable mid- and long-term returns; it is not an old agency that does not consider returns. She added that the Silk Road Fund will not be the sole financer of projects; rather it will seek cooperation with other financial institutions in the investment of future projects (Silk Road Fund, 2015).

CHAPTER 2

Balancing Innovation and Risks in Digital Financial Inclusion—Experiences of Ant Financial Services Group

Tao Sun[#]

Contents

2.1 Introduction 37

2.2 Definition 38

2.2.1 Digital Financial Inclusion 39

2.3 Experiences of Ant Financial 40

2.3.1 Financial Innovation at Ant Financial 40

2.3.2 Risk Management at Ant Financial 42

References 43

2.1 Introduction

There has been a growing consensus in promoting financial inclusion around the world in recent years, when the authorities in advanced and emerging economies have undertaken comprehensive measures to dodge the challenge of the expanding income inequality and mediocre growth.

A successful model of financial inclusion could contribute to improving resource allocation, raising consumption, and lifting living standard. However, global experiences show that financial inclusion could also bring up risks that make it be unsustainable.

Against this background, digital financial inclusion emerges as a dynamic force by striking a balance between innovations and risk management. Many national and global efforts have also been made to promote digital financial inclusion.

Senior Director, Ant Financial Services Group.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00002-4
Copyright © 2018 Elsevier Inc. All rights reserved.

Ant Financial Services Group (referred to as Ant Financial below), a leading digital inclusive financial firm in China, has been promoting digital financial inclusion and has demonstrated strong capabilities in striking a balance between innovation and risk management. As a reflection of these efforts, Ant Financial has gradually contributed to improving resource allocation, raising consumption, and lifting living standard. Therefore, a series of questions naturally arise:

- What financial products have been initiated by Ant Financial?
- How does Ant Financial strike a balance between financial innovation and risk management?
- What policies can potentially promote financial inclusion?

This chapter takes Ant Financial as an example of promoting digital financial inclusion. It starts with a brief overview of definition of financial inclusion and digital financial inclusion. It then introduces the experiences of Ant Financial in promoting digital financial inclusion by enhancing innovation. Finally, it summarizes the measures/approaches to balance innovation and risks.

2.2 Definition

Put simply, financial inclusion is the access to and use of formal financial services by households and firms. It is seen by policymakers as a way to improve people's livelihoods, reduce poverty, and advance economic development (IMF, 2015). Financial inclusion may also be interpreted as having access to and using the type of financial services that meet the user's needs (BIS, 2015).

There are a couple of issues on critical areas underpinning digital financial inclusion. On the one hand, financial inclusion can introduce potential benefits to the safety, soundness and integrity of the financial system. On the other hand, it can also bring potential risks to providers and customers alike, and entail the transfer of risks to new players. Research at the IMF suggests that financial inclusion significantly increases macroeconomic growth, although broadening access to credit can compromise macrofinancial stability when combined with poor quality of banking supervision (IMF, 2015).

While having made some progress in financial inclusion in the past couple of decades, the world still faces challenges in achieving a sustainable, affordable, and comprehensive financial inclusion. Globally, it is not the largest corporates and the wealthiest individuals that are lacking financial support, but SMEs and individuals that have been demanding more financing. In developing countries, two billion people have no bank accounts, and only ten percent of population have credit cards. Among those people with financing needs, only 21% can get

loans from financial institutions. Undoubtedly, it remains a global challenge to provide financial services to these underserved/unserved groups.

In this context, digital financial inclusion can potentially play a vital role, and today's momentum can be amplified to unlock transformational levels of financing for sustainable financial inclusion. In this regard, financial system itself can also be gradually reshaped to mobilize sufficient capital for sustainable development.

2.2.1 Digital Financial Inclusion

'Digital' financial inclusion involves using digital means to reach financially excluded and underserved populations with a range of formal financial services suited to their needs, delivered responsibly at a cost affordable to the customer and sustainable for the providers (BIS, 2016).

The emergence of digital financial inclusion can potentially solve the problems that traditional approach has long been hard to address. Traditional approach doesn't work well enough to provide a sustainable financial inclusion. For instance, Grameen Bank in Bangladesh has provided total loans of $17.4 billion in the past 29 years. While being a great achievement in the financial inclusion world, the potential of financial inclusion has been far from reached through this approach.

Recent experiences in countries, such as China and India, demonstrated the great potential of digital financial inclusion. Digital financial inclusion works better for three reasons: mobile technology makes inclusiveness more accessible; cloud computing reduces the costs of financial inclusion; big data technology helps assess risk.

Because of the weaknesses of traditional approach and the comparative advantages of the digital one, digital financial inclusion gained both national and global endorsement. At the national level, Chinese authorities, for instance, adopted digital financial inclusion as a national strategy. In 2016, the State Council issued "Development plan for promoting financial inclusion (2016–2020)". This plan elevates financial inclusion to the level of national strategy and emphasizes the promotion of financial inclusion with innovative financial products and services.

At the global level, on July 24, G20 Finance Ministers and Central Bank Governors Meeting issued "G20 High-level Principles for Digital Financial Inclusion" to encourage adoption of these principles for broader coverage of financial inclusion planning, in particular with digital financial inclusion. Therefore, digital technology has been taken as a breakthrough point for financial inclusion.

www.elsevierdirect.com



Figure 2.1: Businesses overview of Ant Financial.

2.3 Experiences of Ant Financial

In 2004, Alibaba established Alipay to address the issue of trust between buyers and sellers online. Alipay became Small and Micro Financial Services Company in 2011. Small and Micro Financial Services Company was rebranded as Ant Financial Services Group in October 2014. Alibaba does not have any ownership interest in Alipay. The two companies are related companies. Ant Financial has made great efforts in promoting financial inclusion by striking a balance between financial innovation and risk management.

2.3.1 Financial Innovation at Ant Financial

Ant Financial is dedicated to using technology to provide inclusive financial services to individuals as well as small and micro enterprises. Ant Financial believes that financial services should be simple, low-cost and accessible to the many, not the few. And the technologies, such as cloud computing and Big Data analytics, make us uniquely placed to achieve this. Ant Financial has developed a wide range of products and services, covering payments, loans, insurance, and wealth management, focusing on the financial needs of small businesses and individuals in an effort to promote digital financial inclusion.

Innovative technology and extensive data analysis underpin everything we do. The cloud and big data power our rigorous credit, security and risk control processes, and allow us to tailor our products to customers' individual needs and operate in the safest, most efficient and cost-effective manner. Technologies make financial inclusion sustainable with more choices, and make transparency and risk management more reachable and reliable (Fig. 2.1).

Specifically, Ant Financial has developed a range of products meeting the diverse financial services needs of our customers. With all our products, our aim is to simplify and democratize the process for our customers, giving access to financial services to the many, not the few.

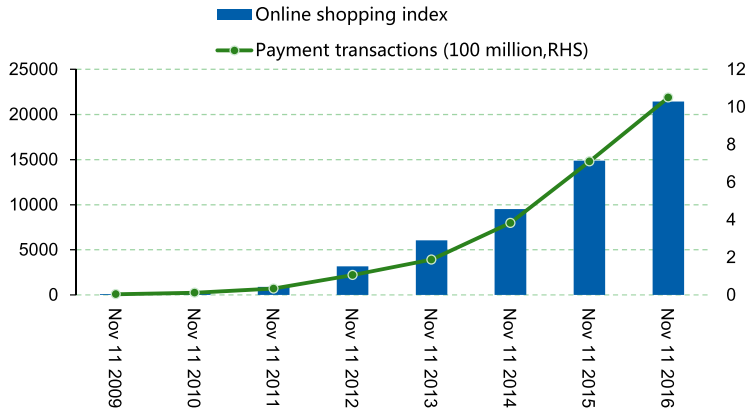


Figure 2.2: Online shopping and payment transactions.

- Alipay. Operated by Ant Financial, Alipay is the world's leading mobile and online payment platform. Launched in 2004, Alipay currently has over 450 million active users and more than 200 domestic financial institution partners. During the 2016 11.11 Global Shopping Festival, China's equivalent of Cyber Monday, Alipay processed RMB 120.7 billion worth of transactions from Alibaba's marketplaces and 1.05 billion transactions with its peak transaction handling volume reaching 120,000 per second (Fig. 2.2). Alipay has evolved from a digital wallet to a lifestyle enabler. Users can hail a taxi, book a hotel, buy movie tickets, pay utility bills, make doctors' appointments or transfer money to each other directly from various modules within the app and purchase wealth management products such as Yu'e Bao. In addition to online payments, Alipay is expanding to in-store offline payments both inside and outside of China. Over 2,000,000 brick-and-mortar merchants now accept Alipay as a payment method across China. As of June 2016, Alipay was supported in 70 overseas markets, with in-store payments covering more than 80,000 retail stores, and tax reimbursement via Alipay is supported in 24 countries and regions, including South Korea, Germany and France. Alipay works with over 40 overseas financial institutions and payment solution providers to enable cross-border payments for Chinese traveling overseas and overseas customers who purchase products from Chinese e-commerce sites. Alipay supports the settlement of 18 currencies.
- Ant Fortune. A comprehensive wealth management app that allows users to manage their finances in one place, Ant Fortune was launched in August 2015. It offers Yu'e Bao and other wealth management products, as well as allowing users to check stock movements in-app.
  - Yu'e Bao. Yu'e Bao is an online wealth management product that offers users higher returns on their current account balance, no matter how tiny their deposit. Jointly launched with China's Tianhong Asset Management in 2013, Yu'e Bao is one of the

www.elsevierdirect.com

largest money market fund in the world and the largest in China by volume. It currently has more than RMB 800 billion in assets under management and 300 million users as of July 2016.

- Koubei. Koubei is a joint venture established in June 2015 by Alibaba Group and Ant Financial Services Group, each of which invested RMB 3 billion as well as user traffic diverted from other synergetic products and services such as Alipay. Koubei allows users to look for local merchants, place orders, conduct payments and write reviews.
- MYbank and Ant Micro Loan. MYbank is a private online bank established on June 25, 2015. It is the first bank to run 'on the cloud'. Prior to the establishment of MYbank, Ant Micro Loan offered small and micro-loans to small and micro enterprises. As of June 2016, Ant Micro Loan and MYbank had provided micro-loans to over 4.11 million small and micro enterprises and entrepreneurs totaling over RMB 740.1 billion.
- Zhima Credit. Based on big data technology, Zhima Credit is an independent organization within Ant Financial offering credit filing and scoring services for individuals, and plans to expand its services to cover enterprises. It was among the first institutions in China to receive an individual credit services license. Zhima Credit is widely used by consumer finance companies, travel agents, hotels, vehicle leasing companies and even online dating sites. Users with a higher Zhima Credit score can book a hotel or hire a public bicycle without a deposit. Building a reliable credit scoring system is a central part of Ant Financial's overall strategy, as credit is the basis for various financial products such as loans and insurance.
- Ant Credit Pay: Ant Credit Pay grants consumer credit for individual users to shop and defer repayment until the following month. It extends credit lines based on a series of indices such as users' consumption frequency and payment habits. Users can shop with their Ant Check Later credit at more than 40 online shopping platforms, including Tmall, Taobao and Amazon.com.
- Insurance products: Ant works with insurance companies to design and provide innovative consumer insurance products like Damage-during-shipping Insurance and Return Insurance, which covers buyers' shipping costs when they wish to return their purchases. Each user has a customized and floating premium for this product, calculated with the help of AI and big data.

2.3.2 Risk Management at Ant Financial

Ant Financial makes great efforts in managing two major types of risks.

- Technology risks. Technology risks arise with the wide use of technology in all sectors in the world, thus it is no wonder a high-tech company such as Ant Financial paid much attention to this type of risk. Ant Financial strengthens systemic stability, reliability and

resilience. Ant Financial sets up unified account registration and monitoring system to prevent fraud risk. Moreover, Ant Financial invests heavily in R&D on cloud computing and big data. These efforts have elevated Ant Financial to become one of the global leaders in financial technology.

- Financial risks. Ant Financial endeavors to establish a sound risk management system to manage credit, liquidity, and market risks. First, empowering other market players with internet platform. This business model can help reduce the reliance on asset expansion, thus lessening risk exposures. Second, making full use of big data and technology to meet customers' needs, and in return, the growing numbers of users greatly improve analytical and risk-assessment capabilities. Third, taking advantage of scenarios (e.g., online shopping). Ant Financial's financial service is closely linked to daily life. The combination of scenarios and digital finance provides financial support to consumption, better serves the real economy, and improves risk management. Fourth, establishing independent risk management framework. Ant Financial sets up firewall to address the potential risks associated with different businesses. Fifth, establishing and improving contingent risk management system to deal with potential sudden external or internal shocks. Sixth, complying with regulatory and supervisory rules and guidance. In sum, these features and advantages help Ant Financial establish a risk-mitigating mechanism arising from its business model, technology, and scenarios, thus greatly strengthening the risk management.

Looking forward, Ant Financial will continue its efforts in promoting digital financial inclusion by striking a balance between financial innovation and risk management.

References

BIS, September 2015. Payment aspects of financial inclusion.

BIS, September 2016. Guidance on the application of the Core Principles for Effective Banking Supervision to the regulation and supervision of institutions relevant to financial inclusion.

IMF, September 2015. SDN/15/17, Financial Inclusion: Can It Meet Multiple Macroeconomic Goals?

CHAPTER 3

Regulating FinTech in China: From Permissive to Balanced

Weihuan Zhou, Douglas W. Arner, Ross P. Buckley

Contents

3.1 Introduction 45

3.2 The Evolution of Digital Financial Services in China 46

3.2.1 Evolution of Traditional DFS 47

3.2.2 Evolution of Non-traditional DFS 48

3.3 Regulation of Digital Financial Services in China 51

3.3.1 DFS Regulation Before 2015 52

3.3.2 DFS Regulation After 2015 54

3.4 Conclusion 57

Notes 58

3.1 Introduction

This chapter explores the evolution of FinTech and its regulation in China.[1] The growth of digital financial services ("DFS") in China in the past decade has been phenomenal. China is now one of the world's largest DFS markets and among the most active of regulators of digital finance. Many factors have contributed to this rapid development, including technological innovation, rapidly increasing use of digital devices and changing consumer behavior, explosive growth of DFS providers, and the policy objective of the Chinese government to enhance financial inclusion via digital finance to support growth and encourage greater innovation. The expansion of financial inclusion for underserved segments, ranging from rural areas to the urban poor to (perhaps most importantly) non-state small and medium sized enterprises ("SMEs"), has been one of the key elements of China's financial sector reforms which in turn have been an integral element of China's overall economic reform and innovation

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00003-6
Copyright © 2018 Elsevier Inc. All rights reserved.

strategies. Another driving force behind the DFS boom in China concerns financial repression due to China's strict control of interest rates of financial institutions since the commencement of its economic reforms with an aim of reducing loan costs of state-owned enterprises ("SOEs") and promoting investment.[2] The interest rates restrictions created difficulties for private firms to obtain loans from banks due to the shortage of deposits from households.[3] This led to strong demands of private firms for other sources of finance and consumers for other channels of investment. The mismatch between these demands and the inadequate supply by traditional financial institutions has provided a fertile ground for the growth of digital finance.[4]

The rapid development of DFS has created various challenges for governments including Chinese regulators. The most imminent challenge has been the need for balanced regulatory frameworks, which allow for the sustainable development of DFS while providing necessary oversight and supervision to ensure financial stability, the protection of consumers and efficient competition in the financial market, and the prohibition of money laundering and other illegal activities.[5] While the Chinese government has been aware of the risks associated with DFS and the need for regulation for almost a decade, the regulatory work has progressed slowly to leave room for the growth of DFS. As these risks become widespread, the Chinese government is now dedicated to establishing a regulatory framework to oversee and supervise DFS so as to ensure its healthy growth. With the release of a new policy framework in July 2015, the Chinese government is seeking to implement a strategically designed framework to balance the sometimes-competing objectives of innovation, growth and financial stability.

3.2 The Evolution of Digital Financial Services in China

In China, DFS developed much later than elsewhere, with major development only beginning in the late 1990s as the financial services sector modernized and developed in the context of the overall process of economic liberalization. Likewise, more recent developments in digital finance (such as Internet payment services and peer-to-peer ("P2P") lending) began to emerge only in the middle of the last decade. Innovations in DFS in China beyond Internet banking and electronic payments are an even more recent phenomenon, dating only from the beginning of this decade. Nevertheless, in many ways, China is experiencing a "last mover" advantage in the context of DFS and now appears to be developing more rapidly than most other jurisdictions.

3.2.1 Evolution of Traditional DFS

Conventional financial institutions, which remain the dominant players in China's financial market, have been active in creating DFS platforms. Some typical examples are set out below.

China has been at the forefront of the development of the ATM market since the introduction of its first ATM by the Bank of China ("BOC") in 1987.[6] For the last decade, in response to the policy directive to enhance financial inclusion, Chinese banks have endeavored to increase the number of banking facilities including ATMs especially in rural areas.[7] In 2013, China became the world's largest ATM market with 520,000 ATMs.[8] While the number of ATMs had soared to 840,800 units by the end of September 2015, there remains a huge demand in the market especially in the rural areas and urban communities and hence a large market potential for continuous growth.[9] In addition, China has focused on the development of advanced technology for ATMs. In May 2015, China launched the world's first facial recognition ATM which includes high-tech functions such as counterfeit bill recognition and high-speed bank note handling.[10]

Internet banking was introduced in China by the BOC in 1996, and was quickly adopted by the other major state-owned and privately-owned banks between 1997 and 2002.[11] Since 2002, the number of Internet banking users has increased rapidly.[12] By 2012, personal and corporate Internet banking transactions had replaced more than 50 percent of over-the-counter transactions in China, with a replacement rate higher than 85 percent at some banks.[13] In 2014, China Minsheng Bank, the largest privately-owned commercial bank in China, launched its Direct Banking platform to move all of its standardized bank products and transactions online.[14] Minsheng Bank's entry into Direct Banking was quickly followed by the state-owned banks and other jointly-owned banks.[15] By the end of 2014, there had been a significant increase in both the number of personal Internet banking users to 909 million (i.e. an annual increase of 16.5 percent) and the value of Internet transactions totaling 60.85 billion (i.e. an annual increase of 22 percent).[16] This signaled a historic move of China's major banks into the digital finance era such that, predictions are now being made that "direct banks will take more than 10% market share of the retail banking industry (in China) by 2020".[17]

In e-payments (such as online and mobile payments), China was a late mover with its nationwide interbank network only being established in 2002.[18] However, the development of e-payments in China has been phenomenal since 2006 when the People's Bank of China ("PBOC"), China's central bank, rolled out the Bulk Electronic Payment System to the whole country.[19] For example, in 2012, major Chinese commercial banks "saw more than 100 percent growth in mobile banking users … and more than 300 percent growth in mobile transaction value."[20] The value and volume of online payments reached RMB 1060.78 trillion and 23.674 billion respectively by 2013, representing an annual increase of 28.89 percent

and 23.06 percent respectively.[21] In 2014, the increases were even more rapid with a total of RMB 8.41 trillion mobile payment transactions (a year-on-year ("y-o-y") increase of 655.51 percent), RMB 1376.02 trillion online payment transactions by banking institutions (a y-o-y increase of 29.72 percent), and RMB 16.21 trillion online payment transactions by payment institutions (a y-o-y increase of 75.5 percent).[22] This trend continued in 2015; for example, the y-o-y increase in the Internet payment business of the PBOC alone reached approximately 81% in volume and 56% in value.[23]

3.2.2 Evolution of Non-traditional DFS

Since 2013, the explosive growth in numbers and scale of non-traditional DFS start-ups has begun to reshape China's financial system.[24] Riding the wave of the increasing adoption of new technologies,[25] a number of major digital finance providers have propelled the development of DFS in China.

The pioneer and leading non-traditional DFS provider in China is the Alibaba Group. As the world's largest e-commerce company, the group has developed many influential digital finance products.[26] The most significant are:

- Alipay, Alibaba's third-party online payment platform launched in December 2004, is the largest and most popular online payment service in China with "more than 300 million registered users in China (and 17 million overseas)" by October 2014.[27] It "handles more than 80 million transactions daily" and had settled 42.3 billion payments by December 2014.[28] Since the same year, Alibaba commenced to implement its global strategy by expanding Alipay to overseas markets such as Australia,[29] the US,[30] and the EU,[31] and by creating mobile applications for payments by both Chinese and foreign consumers in cross-border transactions.[32] By the end of 2015, Alipay had secured 400 million registered users and a share of approximately 70% in China's mobile payment market.[33]
- Alipay introduced Yu'e Bao and its associated mobile application "Alipay Wallet" in June 2013. Yu'e Bao is essentially an online money market fund in which Alipay customers can deposit money left in their Alipay accounts and earn interest at rates generally much higher than those offered by banks.[34] Yu'e Bao does not require minimum deposits and allows withdrawal at any time.[35] In addition, as "up to 90 percent of Yu'e Bao funds are invested in interbank deposits at 29 large banks, including the big state-owned ones," investment in Yu'e Bao is secure.[36] With these advantages compared to conventional financial products, Yu'e Bao has quickly become China's largest online money market fund[37] and the fourth largest worldwide.[38] After only one year, Yu'e Bao had 100 million investors and RMB 570 billion (or more than $90 billion) assets under management.[39] By the end of 2015, Yu'e Bao had total assets of RMB 620.7 billion and 260 million users.[40]

- AliFinance, one of the pilot financial products launched by Alibaba in 2010, provides micro-loans to vendors registered on Alibaba and TaoBao platforms.[41] This product is aimed at serving SMEs and sole proprietors which have difficulties in obtaining loans from banks. The product allows all transactions to be done online and provides flexible repayment terms. While individual loan amounts are small, the aggregate scale of AliFinance loans is not insignificant given the large number of registered users with Alibaba and TaoBao. For example, it has been reported that by October 2013 AliFinance had "409,444 borrowers spanning the country with an outstanding portfolio of RMB 105 billion ($17.2 billion)."[42] Although AliFinance's market share remains marginal,[43] it is a successful example of digital lending targeting underbanked customers and has continued to grow. More recently, AliFinance appears to have been replaced by Ant Credit, a new digital finance product of Alibaba aimed at providing micro loans to SMEs and individuals. Partnering with the International Finance Corporation, a member of the World Bank Group, Ant Credit launched the "first Internet-based gender-finance program in China" on 27 January 2015 committing to "expand financing for women entrepreneurs."[44]
- In late 2014, Alibaba restructured its major digital finance businesses such as Ant Credit, Alipay, Ali Wallet, and Yu'e Bao by placing all of the businesses under Ant Financial Services Group ("Ant Financial") which became Alibaba's key digital finance provider.[45] With the consolidated businesses, Ant Financial aims to bring finance to SMEs, individuals and other underserved segments via Internet-based solutions and technology, and to work with other financial institutions "to create a new financial ecosystem" in China.[46] For example, via its digital finance platforms, Ant Financial has successfully expanded digital financial inclusion in underdeveloped rural areas and has committed to continue to do so by building more digital finance infrastructure and channels in these areas.[47] In November 2015, Ant Financial launched "ANTSDAQ", one of the three online equity crowdfunding platforms approved by Chinese authorities.[48] In April 2016, Ant Financial successfully "raised a record $4.5 billion from private investors, valuing the company at almost $60 billion and moving it a step closer to launching a hotly anticipated initial public offering."[49]
- In June 2015, Alibaba opened its Internet bank called MYbank to offer loans of up to RMB 5 million (or $800,000) to SMEs.[50] MYbank was one of the private banks approved by the Chinese government in 2014; the first approved was Tencent's WeBank (which will be considered below). In its first eight months of operation up to March 2016, MYbank had served over 800,000 SMEs with a total credit value of RMB 45 billion and 40,000-50,000 micro-loans on a daily basis.[51]

Alibaba's stunning success in DFS has stimulated other Internet giants and conventional financial institutions in China to rush into the digital financial market by offering similar digital financial products.

For example, Tencent, one of China's oldest and largest Internet social-networking and entertainment companies, currently has more than 1.5 billion users registered with its massively popular messaging products QQ and WeChat.[52] Listed on the Hong Kong Stock Exchange since 2004, Tencent's market value reached $206 billion in April 2015, exceeding that of Oracle ($190 billion), Amazon ($178 billion) and IBM ($161 billion).[53] Tenpay, Tencent's online payment product providing B2B, B2C and C2C payment services, is China's second largest online payment platform after Alipay.[54] During China's 2014 Spring Festival, Tencent launched another innovative online product named "Red Envelope", tailored to the Festival traditions. It allows customers to give lucky money or red packets to family members and close friends via WeChat.[55] Two days after its launch, the promotion attracted more than 5 million users exchanging over 20 million envelopes.[56] The digital "Red Envelope" carried on its success to the 2015 Spring Festival witnessing the exchange of 1 billion virtual red envelopes on New Year's Eve and trumping Alipay in the "red envelope war".[57] The success of "Red Envelope" has made Tencent a formidable competitor in China's digital payment market. As the giving of red envelope requires users to link their bank accounts to their WeChat accounts, the product creates "the basis for [Tencent's] further financial applications".[58] For example, in January 2014, Tencent, following in the footsteps of Alibaba, introduced a "Wealth" function into WeChat allowing users to store savings in the investment fund without minimum deposit requirements and to earn an annual interest rate of 6.435 percent.[59] In January 2015, Tencent launched China's first Internet-based bank "WeBank" to serve small-scale borrowers with limited access to loans from state-owned banks.[60] In September 2015, Tencent rolled out to its hundreds of millions of users a facility that enables applying for a micro loan up to RMB 200,000 (about $31,350) directly from "Weilidai", a new loan feature of WeChat, which is to be operated by WeBank.[61] By January 2016, WeBank was valued at around $5.5 billion after successfully raising some $450 million.[62]

Another example is Baidu, one of China's most famous web services companies that operates China's largest Internet search engine.[63] In October 2013, Baidu launched its own online wealth management product called "Baifa".[64] Similarly to Alibaba's Yu'e Bao and Tencent's "Wealth", Baifa provides a personal investment platform which allows customers to "make a minimum investment of RMB 1 (about $0.16) and ... [earn] annual interest rates of up to eight percent" higher than the interest rates offered by Yu'e Bao and "Wealth".[65] While less popular than Yu'e Bao and WeChat, Baifa "reportedly raised USD 165 million from 120,000 customers on the day it launched".[66] In addition, Baidu has its own personal loan platform called Baidu Finance which allows customers to "borrow up to ten times their monthly income" with a flexible repayment term up to 3 years.[67] Loan applications and approvals are all processed online within as quickly as 5 minutes.[68] In 2014, Baidu launched another online investment fund called "Baifa Youxi" or "Baifa Me" which "lets users crowd-invest in upcoming movies and television shows" and offers an expected interest rate of 8 percent.[69] Most

recently, Baidu partnered with Citic Bank to launch Baixin Bank – China's first online bank established by a joint venture between a major Internet company and a traditional bank – aiming to leverage the expertise and strengths of the partners including CITIC Group's massive assets and operations in China and Baidu's hundreds of millions users.[70]

In addition to the Internet or e-commerce giants above, a large number of other non-financial institutions have engaged in various types of digital finance businesses. For example, the PBOC has reported that by 2013 there were more than 250 Internet payment institutions, "more than 350 active P2P online lending platforms", and around 21 crowdfunding platforms in the market.[71] These numbers increased dramatically in the past years. For example, while China was already the world's largest P2P lending market by 2013, the number of P2P lending platforms has since continued to grow at a phenomenal pace. By June 2016, there were 4,127 P2P lending platforms in China with settlements of around RMB 842.2 billion transactions for the first half of the year.[72] In respect of crowdfunding, the number of platforms increased to 283 by the end of 2015 (compared to 116 platforms in 2014) and they raised a total of RMB49.5 billion ($7.5 billion) in that year (compared to RMB 915 million (about $148 million) in 2014).[73] The rapid growth of these digital finance platforms shows the great potential of China's DFS market and the fast-growing demand of investors and consumers for DFS in China. It has been estimated that with Ant Financial's $4.5 billion private placement, Chinese DFS companies are well-positioned to attract the largest investments around the globe in 2016 and will continue to grow.[74]

3.3 Regulation of Digital Financial Services in China

The Chinese government has made great efforts to promote financial inclusion since 2005. The expansion of financial inclusion for SMEs and in rural areas was one of the policy priorities in China's 11th Five-Year Plan.[75] With the rapid advancement and wide adoption of technology, digital finance has been treated by the government as one of the most important means to improve financial inclusion. For example, China's 12th Five-Year Plan for the Development and Reform of the Financial Industry gave strong policy direction for the promotion of technology and e-transactions in the financial sector.[76] In line with the policy direction, China's major banking regulators, the PBOC and the China Banking Regulatory Commission ("CBRC"), have issued many statements and rules consistently aimed at encouraging the use of technology in the financial industry.[77] For example, in the PBOC Report 2014, the PBOC endorsed five major contributions digital finance has made to the Chinese economy: (1) promoting inclusive finance, (2) propelling the development of private capital, (3) satisfying the demand of e-commerce development, (4) reducing transaction costs and improving allocation of resources, and (5) encouraging financial product innovation.[78] The CBRC, as early as 2006, introduced *Guidelines of Financial Innovation of Commercial Banks*

to "encourage financial innovation, supervise innovative activities, and speed up healthy and continuous development of new banking products and services".[79] More recently in 2012 and 2013, the CBRC re-emphasized the significance of digital finance to the enhancement of financial inclusion and the development of China's financial sector.[80]

As mentioned above, while encouraging the continuous development of digital finance, the Chinese government has been aware of the potential risks associated with DFS and the need for regulation. The PBOC Report 2014 identified some of the risks in relation to financial stability, consumer protection, competition in and efficiency of the financial sector, and illegal activities.[81] In a policy briefing held by the State Council in January 2015, the need for balanced regulation and supervision of digital finance was emphasized.[82] Two months later during the 3rd Session of the 12th National People's Congress, PBOC Deputy Governor Pan Gongsheng reportedly disclosed to the media that a regulatory framework on digital finance will be gradually established within the year and the goal of regulation is to "leave certain space for the development of Internet finance while drawing the bottom line clearly."[83] The balanced approach to the regulation of DFS was eventually endorsed in China's 13th Five-Year Plan (2016–2020) which emphasizes on the healthy development of DFS as an integral element of the continuous reforms of China's financial system.[84] With respect to the division of labor in the regulatory and supervisory framework, the role of the regulators has gradually taken shape. The PBOC leads regulatory activities generally and is "primarily responsible for overseeing payment-related services (such as third-party payment)", anti-money laundering activities and the credit reporting industry.[85] The CBRC, with its local offices and supervisory agencies, is mainly responsible for the supervision of P2P lending platforms and crowdfunding and for consumer protection.[86] In addition, the National Internet Finance Association of China, which was created in 2014 and commenced operation in March 2016, will be responsible for promoting self-regulation of the industry in line with the rules developed by the financial regulators.[87]

China's regulatory framework for DFS can be divided into two periods: the initial period before 2015 and the development period since 2015. The remainder of this section considers China's regulatory activities before and after 2015.

3.3.1 DFS Regulation Before 2015

The initial period of China's regulation of DFS before 2015 witnessed the promulgation of several rules by China's banking regulators on certain types of digital finance. The major regulations include (1) the *Rules on the Administration of Electronic Banking* ("E-banking Rule")[88] and the *Guidelines on E-banking Security Evaluation*[89] ("E-banking Guideline") issued by the CBRC in 2006, and (2) the *Rules on the Administration of Payment Services*

Provided by Non-Financial Institutions[90] ("Payment Rule") and *Measures on the Implementation of the Rules on the Administration of Payment Services Provided by Non-Financial Institutions*.[91]

The E-banking Rule applies to e-banking services provided by a financial institution via the Internet, telephone, mobile phone and wireless networks, and other digital devices and networks (Article 2). It requires financial institutions proposing to conduct domestic or cross-border e-banking businesses to (1) seek approval of the CBRC (Article 4), and (2) establish a comprehensive internal risk management and control system and a department with competent personnel to operate and manage the system (Article 6). The rule lays down detailed criteria and procedures for the assessment of whether financial institutions are qualified to conduct e-banking businesses. With the E-banking Guideline, the rule also sets forth a comprehensive framework for the internal risk management and external professional evaluation of qualified financial institutions. However, the two measures have a number of weaknesses. For example, they do not provide detailed rules on the protection of clients' information and privacy and the E-banking Rule does not set out in detail the disclosure obligations of financial institutions and hence do not provide sufficient protection for consumers.

The Payment Rule aims to regulate the provision of payment services by non-financial institutions and to protect the legitimate interests of consumers and other stakeholders (Article 1). It prohibits non-financial institutions or individuals from providing defined third-party payment services unless they hold a Payment Services Licence ("PSL") issued by the PBOC and become a payment institution (Article 3). It sets out the licensing requirements, the term of license, notification requirements for any changes of PSL holders, and procedure for renewal applications. It imposes a number of restrictions on PSL holders, such as, on how they shall deal with funds received from clients for payment services (Articles 24–30). Despite the restrictions, the PBOC has clarified that the rule is not intended to impose any quantitative restrictions and will allow the issuance of a PSL to all qualified applicants.[92] According to the PBOC, there have been around 267 licensed payment institutions by January 2016.[93] The rule, therefore, accords with the Chinese government's commitments to a balanced approach to the regulation of Internet finance. However, given the low legislative level of the rule, it has caused difficulties in encouraging coordination between the PBOC and other regulatory authorities in enforcing it.[94] Further, although the rule attempts to prohibit the misappropriation of clients' funds by payment institutions, it is silent on issues such as the payment of interests on funds and whether the funds may be used for investment. Finally, the rule does not contain specific provisions on the regulation and supervision of cross-border third party payment businesses.

Besides the weaknesses of the existing regulations, another major weakness of China's DFS regulatory framework before 2015 concerns the lack of specific legislation on peer-to-peer

(P2P) lending, crowdfunding, and online investment or management of funds. For example, since 2011, increasing numbers of P2P lending companies have abruptly collapsed due to financial difficulties, and strong voices have been calling for the promulgation of regulations on P2P lending.[95] In response, the CBRC issued the *Circular on Risks Associated with Peer-to-Peer Lending* on 23 August 2011.[96] However, instead of providing specific rules on P2P lending, the Circular merely identifies a number of risks associated with P2P lending as a result of the lack of regulation and supervision, such as illegal funding, fraudulent activities, money laundering, credit and reputational risks, etc. The Circular has been proven ineffective to control these risks by the high and increasing default rates in P2P lending between 2011 and 2014.[97] These risks may also arise from crowdfunding activities.[98] Apart from the Circular, there were no specific regulations or rules on P2P lending before 2015. With respect to crowdfunding, the latest development was the publication of a consultation draft of *Measures on the Administration of Equity Crowdfunding* in December 2014 by the China Securities Regulatory Commission ("CSRC") and the Securities Association of China ("SAC").[99] This instrument makes equity crowdfunding activities lawful and sets out the entry criteria, obligations and liabilities, registration and reporting requirements in relation to equity crowdfunding platforms and investors. However, it appears that the measure is intended to be an industry self-discipline instrument to be administered by the SAC rather than be a CSRC rule. Further, it only covers equity crowdfunding and does not apply to other forms of crowdfunding activities which have represented the majority of crowdfunding platforms in China.[100]

Thus, China's regulatory framework on digital finance before 2015 was very preliminary. Chinese financial authorities, businesses and scholars were of the view that it was insufficient to properly regulate the rapidly growing digital finance sector.[101] A comprehensive regulatory framework was much needed to "specify the bottom line, strengthen the oversight of the business and guide the industry, which is motivated by innovation, to develop in a healthy and sustainable way."[102]

3.3.2 DFS Regulation After 2015

From early 2015, there was growing recognition, from both official and unofficial sources, that China needed to accelerate the development of DFS regulation so as to establish a preliminary regulatory framework by the end of the year. A landmark regulatory achievement was the joint promulgation of the *Guideline on the Promotion of the Health Development of Internet Finance* ("Guideline") by ten central government ministries and commissions on 18 July 2015.[103] The Guideline was significant in many aspects. First, it invigorated regulatory efforts by mandating the relevant authorities to formulate detailed rules on different types of DFS such as Internet payment, online lending including P2P lending and micro-loans, crowdfunding, and online wealth management funds. Second, it reiterated the policy orientation as

being to promote the development and growth of DFS and set out approaches to achieve this. These approaches included encouraging (1) banks to provide deposit, fund management and settlement services to DFS providers; (2) entities and individuals to provide finance to DFS providers; (3) regulators to support DFS providers by simplifying administrative process and providing tax benefits for DFS start-ups; (4) the establishment of DFS infrastructure. Third, it laid down basic principles on the regulation of DFS including: (1) clearly defining the entry thresholds and boundaries of different types of DFS and the roles of different DFS providers; (2) limiting DFS to small value transactions; (3) strengthening the preservation and management of funds received from clients for DFS (e.g. online payment services); (4) establishing detailed rules on product and risk disclosure and risk management; (5) reinforcing the protection of consumers, Internet security and information safety, and the prohibition of money laundering activities and financial crimes. In addition, the Guideline clarifies the division of labor among the regulators such that the PBOC, the CBRC, and the CSRC will, respectively, be responsible for the regulation and supervision of Internet payment services; online lending services; and equity crowdfunding and online investment fund management services. Accordingly, the Guideline lays the groundwork for the development of DFS regulation and is a significant achievement in the regulatory process. Following the publication of the Guideline, a number of pieces of draft legislation have been released for consultation, echoing the Guideline's mandate to accelerate regulatory activities.

On 31 July 2015, the PBOC published a consultation draft of the *Rules on the Administration of Internet Payment Business by Non-Bank Payment Institutions*[104] and the consultation was completed on 28 August 2015. The Rules were subsequently promulgated by the PBOC on 28 December 2015 and took effect on 1 July 2016.[105] The Rules aim to regulate Internet payment services provided by non-bank payment institutions, to manage the potential risks associated with such services, and to protect the interests of consumers. To achieve these objectives, a wide range of detailed and strict provisions are introduced. For example, payment institutions must hold an Internet Payment Services License to provide Internet payment services which, in principle, are limited to small value transactions (Articles 2 and 3). Payment institutions must not undertake the following businesses including deposit and withdrawal, lending, finance, fund management, guarantee, or currency exchange (Article 9). A "payment account" must be opened only in accordance with the instructions of clients and must not be overdrawn, lent, transferred, or used for illegal activities. Payment institutions must verify and use the genuine information of clients for the purpose of opening a "payment account" (Article 6). Every payment transaction undertaken by a payment institution on behalf of a client must be authorized by the client and the client's bank (Article 10). Based on the level of security check on clients' information, "payment account" is classified into different categories, i.e. Category I–III, under which different limits are imposed in terms of transaction values (Article 11). The transaction value under Category I, which is opened with the lowest level of

www.elsevierdirect.com

security verification, must not accumulatively exceed RMB 1,000. Under Categories II and III, the annual limits on transaction value are RMB 100,000 and 200,000 respectively. For business clients, any single payment beyond RMB 50,000 must be supported by documents that trigger the payment, amongst other evidence (Article 14). In addition, limitations are also applied to the value of daily transactions depending on the level of security check on clients' information and the rank of payment institutions' qualifications (Articles 24 and 35). Finally, the Rules contain detailed provisions on risk management and consumer protection, requiring payment institutions to establish and maintain a "clients' risk ranking and management system" (Article 17), a "risk reserve fund and compensation policy" (Article 19), to name a couple. Without a doubt, the publication of the Rules is a significant progress in China's regulation of DFS. It considerably strengthens the supervision and disciplining of non-bank payment institutions in providing Internet payment services. The rules are much-needed given the significant share of these institutions in Internet payment businesses (represented by Internet giants such as Alibaba and Tencent) and the rapid growth of smaller and new payment institutions. Given the strict requirements, the Rules are likely to have the effect of reducing the number of payment institutions over time so that only payment institutions with a high level of risk management and security protection will remain in the market and hence the healthy development of Internet payment services will be promoted.

On 12 August 2015, the State Council released a consultation draft *Regulation on Non-Depositing Loan Institutions*[106] with a 1-month consultation period. The Regulation deals with loan entities that do not engage in deposit business and hence use their own funds for lending activities. As a general rule, no entities are allowed to conduct lending business without having obtained a lending business permit ("LBP") from authorities designated by provincial governments. Detailed entry criteria and LBP application procedures are contemplated to standardize the financial and other qualifications of lending institutions. Also set out in detail are various obligations of loan institutions in relation to loan agreements, internal risk management, assessment of borrowers' credit, repayment capability and other information, debt collection, etc. In addition, the Regulation imposes detailed obligations on supervisory authorities and stringent penalties on lending institutions. Last but not least, the Regulation applies to online lending institutions and mandates the CBRC to formulate detailed rules on online lending activities. Accordingly, the Regulation lays down a basic framework for the regulation and supervision of loan institutions and lending activities especially those not yet covered by existing legislations such as online lending activities. While the Regulation explicitly applies to online micro-loan businesses, it is less clear whether it applies to P2P lending activities. This is because the scope of the Regulation appears to be limited to lending activities as opposed to lending services, such as P2P platforms, where service providers merely act as a middleman between borrowers and lenders. Despite the lack of clarity, the Regulation

provides a model for the regulation of P2P lending activities and a clear mandate to CBRC to complete the regulatory work.

To implement the regulatory mandate contemplated in the regulation of the State Council above, the CBRC issued a consultation draft of the *Provisional Rules on the Administration of the Business Activities of Online Lending Intermediaries*[107] on 28 December 2015 and completed the consultation on 27 January 2016. It is commonly understood that these Rules aim to target P2P lending activities.[108] The Rules seek to regulate Internet-based lending information intermediaries in their provision of services for online lending activities between individuals, corporations and other organizations (Article 2). The scope of the services is strictly confined to the provision of information relevant to the lending activities to borrowers and lenders such that the intermediaries themselves must not provide loans, set up fund pools, illegally raise funds, or engage in crowdfunding activities, amongst other restrictions (Articles 3 and 10). Before undertaking the online lending services, the intermediaries must obtain a business license and register with the relevant local branches of the CBRC (Article 5). The Rules set out detailed obligations of the intermediaries such as collection, organization, assessment and online publication of lending information; verification of the qualifications of lenders and borrowers and the authenticity of financing projects; taking reasonable measures to prevent and disclose fraudulent behaviors; creation of client identification system; anti-money laundering and anti-terrorist financing obligations; and submission of loan information to a central database to be established for the online lending industry (Articles 9, 25–28, 30–32). These obligations are imposed for the purpose of protecting borrowers and lenders and minimizing the risks associated with online lending activities, particularly P2P lending.

With the release of the new measures above, China is making significant progress in establishing a comprehensive framework for the regulation of DFS. A practical question for the government, however, is whether the measures are overly strict such that they may drive smaller institutions out of the market, discourage new entrants, and consequently hamper the growth of digital financial services.

3.4 Conclusion

With the explosive growth of DFS in China in recent years, Chinese financial regulators were alarmed about the problems created by DFS and committed to develop a preliminary framework for the regulation of DFS by the end of 2015. To meet this aggressive deadline, rigorous efforts have been made since mid-2015 with the publication of the Guideline and several draft regulations. The Guideline provides the fundamental principles and roadmap for DFS regulatory work, and the draft regulations, following the principles and mandate of the Guideline, set out the detailed rules for the regulation and supervision of specific types of DFS. This

www.elsevierdirect.com

remarkable regulatory progress in such a short period of time suggests that more specific legislation may be issued in the imminent future, and that China will most likely become a front-runner worldwide in development of a sustainable, effective regulatory framework for DFS. The major challenges ahead are: (1) to ensure the existing and future legislation have the potential to deal with new forms of, and new problems associated with, DFS; (2) to ensure the new regulations are effectively and efficiently enforced; (3) to balance the regulation of DFS with its healthy growth and not diminish competition in the sector too severely.

Notes

1. This chapter is based on Weihuan Zhou, Douglas Arner & Ross Buckley, "Regulation of Digital Financial Services in China: Last Mover Advantage?" (2015) 8(1) *Tsinghua China Law Review* 26–62. For a thorough review of the evolution of Fintech as a global phenomenon over the past decades, see Douglas W. Arner, Jànos Nathan Barberis & Ross P. Buckley, "The Evolution of Fintech: A New Post-crisis Paradigm?" (Sept. 2015), available at http://ssrn.com/abstract=2676553.

2. For a discussion of China's interest rate policy reforms during this period, see Alexander Ballantyne, Jonathan Hambur, Ivan Roberts & Michelle Wright, Financial Reform in Australia and China, Reserve Bank of Australia, Sept. 2014, at 23–25, available at http://www.rba.gov.au/publications/rdp/2014/pdf/rdp2014-10.pdf.

3. Bo Hu, Financial Repression and Interest Rate Liberalization in China, Jordan River Economic Conference 2014, Apr. 2014, at 2, available at https://economics.indiana.edu/home/conferences/2014-jordan-rivereconomics-conference/files/2014-05-02-05.pdf.

4. Tjun Tang, Yue Zhang & David He, "The Rise of Digital Finance in China: New Drivers, New Game, New Strategy", The Boston Consulting Group, Oct. 2014, at 5–6.

5. Financial Stability Analysis Group of the People's Bank of China, "China Financial Stability Report 2014", Apr. 2014, at 178–179, available at: http://www.centerforfinancialstability.org/fsr/chn_fsr_201407.pdf.

6. ResearchInChina, China ATM (Automatic Teller Machine) Market Report, Aug. 2008, available at http://www.researchinchina.com/FreeReport/PdfFile/633879276546958750.pdf; China's First ATM Card, Bank of China, http://www.boc.cn/en/aboutboc/ab5/200811/t20081119_1602016.html.

7. Pete Sparreboom & Eric Duflos, CGAP & World Microfinance Forum Geneva, "Financial Inclusion in the People's Republic of China: An Analysis of Existing Research and Public Data", (Aug. 2012) 1–45.

8. Retail Banking Research, "China Overtakes USA as World's Largest ATM Market", 20 Jun. 2014, available at: http://www.rbrlondon.com/newsletters/b325e.pdf.

9. ReportLinker, "China Automatic Teller Machine (ATM) Industry Report, 2016–2020", Apr. 2016, available at: http://www.reportlinker.com/p03767878-summary/China-Automatic-Teller-Machine-ATM-Industry-Report.html.

10. Jason Hahn, "The World's First ATM with Facial Recognition Technology is Unveiled to the Public in China", Digital Trends (31 May 2015), available at: http://www.digitaltrends.com/cool-tech/the-worlds-first-atm-with-facial-recognition-technology-is-unveiled-to-the-public-in-china/.

11. Xina Yuan, "Present and Future of Internet Banking in China" (2010) 15(1) *Journal of Internet Banking and Commerce* 1–10 at 3.

12. Ibid., at 4.

13. See above note 4, Tang, Zhang & He, "The Rise of Digital Finance in China", at 32.

14. Ibid., at 4.

15. See Wu Hongyuran, "Minsheng Bank is Latest to Join E-Commerce Fray", Caixin online (23 Aug. 2013), available at: http://english.caixin.com/2013-08-23/100573307.html; Li Xiaoxiao & Liu Caiping, "Banks Trying Direct Route to Online Future", Caixin online (22 Jan. 2015), available at: http://english.caixin.com/2015-01-22/100777224.html.

16. See China Daily, "China reports surge of Internet banking transactions", (25 Mar. 2015), available at: http://www.chinadaily.com.cn/business/2015-03/25/content_19908598.htm.

17. See Hua Zhang, "China's Direct Banks: Birth of a New Banking Sector", CELENT (5 Jan. 2015), available at: http://www.celent.com/reports/chinas-direct-banks-birth-new-banking-sector.

18. Arlyss Gease and Joan Qiu, "China 20/20: The Future of Mobile Payment in China", Maverick China Research (Dec. 2012), at 4, available at: http://www.maverickchina.com/reports/china-20-20-whitepapers.

19. Ibid. Also see China UnionPay, "Brief Review on the Development of China's Payment System", undated, available at: http://en.unionpay.com/merchantService/knowledge/file_4420451.html (describing the Bulk Electronic Payment System as the "public platform for financial institutions and payment and settlement organizations in the banking industry to develop creative payment services and extend service functions").

20. See Leesa Shrader and Eric Duflos, "China: A New paradigm in Branchless Banking", CGAP (Mar. 2014), at 37.

21. See above note 5, PBOC, "China Financial Stability Report 2014", at 116.

22. See Financial Stability Analysis Group of the PBOC, "China Financial Stability Report 2015" (May 2015) at 123, available at: http://www.pbc.gov.cn/publish/english/959/index.html.

23. See Financial Stability Analysis Group of the PBOC, "China Financial Stability Report 2016" (Jun. 2016) at 99, available at: http://www.gov.cn/xinwen/2016-06/28/5086110/files/11c908711c0d4acdbe8d3ab1bf4a254a.pdf (in Chinese).

24. See above note 4, Tang, Zhang & He, "The Rise of Digital Finance in China", at 1–11. For a more detailed overview of the development of DFS in China, see above note 5, PBOC, "China Financial Stability Report 2014", at 171–176.

25. See above note 20, Shrader and Duflos, "China: A New paradigm in Branchless Banking", at 6–8, 15–17.

26. For an overview of the business of the Alibaba Group, see Leesa Shrader, "Microfinance, E-Commerce, Big Data and China: The Alibaba Story", CGAP (11 Oct. 2013), available at: http://www.cgap.org/blog/microfinance-e-commerce-big-data-and-china-alibaba-story.

27. See Christina Larson, "Alipay Leads a Digital Finance Revolution in China", MIT Technology Review (26 Jan. 2015), available at: http://www.technologyreview.com/news/534001/alipay-leads-a-digital-finance-revolution-in-china/.

28. See Alibaba Group, "Alipay 2014 Spending Report Sheds Light on Chinese Online Spending Behavior", Press Release (8 Dec. 2014), available at: http://www.alibabagroup.com/en/news/article?news=p141208.

29. See Yolanda Redrup, "Alibaba launches in Australia with Alipay", Sydney Morning Herald (18 Nov. 2014), available at: http://www.smh.com.au/business/alibaba-launches-in-australia-with-alipay-20141118-11p3ly.html. Most recently, Alibaba "revealed plans to significantly expand its presence in Australia", see John McDuling, "Alibaba reveals how Australia fits into world domination plans", Financial Review (18 Jul. 2016), available at: http://www.afr.com/technology/alibaba-reveals-how-australia-fits-into-world-domination-plans-20160717-gq7f73.

30. See Leena Rao, "Alipay's US chief talks expansion", FORTUNE (19 Jun. 2015), available at: http://fortune.com/2015/06/19/alipay-china-uber-alibaba/.

31. See Arjun Kharpal, "Alipay to launch in Europe as Alibaba steps up payments game", CNBC (5 Apr. 2016), available at: http://www.cnbc.com/2016/04/05/alipay-to-launch-in-europe-as-alibaba-steps-up-payments-game.html.

32. For the various products of Alipay, see Alipay's global website at: https://global.alipay.com/ospay/home.htm.

33. Craig Smith, "By the Numbers: 22 Crazy Alipay Statistics", DMR Updates (1 Apr. 2016), available at: http://expandedramblings.com/index.php/alipay-statistics/.

34. For an introduction of Yu'e Bao, see Moran Zhang, "Alibaba's Online Money Market Fund Yu'e Bao: 8 Things You Need To Know", International Business Times (11 Mar. 2014), available at: http://www.ibtimes.com/alibabas-online-money-market-fund-yue-bao-8-things-you-need-know-1560601. Also see the official website of Yu'e Bao here: https://bao.alipay.com/yeb/index.htm (in Chinese).

35. Ibid.

36. Ibid.

37. Ibid.

38. See above note 4, Tang, Zhang & He, "The Rise of Digital Finance in China", at 4.

39. Ibid.

40. Research in China, "Summary – China Internet Crowdfunding and Wealth Management Industry Report, 2016" (Jun. 2016), available at: https://www.reportbuyer.com/product/3226800/china-Internet-crowdfunding-and-wealth-management-industry-report-2016.html.

41. See above note 26, Shrader, "Microfinance, E-Commerce, Big Data and China: The Alibaba Story".

42. Ibid.

43. Simon Rabinovitch, "Alibaba Digs Deep for Chinese Banking Treasure", Financial Times (25 Aug. 2013), available at: http://www.ft.com/intl/cms/s/0/f956b004-ffee-11e2-9c40-00144feab7de.html#axzz3emowunHf.

44. See Susan Wang, "China's Women Entrepreneurs Targeted for Small-Business Loans", Alizila (27 Jan. 2015), available at: http://www.alizila.com/chinas-women-entrepreneurs-targeted-small-business-loans.

45. See Alibaba Group, "Official Launch of Ant Financial Services Group Brings New Financial Ecosystem to China", Press Release (16 Oct. 2014), available at: http://www.alibabagroup.com/en/news/article?news=p141016.

46. Ibid.

47. See Susan Wang, "Ant Financial Brings Biz Loans, Investment Products to Rural China", Alizila (17 Mar. 2015), available at: http://www.alizila.com/ant-financial-brings-biz-loans-investment-products-rural-china.

48. See Tracey Xiang, "Alibaba's Online Equity Crowdfunding Platform ANTSDAQ Launches Beta", Technode (25 Nov. 2015), available at: http://technode.com/2015/11/25/alibabas-onilne-equity-crowdfunding-platform-antsdaq-launches-beta/.

49. See Ray Chan, "Ant Financial raises record $4.5b", FinanceAsia (26 Apr. 2016), available at: http://www.financeasia.com/News/407679,ant-financial-raises-record-45b.aspx.

50. See The Australian, "China's Alibaba launches Internet bank", 26 Jun. 2015, available at: http://www.theaustralian.com.au/business/latest/chinas-alibaba-launches-Internet-bank/story-e6frg90f-1227415805816.

51. See Cecilia Wu, "Alibaba's MYbank, how does it go in the past 8 months?", Sapidaily (11 Mar. 2016), available at: http://www.sapidaily.com/alibabas-mybank-how-does-it-go-in-the-past-8-months/.

52. Tencent's official website is available at: http://www.tencent.com/en-us/at/abouttencent.shtml.

53. Reuters, "China's Tencent hits $200 billion market cap for first time", 13 Apr. 2015, available at: http://www.reuters.com/article/2015/04/13/us-tencent-valuation-idUSKBN0N40WN20150413.

54. Vaseem Khan, "Alipay Vs Tenpay – The China Payments Rivalry", LTP (12 Feb. 2015), available at: http://letstalkpayments.com/alipay-vs-tenpay-the-china-payments-rivalry-2/.

55. See Wikipedia, "WeChat Red Envelope", last modified on 29 Mar. 2015, available at: https://en.wikipedia.org/wiki/WeChat_red_envelope.

56. See Josh Horwitz, "Chinese WeChat users sent out 20 million cash-filled red envelopes to friends and family within two days", TECHINASIA (5 Feb. 2014), available at: https://www.techinasia.com/wechats-money-gifting-scheme-lures-5-million-chinese-users-alibabas-jack-ma-calls-pearl-harbor-attack-company/.

57. See David Yin, "Tencent's WeChat Sends 1 Billion Virtual Red Envelopes on New Year's Eve", Forbes (19 Feb. 2015), available at: http://www.forbes.com/sites/davidyin/2015/02/19/tencents-wechat-sends-1-billion-virtual-red-envelopes-on-new-years-eve/; Gabriel Wildau, "Tencent Beats Alibaba in 'red envelope' app war", Financial Times (27 Feb. 2015), available at: http://www.ft.com/intl/cms/s/0/c39c96c6-be2a-11e4-8cf3-00144feab7de.html#axzz3eyf3RyLo.

58. See above note 4, Tang, Zhang & He, "The Rise of Digital Finance in China", at 4.

59. See Paul Bischoff, "WeChat leaps into banking, lets users set up online investment fund", TECHINASIA (16 Jan. 2014), available at: https://www.techinasia.com/wechat-leaps-banking-lets-users-set-online-investment-fund/.

60. See Gabriel Wildau, "Tencent launches China's first online-only bank", Financial Times (5 Jan. 2015), available at: http://www.ft.com/intl/cms/s/0/ccc5a6dc-9488-11e4-82c7-00144feabdc0.html#axzz3f4JCnBsS.

61. Juro Osawa, "Tencent's WeChat App to Offer Personal Loans in Minutes", The Wall Street Journal (11 Sep. 2015), available at: http://www.wsj.com/articles/tencent-to-add-personal-loan-feature-to-wechat-app-1441952556.

62. Abdullah Saeed Qureshi, "Tencent-Backed WeBank Closes in on Raising Funds at $5.5 Billion Valuation", China Business News (27 Jan. 2016), available at: http://www.chinabusinessnews.com/2232-tencentbacked-webank-closes-in-on-raising-funds-at-55-billion-valuation/.

63. See Wikipedia, "Baidu", last modified on 18 Jun. 2015, available at: https://en.wikipedia.org/wiki/Baidu.

64. See Josh Horwitz, "Baidu announces upcoming launch of Baifa as it moves into personal finance", TECHINASIA (21 Oct. 2013), available at: https://www.techinasia.com/baidu-announces-upcoming-launch-baifu-moves-personal-finance/.

65. Ibid.

66. Nisha Koul, "Chinese Internet Companies Alibaba, Baidu Offer Financial Services Through Subsidiaries Yu'e Bao, Baifa", MicroCapital (5 Feb. 2014), available at: http://www.microcapital.org/microcapital-brief-chinese-Internet-companies-alibaba-baidu-offer-financial-services-through-subsidiaries-yue-bao-baifa/.

67. Paul Bischoff, "Baidu rebrands online finance service, introduces loans", TECHINASIA (25 Apr. 2014), available at: https://www.techinasia.com/baidu-rebrands-online-finance-service-introduces-loans/.

68. Ibid.

69. Paul Bischoff, "Baidu now lets anyone invest in movies, will make Chinese version of *Gone with the Wind*", TECHINASIA (22 Sep. 2014), available at: https://www.techinasia.com/baidu-lets-invest-movies-chinese-version-emgone-windem/.

70. Arjun Kharpal, "Baidu launches online bank to take on rivals Alibaba, Tencent", CNBC (18 Nov. 2015), available at: http://www.cnbc.com/2015/11/18/baidu-launches-online-bank-to-take-on-rivals-alibaba-tencent.html.

71. See above note 5, PBOC, "China Financial Stability Report 2014", at 174–175.

72. The data information is provided by www.wangdaizhijia.com a Chinese website providing all sorts of information on P2P lending in China. For the P2P data, see http://shuju.wdzj.com/industry-list.html (in Chinese). For a recent report on the development of P2P lending in China, see Mingkang Liu, "Internet Finance and Regulation in China", FGI Report (Aug. 2015), available at: http://www.asiaglobalinstitute.hku.hk/en/Internet-finance-regulation-china/.

73. Dongmei Li, "China Crowdfunding Platforms Raised $1.7B in 2015", China Money Network (13 Jan. 2016), available at: http://www.chinamoneynetwork.com/2016/01/13/china-crowdfunding-platforms-secured-1-7b-in-2015; Tracey Xiang, "China's Crowdfunding Market as of 2014", TechNode (23 Jan. 2015), available at: http://technode.com/2015/01/23/chinas-crowdfunding-market-2014/.

74. Ray Chan, "Fintech: how China is taking the lead", FinanceAsia (23 Jun. 2016), available at: http://www.financeasia.com/News/427152,fintech-how-china-is-taking-the-lead.aspx.

75. See Zhou Xiaochuan, "Achievements of Financial Sector Reform and Development in the 11th Five-Year Plan Period", The People's Bank of China (9 Dec. 2010), available at: http://www.pbc.gov.cn/publish/english/955/2011/20110217095304062355521/20110217095304062355521_.html.

76. See The 12th Five-year Plan for the Development and Reform of the Financial Industry, at 38, available at: http://www.csrc.gov.cn/pub/csrc_en/newsfacts/release/201210/W020121010631355001488.pdf.

77. See generally above note 4, Tang, Zhang & He, "The Rise of Digital Finance in China", at 11–12; above note 20, Shrader and Duflos, "China: A New paradigm in Branchless Banking", at 21–27.

78. See above note 5, PBOC, "China Financial Stability Report 2014", at 172–173.

79. See CBRC, *Guidelines on Financial Innovation of Commercial Banks*, promulgated on 6 Dec. 2006 and effective on 11 Dec. 2006, official translation available at: http://www.cbrc.gov.cn/EngdocView.do?docID=2897.

80. See above note 20, Shrader and Duflos, "China: A New paradigm in Branchless Banking", at 21, 23.

81. See above note 5, PBOC, "China Financial Stability Report 2014", at 178–179.

82. See The State Council of the PRC, "Full transcript of policy briefing of the State Council on Jan. 23, 2015", 23 Jan. 2015, available at: http://english.gov.cn/news/policy_briefings/2015/01/23/content_281475043823916.htm.

83. See China Daily, "China to issue guidelines for Web finance companies", 5 Mar. 2015, available at: http://www.ecns.cn/business/2015/03-05/156739.shtml.

84. See Chapter 16 "Promotion of Financial System Reforms" in China's 12th Five-Year Plan, available at: http://news.xinhuanet.com/politics/2016lh/2016-03/17/c_1118366322_5.htm (in Chinese).

85. See generally above note 4, Tang, Zhang & He, "The Rise of Digital Finance in China", at 12; above note 20, Shrader & Duflos, "China: A New paradigm in Branchless Banking", at 22. Also see China Daily, "Self-regulation of online financial industry", 4 Apr. 2014, available at: http://china.org.cn/business/2014-04/04/content_32001588.htm.

86. Ibid.

87. See above note 85, "Self-regulation of online financial industry". Also see Xinhua News, "China Internet Finance Association Established in Shanghai" (25 Mar. 2016), available at: http://news.xinhuanet.com/fortune/2016-03/25/c_1118444675.htm (in Chinese).

88. *Dian Zi Yin Hang Ye Wu Guan Li Ban Fa*, promulgated by CBRC Decree No. 5 on 26 Jan. 2006, effective on 1 Mar. 2006.

89. *Dian Zi Yin Hang An Quan Ping Gu Zhi Yin*, promulgated by CBRC Decree No. 9 on 26 Jan. 2006, effective on 1 Mar. 2006.

90. *Fei Jin Rong Ji Gou Zhi Fu Fu Wu Guan Li Ban Fa*, promulgated by PBOC Decree No. 2 on 14 Jun. 2010, effective on 1 Sep. 2010.

91. *Fei Jin Rong Ji Gou Zhi Fu Fu Wu Guan Li Ban Fa Shi Shi Xi Ze*, promulgated by PBOC Decree No. 17 on 1 Dec. 2010, effective on the same date.

92. Ren Min Yin Hang Jiu *Fei Jin Rong Ji Gou Zhi Fu Fu Wu Guan Li Ban Fa* Da Wen (PBOC Answers Questions of Reporters on *Rules on the Administration of Payment Services Provided by Non-Financial Institutions*), 28 Jun. 2010, available at: http://cfg.fabao.cn/falvfagui/sfwj/n214184927.shtml (in Chinese).

93. PBOC, Yi Huo Xu Ke Ji Gou (Zhi Fu Ji Gou) (Licensed Payment Institutions), available at: http://www.pbc.gov.cn/zhengwugongkai/127924/128041/2951606/1923625/1923629/d6d180ae/index1.html (in Chinese).

94. Yuzhe Zhang, Zhou Dong Xue Dai Biao: Ying Jin Kuai Chu Tai *Fei Jin Rong Ji Gou Zhi Fu Fu Wu Guan Li Tiao Li* (Representative Zhou Dongxue: *Regulations on Payment Services Provided by Non-Financial Institutions* should be promulgated), CAIXIN (4 Mar. 2015), available at: http://topics.caixin.com/2015-03-04/100787732.html (in Chinese).

95. Takeshi Jungu, "Risks and Opportunities in China's Growing P2P Lending Market", Nomura Research Institute (10 Sep. 2014), at 2, available at: https://www.nri.com/~/media/PDF/global/opinion/lakyara/2014/lkr2014202.pdf; Jinyan Zhang, "Lun Wo Guo Ren Ren Dai De Fa Zhan Xian Zhuang, Zhu Yao Feng Xian Ji Fa Lv Gui Fan" (An Analysis of the Current State, Major Risks and Regulations of P2P Lending in China) (2013)(3) *Xi Nan Jin Rong* (*Southwest Finance*), available at: http://202.119.108.161:93/modules/showContent.aspx?title=&Word=&DocGUID=fa477088bf1a45139fa721de20468e8d (in Chinese).

96. *Guan Yu Ren Ren Dai You Guan Feng Xian Ti Shi De Tong Zhi*, promulgated by the General Office of the CBRC Circular No. 254 on 23 Aug. 2011, effective on the same date.

97. See above note 72, Liu, "Internet Finance and Regulation in China", at 15.

98. Jerin Mathew, "China Warns of Illegal P2P Lending and Crowd Funding Loopholes", International Business Times (22 Apr. 2015), available at: http://www.ibtimes.co.uk/china-warns-illegal-p2p-lending-crowd-funding-loopholes-1445535.

99. A Chinese version of the consultation draft is available at: http://www.sac.net.cn/tzgg/201412/P020141218543931814762.doc.

100. See Tracey Xiang, "China's Crowdfunding Market as of 2014", TechNode (23 Jan. 2015), available at: http://technode.com/2015/01/23/chinas-crowdfunding-market-2014/.

101. See, for example, above note 83, "China to issue guidelines for Web finance companies"; J. An, B. Zhao & W. Wang, "The Internet Finance in China: The Living Space and the Regulations" (2015)8(S4) *Indian Journal of Science and Technology* 106–114; BangKun An & Jinyang Ruan, "Hu Lian Wang Jin Rong: Jian Guan Yu Fa Lv Zhun Ze" ("Internet Finance: Regulation and Legal Principles") (2014)3 *Jin Rong Jian Guan Yan Jiu* (*Financial Regulation Studies*) 57–70. (in Chinese); Li Youxing, Chen Fei & Jin Youfang, "Hu Lian Wang Jin Rong Jian Guan De Tan Xi" (A Study on the Regulation of the Internet Finance) (2014) 44(4) *Journal of Zhejiang University* 87–97 (in Chinese).

102. See above note 5, PBOC, "China Financial Stability Report 2014", at 178.

103. *Guan Yu Cu Jin Hu Lian Wang Jin Rong Jian Kang Fa Zhan De Zhi Dao Yi Jian*, promulgated on 18 Jul. 2015.

104. The official Chinese version of the consultation draft is available at: http://www.gov.cn/xinwen/2015-07/31/content_2907209.htm.

105. *Fei Yin Hang Zhi Fu Ji Gou Wang Luo Zhi Fu Ye Wu Guan Li Ban Fa*, promulgated by PBOC Circular No. 43 on 28 Dec. 2015, effective on 1 Jul. 2016, official Chinese version available at: http://www.gov.cn/gongbao/content/2016/content_5061699.htm.

106. *Fei Cun Kuan Lei Fang Dai Zu Zhi Tiao Li* (*Zheng Qiu Yi Jian Gao*), official Chinese version available at: http://www.chinalaw.gov.cn/article/cazjgg/201508/20150800478726.shtml.

107. *Wang Luo Jie Dai Xin Xi Zhong Jie Ji Gou Ye Wu Huo Dong Guan Li Zan Xing Ban Fa* (*Zheng Qiu Yi Jian Gao*), official Chinese version available at: http://www.gov.cn/xinwen/2015-12/28/content_5028564.htm.

108. See, for example, Takeshi Jingu, "China set to step up regulation of Internet finance from 2016", Nomura Research Institute (10 Mar. 2016); Shaohui Tian, "China tightens regulation over P2P lending", Xinhua News (28 Dec. 2015), available at: http://news.xinhuanet.com/english/2015-12/28/c_134958998.htm.

CHAPTER 4

Big Data Technology: Application and Cases

Liu Dawei, Hu Anzi, Li Gen

CreditEase, China

Contents

4.1 Why Big Data Technology Matters? 66

4.1.1 Introduction to Big Data Technology 66

4.1.2 Problems and Obstacles of Traditional Financial Service 67

4.2 How Big Data Technology Helps Improving Credit Performance 68

4.2.1 Big Data Technology Empowers Digital Finance to Innovate 68

4.2.2 Big Data Credit Investigation 70

4.3 Brief Introduction of CreditEase: Better Technology, Better Finance 72

4.4 An Instance of Big Data Technology: CreditEase Financial Cloud 75

4.4.1 Ultra Large Data Scale 78

4.4.2 Leading Data Processing Technique 78

4.4.3 Advance Knowledge Map Technology 79

4.4.4 Expert Experience and Data Closed-Loop 79

4.5 Cases and Application Scenarios for CreditEase Financial Cloud 80

4.5.1 E-Commerce Platform Cooperation 81

4.5.2 ERP (Enterprise Resource Planning) Software Platform Cooperation 81

4.5.3 Car Rental by Credit 81

4.5.4 Instant Installments 82

References 82

Notes 82

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00004-8
Copyright © 2018 Elsevier Inc. All rights reserved.

4.1 Why Big Data Technology Matters?

4.1.1 Introduction to Big Data Technology

As the techniques of Internet and mobile Internet grow, E-commerce and Social Networking site (SNS) based on these techniques are broadly used, which leads to the huge increase of Internet users and Internet penetration rate. According to statistics from Internet World Stats, in the end of June 2016, Internet users has grown to nearly 3.7 billion people worldwide. Meanwhile, the Internet penetration rate (the percentage of the total population that uses Internet) becomes above 50%.[1] A lot of people are using Internet during this moment. All the activities happening online, including shopping, chatting, web scanning, searching, etc., produce vast data. The scale of data makes storage and computation exceed what traditional distributed storage and computation can handle. The need for new technique makes big data technology and cloud computing come into being.

Big data technology early originated from Internet search, which is now widely used search engine. The application of big data technology dates back to around year 2000, born with rapid growth of Internet. During that time, web pages were booming, with nearly 7 million new pages increased daily. Internet users were facing remarkable obstacle when retrieving information. In order to solve the issue, Internet companies like Google firstly built information library covering billions of web pages, to provide precise search service for users. The solution greatly improves efficiency of using Internet, and becomes the origination of big data application. Following the emergence of Internet industry, this innovative technique of processing massive data was applied gradually to e-commerce, targeted advertisement, intelligent recommendation, social network site, etc. The applications all achieved great business successes. People are inspired and start to recognize the huge value of big data.

> *'Big Data does not imply that the current data volumes are simply 'bigger' than before, or 'bigger' than current techniques can efficiently handle. The need for greater performance or efficiency happens on a continual basis. However, Big Data represents a fundamental change in the architecture needed to efficiently handle current data sets.'*
>
> ***NIST Big Data Interoperability Framework: Volume 1, page 4, 2 Big Data and Data Science Definitions***

Big data greatly benefits analytics due to the capacity of processing large amounts and various types of information. In the past, structured data has typically been the major material for analytics, and has been processed through the use of the relational data model. However, the quantity of unstructured data, such as micro-texts, web pages, forum posts, relationship data,

images and videos, has exploded, and the trend indicates an increase in the incorporation of unstructured data to generate value, in which big data technology is playing the most significant role.

4.1.2 Problems and Obstacles of Traditional Financial Service

The development of finance has positive effect on the increase of economy. Schumpeter brought forward the theory that entrepreneurship and technology innovation can only function well in economic aspects and promote economic growth, with the support of credit or financial market (Joseph A. Schumpeter, 1912, 1934). Other scholars came to the conclusion that there exists parallel relationship between financial development and economic growth (Goldsmith, 1999; King and Levine, 1993; Levine and Zervos, 1996). Financial development can promote economic growth (Beck et al., 2000). However, there is a premise needed for finance to take effect, which is that the structure of finance must fit the structure of economy. The corresponding relationship is directly reflected by the harmony of structural supply and demand.

There is study that confirms that the unbalanced total supply, especially total supply beyond total demand, has negative effect on economic growth. Easterly et al. (2000) found financial deepening has a nonlinear relationship with production. When the credit supply to private sector out of GDP is beyond 100%, industrial sector will be consequently more unstable. Arcand, Berkes and Panizza (2012) for study used data of 30 years (1970–2000) from 33∼42 countries, and further proved that credit supply to private sector accounting for 100% proportion of GDP is the critical point of finance taking positive effect on economic growth. Beyond this critical point, finance will reversely have a negative effect on economic growth, which is called 'Too Much Finance'.

With structural imbalance between supply and demand of financial structure relative to economic development, there will be a structural excessive and inadequate relationship between financial supply and demand, which eventually causes harm to economic growth. Financial structure is the relative proportion and composition of various financial system arrangements within the financial framework, including composition of direct financing and indirect financing, composition of formal finance and informal finance, composition of finance for huge corporations and finance for MSMEs (Micro-, Small, and Medium Enterprises), and degree of banking competition and bank size, etc. (Lin et al., 2009). Whether the structure of financial supplies fits the structure of financial demands, essentially determines the development of finance and eventually decides the effect of finance on economy.

The shortcoming of traditional financial service is that both excess of financial resources and insufficiency of financial resources exist. The fundamental reason for this phenomenon is that

www.elsevierdirect.com

there exists mismatch of financial supplies within traditional financial institutions. Furthermore, the lack of willingness to serve MSMEs and inadequacy of capacity to serve MSMEs within traditional financial institutions lead to this mismatch.

During the development of traditional finance, due to governance and regulation of the government, or institutional monopoly and market failure, financial institutions target high net worth population and large enterprises as the key service object for long time. From a business operation perspective, owing to the small amount and low profits of financial service for MSMEs, institutions need to have a certain scale of business in order to achieve profits. In contrast, financial services for large corporations and high net worth population have features of huge amount and high profits, which allow financial institutions to serve a small number of clients and still gain huge profits. Obviously, financial institutions lose the motivation and willingness to serve MSMEs as a result of the pursuit of the interests. As a significant component of social production, MSMEs contribute the majority of GDP and employments, whereas MSMEs still are facing problems of difficulties in financing and expensive financing, as a result of financial exclusion. Within the traditional financial framework, financial demands of MSMEs can only be satisfied by policy finance subsidized by government and usurious loans.

Traditional financial institutions lacking willingness of serving MSMEs can also be owed to the inadequate capacity for serving MSMEs. On one hand, clients of finance for MSMEs do not have enough traditional activities in record, so financial institutions have difficulties in recognizing their credit degrees, resulting in fact that financial institutions are more likely to assign them to groups of poor credit as a result of lacking collaterals; on the other hand, traditional finance is product driven, with the absence of review based on clients' needs, and eventually ignores the needs for flexibility and rapidity of MSMEs. This forces MSMEs to turn to informal finance.

Internet finance is the complement which makes up for the defects of traditional finance. The emergence of Internet finance is the result of relying on market forces to adjust the problem of financial resources mismatch. To some extent, the rapid growth and huge scale of Internet finance reflect the serious financial repression and the deep imbalance of financial institutions.

4.2 How Big Data Technology Helps Improving Credit Performance

4.2.1 Big Data Technology Empowers Digital Finance to Innovate

Technologies like Internet, big data technology, and cloud computation facilitate the undergoing profound changes happening in the production and lifestyle of people. They have disrupted many traditional industries, and the financial industry is not an exception. Internet finance is the disruptive product of deep fusion of finance and technology. The application of

big data technology brings changes in three aspects, broadens the effective frontier of financial services, and provides a new path for the implementation of financial inclusion.

Information asymmetry is the key cause for the restriction of traditional financial institutions providing financial services to small and micro businesses. Big data technology provides a new solution, replacing the traditional ways such as collateral and guarantee. Through the correlating of multidimensional information, big data technology is capable to characterize fine portraits of each customer, which can be used not only for cross-validation of a certain type of customer's information. The analysis of massive and dynamic data can reveal the nature of the data behind the phenomenon, comprehensively describe the features of each individual such as creditworthiness, preferences, behavior patterns, habits and other characteristics. And eventually financial service will be offered to clients precisely and fairly.

From the perspective of transaction cost theory, Ronald Harry Coase came up with the conclusion that the elimination of negative externality will contribute to achieving effective allocation of resources, increase efficiency, and eventually reduce transaction costs. The high transaction costs of finance for MSMEs are mainly because financial institutions have to put in a lot of time and manpower into investigation and process of every business, which generates a lot of operation costs, as a result of transaction process being cumbersome and opaque. The application of big data technology offers a new effective approach for reducing transaction costs. Big data credit investigation makes measuring the default rate of a credit applicant in few minutes a reality. It can also give an interest rate recommendation based on that default rate (risk-based pricing). Credit applicants no more need to deal with complicated application process and prolix documents filling. Applying big data technology, Internet financial institutions can actively acquire a large number of multi-dimensional customer information. Applicants are allowed to complete their process all online and submit less documents which can ultimately simplify the whole application procedure.

Being based on customer demand-oriented methodology is an important innovation of Internet finance. The application of big data offers the technology base for product innovation and design based on clients' perspective. Internet finance applied big data technology to customized products design and differentiated marketing campaign. Through data and behavior analysis, specific financial products can be offered to targeted customers and just satisfy their current needs. For example, there is an Internet insurance company, which uses their clients' transaction data for analysis and predicts the timeline of their future 'big events in life' based on the whole analysis. The company found that clients who will have baby born in family have greatest potential demand for life insurance products. And they also discovered that through shopping data analysis, the specific family can be easily recognized: In that kind of a family, the future moms are starting to purchase a certain type of medicine and expense related to goods for baby begins to increase. Through this meticulous analysis, customers' financial needs can be satisfied accurately and promptly.

4.2.2 Big Data Credit Investigation

Normally, Internet finance offers more service to the long tail of the population, including farmers, students, MSMEs owners, urban low-income families and other high growth population. They are excluded by traditional financial system, and are not served or not sufficiently served by traditional institutions (unbanked or underbanked). Internet financial institutions providing service to these group need to mitigate the risk of information asymmetry, and big data technology is the exact tool for breaking the boundary of asymmetrical information. Big data credit investigation fully utilizes modern digital information technique. It can eliminate information asymmetry in the credit business with a lower cost. The deficiency and absence of traditional credit information can be compensated by big data through the usage of massive and multidimensional alternative information and data. By increasing the breadth, accuracy, and immediacy of information content, big data credit investigation mitigates the shortcomings of single dimension and little information which is the features of traditional way, and further realizes a comprehensive 'holographic' portrait of customer credit situation. Meanwhile, big data credit investigation also overcomes the obstacles caused by 'Information Island'. There are different expression forms of 'Information Island', but the fundamental reason is that data are stored in diverse sectors with distinct formats and structures of storage, which leads to the isolation of information between each sectors and separation between data from different sectors. Big data credit investigation breaks barriers between insolated sectors and increases the value of information. Furthermore, expansion of credit coverage in society will help form a well social atmosphere. By enhancing the restraint of reputation mechanism on borrowers, social credit risks can be better controlled.

Financial transactions and public record information are the majority resources of traditional credit reporting. The features of the traditional way are that information usually originates from offline activities and founds on borrowing and lending, and the credit model may contain tens or hundreds of variables. From the perspective of the Internet, traditional credit investigation can also be called offline credit investigation. On the contrary, big data credit investigation takes abundant information into account, including huge data both online and offline from various resources. Taking CreditEase Big Data Financial Cloud as an example, the system processes millions PB (Peta Bytes)[2] of data per day. The data include users' forum posts, Internet footprint, social network information, relationship network and others, and as to e-commerce business owners, more data will be used, such as inventory information, the sale transaction records, clients' comments and so on (see Table 4.1).

The process of big data credit investigation can be summarized as three procedures and two types of variables. The three procedures are data processing, variable generating, and credit modeling, respectively. The two types of variables refer to weak variable and strong variable generated through data processing, respectively. From data processing to variable generating,

Table 4.1: Big data credit investigation vs. Traditional credit investigation.

Item	Big data credit investigation	Traditional credit investigation
Data Source	various data from both online and offline	borrowing offline and performance data
Data Type	transactions, social behaviors, online activities, traditional credit history, public records	borrowing history, utilities payments, fines
Data Feature	fragmental, lifestyle, reflecting character, and psychology of people, dynamic information	strong financial properties, static information
Data Format	massive unstructured data, structured data	structured data
Model Technique	relative dynamic	relative static
Credit Rating Methodology	using real-time behavior to reflect the relative stable probability of default can prospectively predict the possibility of performance, risk-based pricing	using credit record history to predict current creditworthiness, lagging in inferring credit performance
Population Coverage	population with enough Internet footprint	population with credit records (debit cards, credit cards, utilities payments, etc.)
Application Scenario	any scenarios with credit performance in life	financial activities

Source: China Finance 40 Forum, Center for Microfinance Initiatives & Network of RUC

firstly the financial information, utilities payments, and other traditional data resources are processed for acquiring strong variable. Secondly, through cleaning and processing of personal basic information, online footprint, and other alternative data, a portrait of individual is created and weak variables are generated. The amount of weak variables can be as many as tens of thousands, and even hundreds of thousands sometimes. Compared to the strong variables which are widely used in traditional credit investigation, those weak variables are not as effective as strong variables when used alone. Whereas, a large quantity of weak variables will be enough to portray an individual, depicting his/her preference, habits, behavior patterns, and other description information. Taking these numerous weak variables into account, comprehensive evaluation results can be more precise than only rating with few strong variables. Finally, rearrange those weak variables into strong variables on the basis of correlation. In the phase of credit modeling, import the generated strong variables into several models which are independent and built with different machine learning algorithms for final process. Then use the result from each data model to calculate the weighted composite credit scores in the end.

The crucial phase of big data credit investigation is to 'portray' the targeted individual. For example, when the portrait of an individual is precisely completed, we will be able to recognize every and each status continuously, dynamically, and broadly, during the whole life cycle, and further we can tell any changes when happening. During the course of 'portray', data including demographic and online behaviors are usually used. The demographic data contains gender, age, phone number, address, company, education, occupation, etc. The online behavior data contains online consumption, online reading, hotel booking, flights, images, audio, video, etc. The relative dynamic modeling approach allows any changes of information used become new information resource and be utilized for credit rating. Through active data acquisition and constant information update, big data credit investigation can improve the hysteresis of traditional credit rating. Full-cycle dynamic risk control makes risks more controllable. Big data credit investigation has strong capacity in handling unstructured data. The current very popular NLP (Natural Language Processing) technique allows information stored in the format of human language also be processed into structured data which is easily applied to analysis.

4.3 Brief Introduction of CreditEase: Better Technology, Better Finance

Founded in 2006, CreditEase is a leading FinTech company in China, specializing in small business and consumer lending, as well as wealth management for high net worth and mass affluent investors. The company is supported by a range of international institutional investors, including Morgan Stanley Private Equity Asia, Kleiner Perkins Caufield & Byers, and IDG Capital Partners. It is a Standing Committee member of China's Internet Finance Industry Association and Chairman of Beijing Marketplace Lending Association. Its majority owned subsidiary Yirendai (NYSE: YRD), an online consumer finance marketplace, is listed on the New York Stock Exchange. Both businesses have their origins in its peer-to-peer lending platform in which CreditEase is the standard setting pioneer and market leader. At the end of 2015, CreditEase had established a strong service network covering 244 cities (including Hong Kong) and 93 rural regions in China (Fig. 4.1).

From the first Chinese P2P company to a leading comprehensive financial service provider, CreditEase has served over 300 million borrowing clients and nearly 800 thousand high-net-worth and mass affluent clients. Based on customer needs oriented strategy, products and services offered by CreditEase expand from P2P borrowing and lending to one-stop financing service, including leasing and mortgage, and comprehensive wealth management, including products such as PE/VC, FOFs, overseas investment and services like global assets allocation and immigration consulting, etc. CreditEase provides customers with diverse lending and wealth management advisory services via the Internet and mobile applications. Building vast sets of "big data" capturing, managing, querying and utilizing the data to construct a world

www.elsevierdirect.com



Figure 4.1: Nationwide service network across China.

class, open financial cloud platform, it now accurately provides target customers with customized products and asset allocation services. Not only does this reduce risks and improve the safety of funds and flow efficiency, but also provides users with flexible and targeted integrated financial solutions (Fig. 4.2).

Four years ago, CreditEase launched one of its subsidiaries Yirendai, which was listed on NYSE and held the first IPOs of a Chinese P2P company in December 2015, and started the online transition. This company applied big data technology to credit scoring and anti-fraud. Through massive alternative data analysis processed automatically by system, credit facility can be reached as soon as in 10 minutes. The system developed in-house by CreditEase is called CreditEase Financial Cloud Ecosystem. CreditEase uses alternative data sources, like e-commerce, phone bill data points, bank card, and credit card, and social media data points that borrowers are willing to share in its credit screening for loans. It also grades borrowers for risk, and applies risk-based pricing based on the borrower's risk grade. In addition, CreditEase partners with well-known e-commerce players such as eBay and Amazon to tap into its borrowers' transaction histories, and gains the capacity to conduct thorough credit verification.

www.elsevierdirect.com

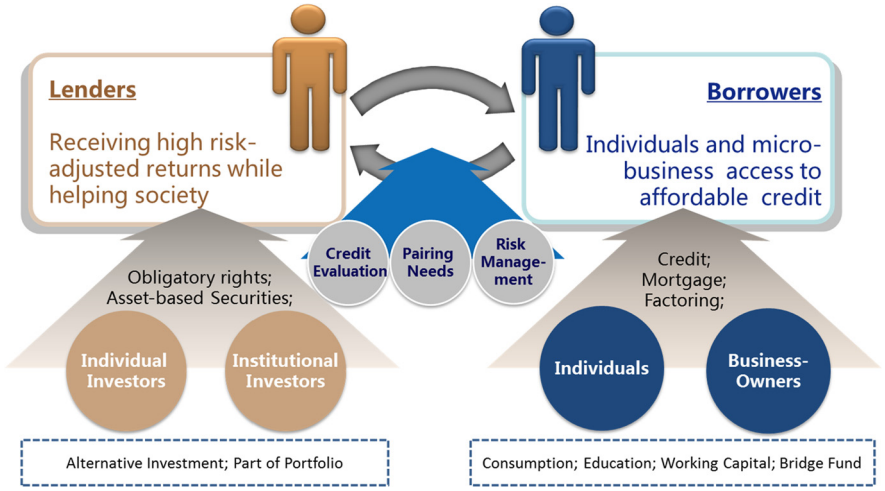


Figure 4.2: Basic business model.

With all technological support, Yirendai, two years ago, launched the world's first and now one of the most leading, in terms of loan volume, consumer borrowing mobile app for individual consumers to borrow anywhere, anytime. Technology prowess also puts this P2P lending platform in a strong position to deploy quick loans. Using CreditEase mobile apps, borrowers can get to know their credit limits as fast as in 60 seconds and complete the entire due diligence procedure within 10 minutes and in a thoroughly automatic way, which is called Speed Mode Borrowing.

Among first P2P companies caring for customer protection, CreditEase relatively early implemented capital custodian in the end of 2015 partnering with Citic bank and GuangFa bank, in order to avoid operating risks and introduce banks supervision. Meanwhile, CreditEase introduced institutional investor to diversify investing capital. Cooperating with CICC, Yirendai established Asset-Backed Securitization valued 250 million RMB in early 2016. By the end of 2015, Yirendai had originated a cumulative $1.9 billion in loans to 189 thousand borrowers.

Over the past ten years, CreditEase has accumulated the industry's largest database, which is a huge asset. While companies in the sector have not reached a consensus on whether to share their credit scores, CreditEase is working with Beijing Zhicheng Credit Service (BZCS) to build a free platform, called ZhiChengAFu, for peer-to-peer lenders, micro lenders and banks, which can use the data for free.

CreditEase offers several customized financial products for SMEs. Shangtongdai is designed for e-commerce business which allows real-time borrowing through alternative data used, including sales transactions and clients' comments, credit vetting. For small-amount equipment

purchaser, they can rent it with installment plan instead of full payment by using CreditEase leasing service. Additionally, CreditEase firstly provides innovative 'livestock leasing' in China helping rancher renting cows.

4.4 An Instance of Big Data Technology: CreditEase Financial Cloud

CreditEase Financial Cloud is a financial service cloud platform built by CreditEase company relying on cloud computation, big data, and knowledge map technology. The system has distributed computing framework, distributed storage, and virtual environment. Through data acquisition, data mining, machine learning, and rules import, the company has deployed the abstracted basic logics of finance wholly on the cloud platform, which can provide open and always accessible functions of anti-fraud, risk management, real-time loan granting, and targeted marketing to third parties (Fig. 4.3).

Using Docker container technique as the core, CreditEase Financial Cloud has built a whole set of Internet finance infrastructure platform, and each component of the financial cloud operates upon this platform. Financial cloud fully takes the advantage of Docker technology. The underlying infrastructure of the financial cloud developed in-house based on Docker technology offers a complete set framework of development, test, deployment, and monitoring, for every and each financial capacity subsystem and upper-level business application within the financial cloud system. With the support of this framework, each subsystem and application of financial cloud can quickly respond to any changes of business needs, and focus on the business logic implementation. Without having to spend a lot of time and manpower on infrastructure building, operating, and maintaining, the framework helps business reduce the cost on human resources and improve the speed of service development and the stability of service at the same time. The financial cloud has also incorporated big data platform based on Hadoop technology, in order to achieve massive data storage and parallel computing capacity. The combination of big data platform and Docker technology allows the upper layer application to easily invoke a cluster of computing power, which is the technological fundament of big data analytics. Taking the YiSou system as an example, it is an in-house developed anti-fraud system. With the utilization of the massive storage and elastic computing ability of financial cloud, YiSou system can actively acquire huge amounts of customers' online data very rapidly, conduct parallelizing arrangement and analysis, create knowledge map for business inquiries, and further provide capacity of credit granting and anti-fraud for financial business. In addition, financial cloud has implanted rich security strategies as a default feature. The feature has packed DDos defense of CreditEase, network firewall, web application firewall, authentication, network attack detection, security audit and other security strategies as a platform service. So any application deployed and operating on financial cloud will be

www.elsevierdirect.com

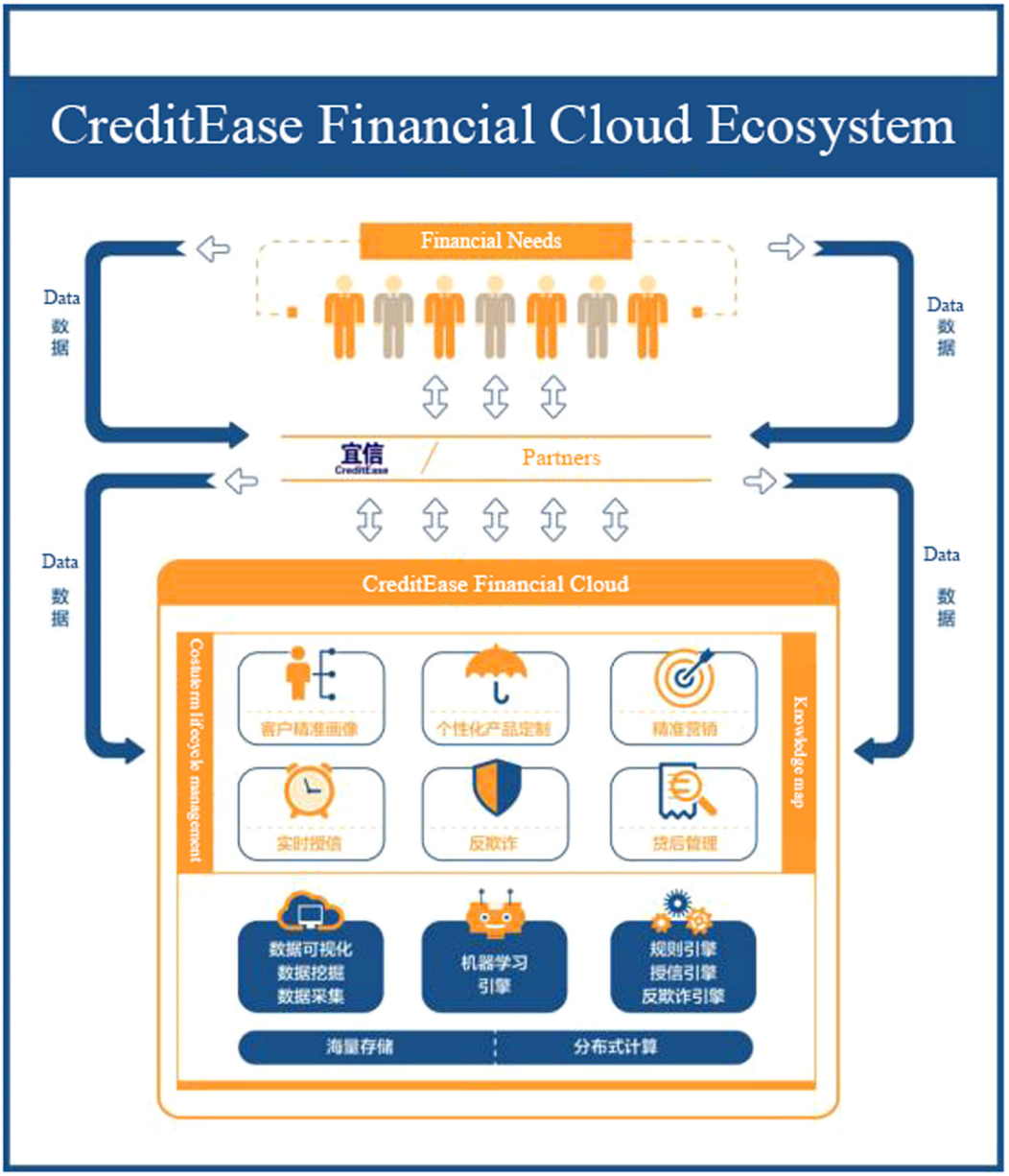


Figure 4.3: CreditEase Financial Cloud Ecosystem.

automatically protected by all the security measures without the need for additional development. Meanwhile, CreditEase Financial Cloud takes the advantage of the flexibility of Docker technology, which in conjunction with SDN (Software Defined Network) technology can re-

www.elsevierdirect.com

alize the dynamic network isolation between applications. Compared with traditional static network isolation between partitions, the new approach pushes forward the security defense line from regional boundary to the application boundary, which is capable of application level protection and safety.

CreditEase Financial Cloud has a layout of four layers consisting of cloud computation, data modeling, knowledge map, and service interfaces.

Cloud computation acts as the infrastructure for the whole system. Trough server clusters and virtualization environment, it supports the distributed computing and mass storage, guarantees the flexibility and scalability of the whole system, and offers a powerful storage and cloud computing capability.

Data modeling has three subsystems consisting of data visualization, machine learning, and rule engine. With the support of mass data acquisition and data mining, data visualization subsystem reveals the association among data and helps business operators achieve insight into data, establish and adjust related rules through visualization tools. Meanwhile, machine learning engine automatically classifies data and builds data model, and eventually offers corresponding decision rules or decision making model. Rule engine is used for the storage and organization of rules achieved through data mining and machine learning. The engine can also use imported rules set manually, and implement the basic logic of credit granting and anti-fraud.

Based on data modeling, using knowledge map technology, and combined with financial logic, the implemented modularized financial service can cover the whole life cycle of customer business, including customer accurate portrait, anti-fraud, real-time credit granting, customized product design, after sale service, precision marketing and other functions.

Service interfaces are developed for financial cloud to provide functions for externals. Institutions which have access can embed a module of CreditEase Financial Cloud and grant specific permissions for the access to corresponding customers' data, when needed. The embedded module will automatically invoke service interface and offer the required customer service and life cycle management services. In the meantime, through service interfaces, data from partner institutions can be interconnected with data on CreditEase Financial Cloud platform. Financial cloud provides service to partner institutions relying on own accumulated data. The introduced customers' data from partner institutions will be used, on one hand, for data modeling to implement specific function (such as credit granting). On the other hand, the data can help financial cloud platform optimize data model and further the platform will be capable of providing more precise service.

www.elsevierdirect.com

4.4.1 Ultra Large Data Scale

So far, CreditEase Financial Cloud has four types of data resources:

CreditEase own accumulated data is the first type, which consists of the whole process data of the company providing service to customers. The data is stored in financial cloud as precious data assets. The second type is public data collected from Internet by search engine YiSou, which is developed in-house by CreditEase. The third type is data acquired from various partners both through online and offline by CreditEase. The fourth is appropriate data authorized to CreditEase by customers, such as the credit report of customer, contacts, payrolls, bank statements, online shopping transactions, credit card statement, call history, etc.

Relying on long-term systematic data accumulation, currently CreditEase Financial Cloud system has millions of user data stored. Through the combination of powerful network search techniques and extensive partnership channels, CreditEase Financial Cloud is able to acquire daily data as large as 50 GB. Data dimensions category reaches hundreds. The number of features used to predict the customers' credit patterns has reached millions.

Another benefit when data dimensions increase to a certain scale is that data fraud can be effectively kept away. There will exist a very complex relationship between drawn conclusion and input data, when a large number of variables exists in the system and all the data is included in the calculation. So, it will be more difficult to deceive individuals or agencies through fabricating data or dressing the data.

4.4.2 Leading Data Processing Technique

The expansion of the data scale makes it more difficult to process data. That kind of difficulty includes the calculation burden caused by large volumes of data, and the professional technique required for data analysis due to large amounts of unstructured data (text, image, audio, etc.) acquired from Internet as well. CreditEase Financial Cloud applies distributed computing framework using a large number of computers together to complete the model training and model building.

Owing to the complexity and large scale of data, it is difficult to process all data with only single risk management model. Typically, multiple models are needed to work collaboratively. For example, as to the most common fraud issue in financial sector, CreditEase Financial Cloud combines a variety of models, including model based on the user's personal information for application, model based on social network of user, model based on historical transactions of user and others. Meanwhile, aiming at the characteristic that many non-linear features exist in the anti-fraud sector, CreditEase Financial Cloud utilizes various machine

learning models to automatically discover the combination of non-linear features, and improve the recognition accuracy. Through the use of multiple data sources and a variety of machine learning algorithms, the accuracy of anti-fraud prediction can be greatly raised.

4.4.3 Advance Knowledge Map Technology

CreditEase Financial Cloud is operating on the basis of knowledge map technology. The concept of knowledge map is first proposed by Google, in order to describe various entities or concepts existing in the real world. In the knowledge map, each entity or concept is a node, and has its own features and properties. Different entity or concept (node) is connected by 'relationship', and a huge net is formed as a result. So the utilization of knowledge map can help understand not only every single entity or concept, but also the relationship between entities or concepts, which can lead to the understanding of a knowledge hierarchy.

The point of CreditEase Financial Cloud using knowledge map technology is to achieve more clear description on the object through the relationship between entities. In the map, person acts as a node, and the relationship between person and environment is the line connecting two nodes. Financial cloud knowledge map integrates 'nodes' with 'lines' for an analysis, therefore to achieve a deeper and more comprehensive understanding of the person's characteristics, creditworthiness, and wealth property. When a client A comes to CreditEase for a loan, the system will make a 'portrait' of A based on the submitted personal information. And a schoolmate of A has an independent knowledge about A, which can form another 'portrait' of A. Financial cloud will calculate and achieve a more accurate portrait of A through the comparison of the two portraits, and finally offers a percentage rate of the client A's information authenticity.

4.4.4 Expert Experience and Data Closed-Loop

Even for big data risk management modeling, knowledge from financial experts plays an essential role. For example, the modeling of 'Instant Loan' starts without the delinquency data of automatical credit information. That results in the difficulty of recognizing the creditworthiness of a new client. With the support of risk management experts, corresponding experience can be introduced to the process. Trough feedback and adjustment, the precision can be improved greatly and quickly. Financial cloud system is not only relying on the automatical calculation by machine, but is also incorporating the intelligence from experienced experts.

In the meantime, system stores data of the whole business life cycle ranging from obtaining clients to loan payments, and it forms a data closed-loop. This means the risk management

Table 4.2: Delinquency rates of Yirendai.

Delinquent for	15–29 days	30–59 days	60–89 days
December 31, 2013	0.2%	0.4%	0.3%
December 31, 2014	0.3%	0.2%	0.2%
December 31, 2015	0.4%	0.5%	0.4%
March 31, 2016	0.5%	0.8%	0.5%
June 30, 2016	0.5%	0.7%	0.5%

Source: FORM 6-K of YIRENDAI LTD. for the month of August 2016

model based on AI (Artificial Intelligence) is capable of self-adjustment ability, and can automatically make adjustment and optimization on models and rules through feedbacks. When the risk management model recognizes a client, it does as a well-qualified client at first, but this client defaults on loan repayments afterwards. The risk management model will learn from this customer case and adjust itself. Thanks to data closed-loop, the performance of models will improve with time passing and data accumulation.

4.5 Cases and Application Scenarios for CreditEase Financial Cloud

CreditEase Financial Cloud has various application scenarios. Any existing scenarios needs for borrowing, credit granting, or credit validation can acquire corresponding service through the financial cloud platform.

As the wholly owned subsidiary of CreditEase, Yirendai (NYSE:YRD) is a leading online consumer finance marketplace in China connecting investors and individual borrowers. The Company was listed on the New York Stock Exchange in December 2015 and has facilitated over RMB 12.0 billion in loans from our inception in March 2012 through December 31, 2015.

With the support of CreditEase Financial Cloud, Yirendai developed in-house the 'Speed Mode' loan application, which grants applicants loan as fast as in 10 minutes. And the risk is well controlled (see Table 4.2).

Yirendai has an industry leading risk management system with proprietary credit decision and fraud detection modules. The Company accumulates data from its expanding borrower base and CreditEase's extensive database to continually enhance the sophistication and reliability of its risk management system. Yirendai's proprietary risk management system enables the Company to assess the creditworthiness of borrowers more effectively in a market where reliable credit scores and borrower databases are still at an early stage of development. This system also enables the Company to appropriately price the risks associated with borrowers and offer quality loan investment opportunities to investors.

4.5.1 E-Commerce Platform Cooperation

In September 2014, based on CreditEase Financial Cloud ShangTongDai was released. It mainly serves e-commerce owners on e-Bay platform. After several months, the service became covering the whole ecological chain in foreign trade business. ShangTongDai cooperates with e-Bay mainly focusing on the sharing of client flow and data, and combination and expansion of services. E-Bay platform opens the interface API (Application Programming Interface). With the authorization from e-commerce shop owners, financial cloud can quickly acquire the appropriate transaction information, account statements and other information, and instantly determine the line of credit for that shop owner. The owner can receive credit funds in no time, once the contract signed online.

Based on the real-time credit granting provided by CreditEase Financial Cloud, ShangTongDai has expanded its service to four core platforms of foreign e-commerce trade: trading platform, ERP software users, payment platform, and warehousing and logistics platform. ShangTongDai has offered credit to thousands of e-commerce sellers, and the cooperation with ERP software providers makes ShangTongDai form one-stop financial service. ShangTongDai has cooperated with tens of warehousing and logistics companies and payment platforms. Every week there are new platforms joining the cooperation.

4.5.2 ERP (Enterprise Resource Planning) Software Platform Cooperation

ERP software providers have access to a lot of customer information. This information typically is only used for software optimization and update. The cooperation with CreditEase Financial Cloud can allow software users to borrow relying on their ERP business data. The business owners can satisfy funds needed through the embedded service and get financed online instantly.

4.5.3 Car Rental by Credit

Car rental companies usually ask for large amounts of deposit for safety. However, this can be the obstacle in the process of renting a car. With embedded financial cloud service, clients can have credit checked only with submission of simple personal information. Car rental companies can receive the credit status of a specific client through the real-time credit granting service provided by CreditEase Financial Cloud, and the line of credit granted to the client will be used to pay the deposit.

www.elsevierdirect.com

4.5.4 Instant Installments

Without credit card, normally it is impossible to make installments plan when shopping in a mall and purchasing expensive items. CreditEase Financial Cloud can provide a new approach for client making installment payments. Only relying on digital data and materials such as online shopping transaction records, personal information and other online information, the financial cloud can provide a line of credit instantly, which will not impact the customers' experience.

References

Arcand, Louis, Berkes, Enrico, Panizza, Ugo, 2012. Too Much Finance?. IMF Working Paper 12 (161).
Beck, T., Levine, R., Loayza, N., 2000. Finance and the sources of growth. Journal of Financial Economics 58 (1), 261–300.
Goldsmith, Raymond, 1999. Financial Structure and Development. Yale University Press, New Haven, CT.
Easterly, William, Islam, Roumeen, Stiglitz, Joseph, 2000. Shaken and stirred. Explaining growth volatility. In: Annual World Bank Conference on Development Economics.
King, Robert, Levine, Ross, 1993. Finance and growth: Schumpeter might be right. The Quarterly Journal of Economics 108 (3), 717–737.
Levine, Ross, Zervos, Sara, 1996. Stock market development and long-run growth. World Bank Economic Review 10 (2), 323–339.
Lin, YiFu, Sun, Xifang, Jiang, Ye, 2009. On the theory of optimal financial structure in economic development. Economic Research Journal (8), 45–49.
Schumpeter, J., 1912. The Theory of Economic Development. Harvard University Press, Cambridge, MA.
Schumpeter, J., 1934. The Theory of Economic Development: An Inquiry Into Profits, Capital, Credit, Interest, and the Business Cycle. Transaction publishers, Piscataway, NJ.

Notes

1. For definitions, disclaimers, and methodology, please refer to http://www.internetworldstats.com/. Internet World Stats collects Internet usage information from data published by Nielsen Online, by the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. The exact number of Internet users is 3,675,824,813.
2. 1 PB = 1024 TB (Tera Byte) = 1024 × 1024 GB (Giga Byte).

www.elsevierdirect.com

CHAPTER 5

Trust Management in Mobile Platforms

Zheng Yan, Yanxiao Cheng, Ping Yan, Robert H. Deng

Contents

5.1 Introduction 84

5.2 Trust, Trust Modeling, and Trust Management 85

5.2.1 Perspective of Trust and Its Characteristics 85

5.2.1.1 Perception of Trust Concept *85*

5.2.1.2 Factors That Influence Trust *86*

5.2.1.3 Characteristics of Trust *87*

5.2.2 Trust Modeling 88

5.2.2.1 Taxonomy of Trust Models *88*

5.2.2.2 Trust Evaluation Technologies *88*

5.2.3 Trust Management and Its Main Technologies 94

5.2.4 Trusted Computing 95

5.2.5 Reputation Systems 96

5.2.6 Hybrid Trust Management Solution 96

5.3 Trust Management in Mobile Platforms 97

5.3.1 Mobile Trusted Computing Platform 97

5.3.1.1 Mobile Computing Platform *97*

5.3.1.2 Trusted Computing Platform *97*

5.3.1.3 Mobile Trusted Computing Platform *98*

5.3.1.4 Perspectives of MTCP *99*

5.3.2 Trust Management on Mobile Software Components 99

5.3.2.1 Trust Challenges of Mobile Software Components *99*

5.3.2.2 Existing Trust Models of Components Based Software System *100*

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00005-X
Copyright © 2018 Elsevier Inc. All rights reserved.

5.3.2.3 Autonomic Trust Management for a Component-Based Software System 101
5.3.3 Trust Evaluation on Mobile Applications 102
5.3.3.1 Challenges of Mobile Application Trust Management 102
5.3.3.2 Existing Trust Evaluation Models of Mobile Applications 103
5.3.3.3 A Trust-Behavior-Based Reputation System for Mobile Applications: TruBeRepec 104
5.3.4 Mobile Malware Detection 106
5.3.4.1 Evolution and Classification of Malware 106
5.3.4.2 Malware Detection and Analysis 107
5.4 Further Discussions 109
5.4.1 Open Issues and Challenges 109
5.4.2 Future Research Trends 110
5.5 Conclusions 110
Acknowledgments 111
References 111

5.1 Introduction

Trust plays a crucial role in our social life to facilitate coordination and cooperation for mutual benefits. The concept of trust has been studied in disciplines ranging from economics to psychology, from sociology to medicine, and to information science. It is hard to say what trust exactly is because it is a multidimensional, multidiscipline and multifaceted concept. We can find various definitions of trust in the literature. Common to these definitions are the notions of confidence, belief, faith, hope, expectation, dependence, and reliance on the goodness, strength, reliability, integrity, ability, or characters of a person or thing (Yan, 2013). Generally, a trust relationship involves two parties: a trustor and a trustee. The trustor is the person or entity that holds confidence, belief, faith, hope, expectation, dependence, and reliance on the properties of another person or thing, which is the object of trust – the trustee.

With the rapid growth of global digital computing and networking technologies, trust becomes an important aspect in the design, establishment and maintenance of a secure computing system and a mobile system. The traditional legal framework is not able to provide the needed trustworthiness for digital entities in an electronic transaction and remote collaboration. Managing trust relationships has become critically important in the development

of a digital system, especially in a mobile computing platform. A computing platform is a framework, either in hardware or software, which allows software to run. A typical mobile computing platform includes a mobile device's architecture, operating system, or programming languages and their runtime libraries. Generally, a mobile computing platform contains three layers: an application layer that provides features to a user; a middleware layer that provides functionality to applications; and a foundational platform layer that includes the OS and provides access to lower-level hardware. For a mobile computing platform, trust management has been proposed as a useful solution to break through new challenges of security and privacy caused by the special characteristics of these systems, such as dynamic topology and mobility. In addition, the growing importance of the third-party software in the domain of component software platforms introduces special requirements on trust. Particularly, the system's trustworthiness is varied due to component joining and leaving. How to manage trust in such a platform is crucial for embedded devices, such as mobile phones.

This chapter introduces the basic knowledge of trust, trust modeling and trust management. We review some basic technologies of trust management in mobile platforms, which include trust evaluation on mobile applications, mobile trusted computing platform, trust management on mobile software components, and mobile malware detection. Further discussions on open research issues and future research trends on mobile platforms trust management are also provided. Finally, we conclude the chapter in the last section.

5.2 Trust, Trust Modeling, and Trust Management

This chapter introduces various perspectives of trust in different disciplines, specific trust characteristics, trust influencing factors, and the technologies of trust modeling and trust management.

5.2.1 Perspective of Trust and Its Characteristics

5.2.1.1 Perception of Trust Concept

We can find various definitions of trust in the literature. For example, it can be loosely defined as a state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk (Boon and Holmes, 1991). Gambetta (2000) defined trust as trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such an action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects

www.elsevierdirect.com

[our] own action. Mayer, Davis, and Schoorman (1995) defined trust as the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.

Trust is expressed in various ways in different contexts and technology areas. Herein, we list a number of examples.

- On-line trust: On-line trust is an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited (Corritore et al., 2003).
- Agent trust: In a multi-agent system, trust is a subjective expectation an agent has about another agent's future behavior (Mui, 2003).
- Software trust: In the area of software engineering, trust is accepted dependability in a software system (Avizienis et al., 2004).
- MANET trust: For a Mobile Ad Hoc Network (MANET), trust was defined as the reliability, timeliness, and integrity of message delivery to the intended next-hop of a node (Liu et al., 2004).
- Internet application trust: Regarding Internet applications, trust is a qualified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a special context (Grandison and Sloman, 2000).

Overall, researchers have defined trust in many different ways. Common to these definitions are the notions of confidence, belief, faith, hope, expectation, dependence, and reliance on the goodness, strength, reliability, integrity, ability, or characters of a person or thing (Yan, 2007).

5.2.1.2 Factors That Influence Trust

Trust is highly related to security, but it is not true that trust is security. Trust relates many factors, such as goodness, strength, reliability, availability, integrity, ability, or other characters of an entity. The concept of trust covers a bigger scope than security, thus it is more complicated to establish, ensure and maintain, in short manage trust than security.

Another important concept related to trust is privacy. The term privacy denotes the ability of an entity to determine whether, when, and to whom information about itself is to be released or disclosed (Yan and Holtmanns, 2008). In our social life, private information should be shared in order to gain trust. With trust, people are willing to share or reveal personal information. A trustworthy digital system should firstly preserve its users' privacy. Trust is beyond and will enhance system security and personal privacy.

Trust is also impacted by context, so its influencing factors could be different in different situations. Despite the richness of the trust concept, we can still summarize the subjective and objective factors that are relevant to a decision of trust, as shown in Table 5.1.

Table 5.1: Factors influencing trust.

Trustee's objective properties	competence; ability; security; dependability; integrity; predictability; reliability; timeliness; (observed) behavior; strength
Trustee's subjective properties	honesty; benevolence; goodness
Trustor's objective properties	assessment; a given set of standards; trustor's standards
Trustor's subjective properties	confidence; (subjective) expectations or expectancy; subjective probability; willingness; belief; disposition; attitude; feeling; intention; faith; hope; trustor's dependence and reliance
Context	situations entailing risk; structural; risk; domain of action; environment (time, place, involved persons), purpose of trust;

Trust is related to the context and both the trustee and the trustor's objective properties and subjective properties. It is subjective because acceptably sufficient trust levels differ for each entity. It is also dynamic, affected by many factors. It can further develop and evolve due to good experiences, but could decay quickly due to bad impacts. From the digital system point of view, trust is an assessment of the trustee based on the trustor's criteria and a number of trust attributes.

5.2.1.3 Characteristics of Trust

Rousseau, Sitkin, Burt, and Camerer (1998) observed considerable overlap and synthesis in contemporary scholarship on trust. Particularly, the most common characteristics of trust, which play as the important guidelines for trust modeling, are:

- Trust is directed: trust is an oriented relationship between the trustor and the trustee. Entity A trusts Entity B doesn't mean B trusts A.
- Trust is subjective: Trust is considered a personal and subjective phenomenon that is based on various factors or evidence, and that some of those may carry more weight than others. Trust is different for each individual in a certain situation (Grandison and Sloman, 2000).
- Trust is context-dependent: Trust is a subjective belief about an entity in a particular context.
- Trust is measurable: A trust value can be used to represent the different degrees of trust an entity may have in another.
- Trust depends on history: Past experience may influence the present level of trust.
- Trust is dynamic: Trust is usually non-monotonically changed with time. It may be refreshed or revoked periodically, and must be able to adapt to the changing conditions of the environment in which the trust decision is made.

www.elsevierdirect.com

- Trust is conditionally transferable: Information about trust can be transmitted/received along a chain (or network) of recommendations. If Entity A trusts B and B trusts C, most possibly A could trust C under a certain condition.
- Trust can be a composite property: "trust is really a composition of many different attributes: reliability, dependability, honesty, truthfulness, security, competence, and timeliness, which may have to be considered depending on the environment in which trust is being specified" (Grandison and Sloman, 2000, p. 3). Trust is not only established based on the personal experiences of a trustor, but also greatly impacted by the recommending opinions on a trustee provided by other entities that are trusted by the trustor.

5.2.2 Trust Modeling

The method to specify, evaluate, set up, and ensure trust relationships among entities is the trust model (Yan and Holtmanns, 2008). The trust model aids the digital processing and controlling of trust. Most existing trust models are based on the understanding of trust characteristics, accounting for factors influencing trust. Current work covers a wide area including ad hoc networks, ubiquitous computing, Peer-to-Peer (P2P) systems, multi-agent systems, web services, e-commerce, component software, and so on (Yan and Holtmanns, 2008). Translation of trust concept into a machine readable and understandable language is the main objective of trust modeling.

Modeling trust in a digital manner is crucial for autonomic trust management in order to sustain dynamically changed trust relationships in a digital system. However, there are many challenges to establish a trust relationship in a mobile computing platform that relates more aspects and issues than in the social world. This is because communications in a mobile computing network rely on not only relevant human beings and their relationships, but also digital components. On the other hand, visual trust impression is missing and need somehow to be compensated. Additionally, it is more difficult to accumulate accurate information for trust assessment. The mapping of our social understanding of trust into the digital world and the creation of trust models that are feasible in practice is challenging.

5.2.2.1 Taxonomy of Trust Models

Trust models can be classified into various categories according to different rules or criteria. Table 5.2 shows the taxonomy of trust models and examples of each category.

5.2.2.2 Trust Evaluation Technologies

The main application of trust modeling is trust evaluation, especially evaluating trust in a digital manner. Trust evaluation is a technical approach of representing trust for digital processing, in which the factors influencing trust will be evaluated by a continuous or discrete

www.elsevierdirect.com

Table 5.2: Taxonomy of trust models.

Criteria of classification	Categories		Examples
Based on the description method	Models with linguistic description		Blaze et al. (1996); Tan and Thoen (1998)
	Models with graphic description		Reiter and Stubblebine (1998)
	Models with mathematic description		Xiong and Liu (2004); Sun et al. (2006)
Based on modeled contents	Single-property modeling		Xiong and Liu (2004); Sun et al. (2006)
	Multi-property modeling		Zhou et al. (2005); Wang and Varadharajan (2005); Yan and Prehofer (2011)
Based on the expression of trust	Models with binary ratings		
	Models with numeral ratings	Continuous ratings	Maurer (1996); Xiong and Liu (2004); weighted voting methods; Bayesian inference methods
		Discrete ratings	Liu et al. (2004)
Based on the dimension of trust expression	Models with a single dimension		Maurer (1996); Xiong and Liu (2004)
	Models with multiple dimensions		Theodorakopoulos and Baras (2006); Jøsang (1999); Yan et al. (2012)
Based on the trusting objects	System trust model		Yan and Prehofer (2011)
	Human trust model		Muir (1994); Muir and Moray (1996)
	Individual trust model		Yan et al. (2013); Li et al. (2004); McKnight et al. (2002)
	Institutional trust model		McKnight et al. (1998); Bigley and Pearce (1998); Mayer et al. (1995)
Based on the development of trust	Initial trust model		McKnight et al. (2002); Li et al. (2004)
	On-going trust model		Yan, Zhang and Deng (2012); Yan et al. (2013)

real number, referred to as a trust value. In the rest of this section, we briefly introduce a number of promising theories or techniques for trust evaluation.

Weighted Voting

Trust in an object or event is evaluated based on the votes from many entities. As its name implies, Weighted Voting (WV) sums up all the votes v_k on the object with each vote weighted by the corresponding trust level of the voter T_k to output the combined trust level of the object/event T:

$$T = \frac{1}{K} \sum T_k v_k \tag{5.1}$$

www.elsevierdirect.com

It should be noted here that decisions on composite objects/events are harder to be performed with this technique since it does not provide formalisms for handling unions and intersections of objects/events (Yan, 2010a). The weighted voting cannot overcome attacks raised by malicious voters to collaboratively frame good objects and/or boost bad ones. It cannot reflect the impact of the number of votes on the trust evaluation.

Bayesian Inference

Among the data fusion techniques, Bayesian Inference (BI) is often used for trust evaluation (Pearl, 1988). In BI, the combined trust level corresponding to event α_i is the posterior probability of α_i given new evidence $e = \{e_1^j, e_2^j, e_3^j, ..., e_k^j\}$; it is expressed in terms of the prior probability $P[\alpha_i]$ using the Bayes' theorem:

$$p[\alpha_i/e] = \frac{P[\alpha_i]\prod_{k=1}^{K} P[e_k^j/\alpha_i]}{\sum_{h=1}^{I}(P[\alpha_h]\prod_{k=1}^{K} P[e_k^j/\alpha_h])}, \tag{5.2}$$

where we assume that evidence is independent for the sake of mathematical tractability. The computation of posterior probabilities for composite events γ (recall that they are unions or intersections of basic events) follows the rules of probability theory. $P[e_k^j/a_i]$ is the probability that evidence k confirms α_i, given that α_i happened. This probability is equal to the trust level of e_i^k: $T(e_k^i) = P[e_k^i/\alpha_i]$. For $j \neq i$, $P[e_k^i/\alpha_i]$ is the probability that evidence k does not confirm α_i (hence, it confirms $\overline{\alpha_i}$, the complement of α_i in Ω), given that α_i happened. Hence,

$$P\left[e_k^i/\alpha_i\right] = 1 - P\left[e_k^i/\alpha_i\right] = 1 - T\left(e_k^i\right). \tag{5.3}$$

Dempster–Shafer Theory

The Dempster–Shafer Theory (DST) is a mathematical theory of evidence (Shafer, 1976), allowing one to combine evidence from different sources and arrive at a degree of belief (represented by a belief function) by taking into account all the available evidence. The Dempster–Shafer theory is based on two ideas: the idea of obtaining degrees of belief for one question from subjective probabilities for a related question, and Dempster's rule for combining such degrees of belief when they are based on independent items of evidence. The Dempster–Shafer theory can be applied into trust evaluation by expressing the trust by combining the degrees of belief generated from the probabilities of related factors.

In DST, the lack of knowledge about an event is not necessarily a refutation of the event. In addition, if there are two conflicting events, uncertainty about one of them can be considered as supporting evidence for the other. The major difference between BI and DST is that the latter is more suitable for cases with uncertain or no information. More precisely, in DST a node can be uncertain about an event, unlike in BI where a node either confirms or refutes the

www.elsevierdirect.com

event. For example, if an entity A confirms the presence of an event with probability p, in BI it refutes the existence of the event with probability $1 - p$. In DST, probability is replaced by an uncertainty interval bounded by belief and plausibility. Belief is the lower bound of this interval and represents supporting evidence. Plausibility is the upper bound of the interval and represents non-refuting evidence. Hence, in this example, entity A has p degree of belief in the event and 0 degree of belief in its absence. In DST, the frame of discernment contains all mutually exclusive possibilities related to an observation. Hence, in our context, it is the set Ω defined previously. The belief value corresponding to an event α_i and provided by evidence k is computed as:

$$b_k(\alpha_i) = \sum_{q:\alpha_q \subset \alpha_i} m_k(\alpha_q), \tag{5.4}$$

which means it is the sum of all basic belief assignments $m_k(\alpha_q)$, α_q being all basic events that compose the event α_i. In this case, only $\alpha_q \subset \alpha_i$ and hence $b_k(\alpha_i) = m_k(\alpha_i)$.

The plausibility value corresponding to event α_i represents the sum of all evidence that does not refute α_i and is computed as:

$$p_k(\alpha_i) = \sum_{r:\alpha_r \cap \alpha_i \neq 0} m_k(\alpha_r). \tag{5.5}$$

Belief and plausibility are related by $p(\alpha_i) = 1 - b(\overline{\alpha_i})$. The combined trust level corresponding to event α_i is the belief corresponding to α_i:

$$T_i = b(\alpha_i) = m(\alpha_i) = \oplus m_k(\alpha_i), \quad (k = 1, \ldots, K), \tag{5.6}$$

where pieces of evidence can be combined using Dempster's rule for combination.

$$m_1(\alpha_i) \oplus m_2(\alpha_i) = \frac{\sum_{q,r:\alpha_q \cap \alpha_r = \alpha_i} m_1(\alpha_q) m_2(\alpha_r)}{1 - \sum_{q,r:\alpha_q \cap \alpha_r = \varphi} m_1(\alpha_q) m_2(\alpha_r)}. \tag{5.7}$$

Herein, the basic belief assignment that confirms α_i is equal to the trust level of $e_i^k : T(e_i^k) = m_k(\alpha_i)$. For composite events γ, belief can be computed similarly using the above equations.

Raya et al. (2008) evaluated evidence with corresponding trust levels using weighted voting, Bayesian inference, and Dempster–Shafer theory. Simulation results show Bayesian inference performs best when prior knowledge about events is available whereas Dempster–Shafer theory handles properly high uncertainty about events.

Subjective Logic

Subjective Logic (SL) was introduced by Jøsang (2001). Trust valuation can be calculated based on Subjective Logic which expresses trust with multiple dimensions: belief, disbelief

www.elsevierdirect.com

and uncertainty. An entity can collect the opinions about other entities both explicitly via a recommendation protocol and implicitly via limited internal trust analysis using its own trust base. It is natural that the entity can perform an operation in which these individual opinions can be combined into a single opinion to allow a relatively objective judgment about another entity's trustworthiness. It is desirable that such a combination operation shall be robust enough to tolerate situations where some of the recommenders may be wrong or dishonest. Another situation with respect to trust valuation includes combining the opinions of different entities on the same entity together using a Bayesian Consensus operation; aggregation of an entity's opinions on two distinct entities with logical AND support or with logical OR support.

Subjective Logic mainly supports the operations between two opinions. It doesn't consider how to directly support context, such as time-based decay, interaction times or frequency; trust standard/policy, like importance weights of different trust factors; popularity, etc. Concretely, how to generate opinions on recommendations based on credibility and/or similarity and how to overcome attacks on trust evaluation are beyond the theory of SL. These need to be further developed in real practice.

Semiring

Semiring was introduced by Theodorakopoulos and Baras (2006). The authors view the trust inference problem as a generalized shortest path problem on a weighted directed graph $G(V, E)$ (trust graph). The vertices of the graph are the users/entities in the network. A weighted edge from vertex i to vertex j corresponds to the opinion that the trustor has about the trustee. The weight function is $l(i, j) : V \times V \rightarrow S$, where S is the opinion space. Each opinion consists of two numbers: the trust value, and the confidence value. The former corresponds to the trustor's estimate of the trustee's trustworthiness. The latter corresponds to the accuracy of the trust value assignment. Since opinions with a high confidence value are more useful in making trust decisions, the confidence value is also referred to as the quality of the opinion. The space of opinions can be visualized as a rectangle $(ZERO_TRUST, MAX_TRUST) \times (ZERO_CONF, MAX_CONF)$ in the Cartesian plane $(S = [0, 1] \times [0, 1])$. Using the theory of Semirings, two nodes in an ad hoc network can establish an indirect trust relation without previous direct interaction. The semiring framework is also flexible to express other trust models.

Generally, two versions of the trust inference problem can be formalized in an ad hoc network scenario. The first is finding the trust-confidence value that a source node A should assign to a destination node B, based on the intermediate nodes' trust-confidence values. Viewed as a generalized shortest path problem, it amounts to finding the generalized distance between nodes A and B. The second version is finding the most trusted path between nodes A and B. That is, find a sequence of nodes that has the highest aggregate trust value among all trust

paths starting at A and ending at B. In the trust case, multiple trust paths are usually utilized to compute the trust distance from the source to the destination, since that will increase the evidence on which the source bases its final estimate. The first problem is addressed with a "distance semiring", and the second with a "path semiring". Two operators are applied to combine opinions. One operator (denoted $\otimes$) combines opinions along a path, i.e., A's opinion for B is combined with B's opinion for C into one indirect opinion that A should have for C, based on B's recommendation. The other operator (denoted $\oplus$) combines opinions across paths, i.e., A's indirect opinion for X through path p_1 is combined with A's indirect opinion for X through path p_2 into one aggregate opinion. Then, these operators can be used in a general framework for solving path problems in graphs, provided they satisfy certain mathematical properties, i.e., form an algebraic structure called a semiring.

Fuzzy Logic

Fuzzy Logic (FL) is a form of many-valued logic; it deals with reasoning that is approximate rather than exact. Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false (Novák et al., 1999).

Fuzzy Logic theory defines fuzzy operators on fuzzy sets. At present, Zadeh operators $\wedge$ and $\vee$ are commonly used to perform calculation and analysis. But they are so imprecise. Thus, several general class fuzzy operators are proposed. To adapt to different sources of uncertainties in trust management, parameterized general intersection and union operators are needed. With different values of the parameters, these operators can flexibly express trust and capture uncertainty. But for a concrete issue, the appropriate fuzzy operator may not be known. For this reason, fuzzy logic usually uses IF-THEN rules, or constructs that are equivalent, such as fuzzy associative matrices. We briefly describe how to evaluate the trust relationship between entity A and B by applying Fuzzy Logic. It contains six steps.

1. Define fuzzy set $F = \{f_1, f_2, \ldots, f_5\}$ for different levels of evaluation, e.g., $f_1 = Excellent$; $f_2 = Good$; $f_3 = Average$; $f_4 = Bad$; $f_5 = Risky$;
2. Justify hierarchical trust factors that influence A's trust in B: the main factors and their sub-factors. For example, for e-commerce transactions, main factors influencing trust could be security technology, vender brand, and customer factor. For the main factor security technology, it contains such sub-factors as payment method, security techniques, and system availability;
3. Determine different weights for every hierarchical trust factors based on A's policy. Suppose the weight's set of first hierarchical trust factors (i.e., main factors) is $W = \{0.5, 0.3, 0.2\}$ and the weights' sets of second hierarchical trust factors (i.e., sub-factors) are $W_1 = \{0.6, 0.2, 0.2\}$, $W_2 = \{0.6, 0.2, 0.2\}$, $W_3 = \{0.6, 0.2, 0.2\}$;
4. Use statistical way of fuzzy to calculate the degree of second hierarchical trust factors to the set f_i $(i = 1, 2, \ldots, 5)$;

www.elsevierdirect.com

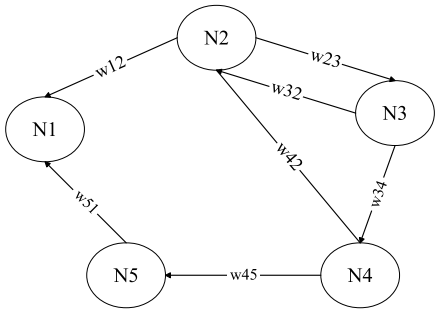


Figure 5.1: An example of fuzzy cognitive map.

5. Make trust evaluation with suitable fuzzy logic operators;
6. Generate unitary representation of evaluation on main factors and trust.

Fuzzy Cognitive Maps

A Fuzzy Cognitive Map is a combination of Fuzzy Logic and Neural Networks (Kosko, 1986). In a graphic illustration, FCM is a sign-directed graph with feedback, consisting of nodes and weighted arcs. A FCM can be used for evaluating trust. In this case, the concept nodes is trustworthiness and the factors that influence trust. The weighted arcs represent influencing relationships among these factors and the trustworthiness. We can utilize it to predict the performance of different trust control mechanisms in order to select the best ones (Yan and Prehofer, 2011), as can be seen in Fig. 5.1.

The nodes take values within [0, 1] and the weights of the arcs are in the interval $[-1, 1]$. Among nodes, three possible types of causal relationships express the type of influence from one node to another. A positive weight (e.g., $w_{12} > 0$) indicates that an increase in the value of one node (N_1) leads to the increase in the value of another node (N_2), and vice versa. Negative causality (e.g., $w_{51} < 0$) signifies that an increase in the value of one node (N_5) leads to the decrease in the value of another node (N_1), and vice versa. No causality (e.g., $w_{34} = 0$) occurs when an increase or decrease in the value of one node (N_3) has no any influence on the value of another node (N_4). FCM also permits updating the construction of the graph, such as adding or deleting an interconnection or a node (Stylios, Georgopoulos & Groumpos, 1997).

5.2.3 Trust Management and Its Main Technologies

Trust management is concerned with: collecting the information required to make a trust relationship decision, evaluating the criteria related to the trust relationship, monitoring and reevaluating existing trust relationships, as well as ensuring the dynamically changed trust relationships and automating the process (Grandison and Sloman, 2000; Yan and Prehofer,

2011). Transforming from a social concept of trust to a digital concept, trust modeling and management help in designing and implementing a trustworthy digital system, especially in mobile and distributed computing.

Various trust management systems are described in the literature. Two important systems are reputation-based trust management systems and trusted computing-enhanced trust management. Trust and reputation mechanisms have been proposed in the domain of mobile and Internet computing and communications; however, most of these focus on a specific system that is very different from the others. Trusted computing-based trust management applies sound security technologies to ensure the trustworthiness of a computer or communication system. This kind of trust management has been applied not only in desktop computers, but also mobile computing platforms (Yan, 2010a). In addition, although a variety of trust models are available, the design of trust models is still at an empirical stage and can't reach the expectation to simulate social trust to a satisfying degree. Current work focuses on concrete solutions in specific systems. Seldom, the usability of trust management is considered in order to achieve usable trust management for easy user acceptance. Basically, the trust model should reflect the characteristics of trust, consider the factors that influence trust, and thus support trust management in a feasible and usable way. It becomes essential to investigate trust management in mobile computing platform to overcome these problems. The third category is a hybrid solution. It applies both the trusted computing and trust evaluation technologies to overcome the disadvantages of the above two kinds of solutions. We will discuss the advantages and disadvantages of each in the rest of this section.

5.2.4 Trusted Computing

The typical trusted computing technologies are specified in the specifications of TCG (Trusted Computing Group) (TCG, 2003), aiming to enhance the overall security, privacy and trustworthiness of a variety of computing devices. The current technologies for Trusted Computing Platform (TCP) are quite similar (Felten, 2003; England et al., 2003). The core of trusted computing technologies of TCG is Trusted Platform Module (TPM), a tamper-resistant module embedded in a platform. A TPM chip is designed to resist all software attacks and moderate hardware attacks. It encloses a non-volatile storage, a set of platform configuration registers (PCRs), and an engine for cryptographic operations. The TCG specifications define a suite of mechanisms including memory curtaining, secure I/O, secure storage, platform measurement, and remote attestation. All are based on the TPM chip and its supporting software called TCG Software Stack (TSS). As a fundamental secure computing module, it plays as the root trust module to establish security and trust in digital computing, communication and networking. Basically, it can provide secure booting and software installation, private data

www.elsevierdirect.com

protection and Digital Rights Management (DRM), as well as remote attestation based communications and collaboration.

The main functions of TCP are memory curtaining, secure storage, platform measurement, and platform attestation. Memory curtaining is a hardware-enforced memory isolation scheme to guarantee the intactness of the process execution. The sealed storage function defined by TCG can securely bind data encryption/decryption to a platform state or configuration. Platform measurement is essential to compute the states or configurations of a platform. Platform attestation is the process with which the platform measurement is signed and transported to a challenger for the purpose of checking the states of an attester platform.

5.2.5 Reputation Systems

As defined by Aberer and Despotovic (2001), reputation is a measure that is derived from direct or indirect knowledge on earlier interactions of entities and is used to assess the level of trust an entity puts into another entity. Trust and reputation mechanisms have been proposed in various fields such as distributed computing, agent technology, grid computing, economics, and evolutionary biology (Yan and Holtmanns, 2008).

Reputation schemes can be classified into three different categories depending on what sort of reputation they utilize. Global reputation is the aggregation of all available assessments by other entities that have had interactions with the particular entity, and thus it has an n-to-1 relationship. On the other hand, the local reputation of an entity is each entity's own assessment based on past history of interaction with the particular entity, thus it is a 1-to-1 relationship. This reflects the social situation that a person trusts another one. Personalized reputation is generated by aggregating all available assessments by tailoring them based on personal historical experiences.

5.2.6 Hybrid Trust Management Solution

Few hybrid trust management solutions can be found in the literature. Balakrishnan and Varadharajan (2005) demonstrated the issues that might creep out in a security design, when a cryptographic technique alone is involved. They also suggested how to counter those issues through the combination of trust management with cryptographic mechanisms. Moreover, they proposed the need to introduce the notion of heterogeneity resource management in the security design to address the divergence among the nodes, which can be taken an advantage to diminish the packet drop attacks in ad hoc networks. To handle the dynamic nature of the medium, the authors proposed that the design of secure mobile ad hoc networks should envisage including trust management as another dimension apart from the cryptographic

www.elsevierdirect.com

mechanisms. In addition, inclusion of trust management alone cannot guarantee secure communications due to some persisting issues such as packet dropping. Therefore, the resource should be also considered in order to provide a trustworthy system. Yan (2010b) presented an autonomic trust management solution for the mobile computing platforms that can support two levels of autonomic trust management: between devices as well as between services offered by the devices in the context of mobile communications, networking, and computing. This solution is based on both a trusted computing technology and an adaptive trust control model. It supports autonomic trust control on the basis of the trustor device's specification, which is ensured by a Root Trust module at the trustee device's computing platform. The solution can effectively avoid or reduce risk by stopping or restricting any potential risky activities based on the trustor's specification. To ensure trustworthy services provided by the trustee device, the adaptive trust control model is applied to ensure that a suitable set of control modes are applied based on runtime trust evaluation in the trustee device in order to provide a trustworthy service expected by the trustor.

Obviously, the hybrid solution can provide comprehensive trust management in terms of supporting multiple trust properties. It integrates the advance of both 'hard' and 'soft' trust solutions and overcomes the disadvantages of each. It can ensure initial trust and also provide intelligence on trust decision. Thus, it is a promising technology towards practical trust management. Notably, the current hybrid solutions are generally complicated. They didn't consider the concern of users and were not designed in a human-centric manner. Thereby, it cannot sufficiently support the usability property of trust.

5.3 Trust Management in Mobile Platforms

5.3.1 Mobile Trusted Computing Platform

5.3.1.1 Mobile Computing Platform

A *computing platform* is a framework, either in hardware or software, which allows software to run. A typical *mobile computing platform* includes a mobile device's architecture, operating system, or programming languages and their runtime libraries. Generally, a mobile computing platform contains three layers: an application layer that provides features to a user, a middleware layer that provides functionality to applications, and a foundational platform layer that includes the OS and provides access to lower-level hardware.

5.3.1.2 Trusted Computing Platform

A *trusted computing platform* is a computing platform that behaves in a way as it is expected to behave for an intended purpose. Trusted Computing (TC) is a technology developed and

www.elsevierdirect.com

promoted by the TCG. It is used to collectively describe technologies enabling the establishment of trust in local and remote computing systems by using trustworthy components and trust anchors, to ensure the integrity of other parts of the system. For example, the most important work about the trusted computing platform is conducted in the TCG [Tcg03]. It defines and promotes open standards for hardware enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specified technology enables more secure computing environments without compromising functional integrity, privacy, or individual rights. Basically, it encompasses several security mechanisms: Platform Integrity, Secure Storage, Isolated Execution, Device Authentication, Attestation, and Provisioning.

5.3.1.3 Mobile Trusted Computing Platform

A *Mobile Trusted Computing Platform* (*MTCP*) is a trusted computing platform that holds the property of mobility for embedded devices. For personal computers, Trusted Computing typically is interpreted to be a software architecture designed around the Trusted Platform Module (TPM). The TPM is a hardware element that serves as the fundament for the architecture that further consists of specific work in, e.g., the domain of embedded devices, trusted network access, and server security. While in embedded devices, the state-of-the art in terms of hardware security and operating systems is significantly different from what is present on personal computers. To stimulate the take-up of TCG technology on handsets, the approved Mobile Trusted Module (MTM) specification (TCG, 2003) defines new interfaces and adaptation options that match the requirements of the handset business ecosystem, as well as the hardware in use in an embedded domain. But the MTM specification significantly differs from its peer TPM specification on a few significant issues:

1) The concept of secure boot is introduced. Many embedded devices and handsets in particular are subject to regulatory approval. That in turn motivates the need for enforced integrity protection of software in fielded devices, and secure boot, i.e., a boot sequence not only measured, but also aborted on any non-approved state transition, is a vital building block for this security service;
2) The specification explicitly supports implementation of the MTM as a software functionality (with necessary hardware security support for isolation, etc.) rather than as a physical implementation in hardware. This makes it possible for device manufacturers to add the MTM as an add-on to already deployed, proprietary security solutions;
3) A reference architecture takes into account the support of several parallel MTM instances in the same device. Some may be discretionary (MTM exposed to user applications) whereas, e.g., the Device Manufacturer's MTM by definition enforces a security policy (mandatory access control). The use for parallel MTMs will become evident in a later section;

www.elsevierdirect.com

4) The MTM specification minimizes the implementation footprint (whether implemented in hardware or software) by defining only a minimal set of the TPM functionality as mandatory in the scope of MTM.

In contrast to the embedded platform solutions listed above, the TPM module by design does not provide secure boot. Instead, it supports a mechanism denoted trusted boot, which can be summarized by that the TPM ASIC does not prohibit or stop the boot-up of the device, even if the booted software is wrong or infected. With MTM, the whole architecture is based on well-defined trust roots that in turn are based on hardware mechanisms. MTM defines two interleaving profiles depending on the entity that holds ownership of the functionality: the remotely owned *Mobile Remote Owner Trusted Module* (MRTM) for system services that are remotely managed, and the user-owned *Mobile Local Owner Trusted Module* (MLTM) for the user's own data, and combining this with the possibility of running many parallel MTM engines on a platform. Intended to be used either by a device manufacturer or a carrier operator, the MTRM defines a necessary security architecture and interfaces to implement a securely booting, integrity-protected device. When it comes to the functions inherited from the TPM specification, a well-defined API to the security mechanisms exists, and is already widely adopted on PC laptops. The MTM specification bridges technology barriers and brings some TPM related services also into the mobile domain.

5.3.1.4 Perspectives of MTCP

The MTM is a security technology that likely will be available in handsets across the globe in a not too-distant future. The description of legacy platform security architectures provides an overview of what kind of enforcement and confidentiality and isolation services a handset of today typically includes on a chip level, and these services will often serve as the foundation (trust roots) of a handset MTM implementation. The main shortcomings of TPM for mobile use-cases have led to the introduction of secure boot and its supporting mechanisms in MTM. Most fundamental TPM mechanisms are also present on the MTM. With the adaption of the MTM into the embedded operating system by means of MTM hierarchies, mobile trusted computing platform era is around the corner. The MTM can bring safe mechanisms to a bright prospect of MTCP.

5.3.2 Trust Management on Mobile Software Components

5.3.2.1 Trust Challenges of Mobile Software Components

Generally, a Component Based Software System (CBSS) consists of a number of components interacting over well-defined interfaces. They are exported to applications capable of combining and using them to provide various features. Thus, common components can be effectively

www.elsevierdirect.com

shared by a number of applications. Typically, such a system allows the addition and deletion of components after deployment. Therefore, the execution of a component in relation to other system entities needs to be considered. Despite component trustworthiness in isolation, its execution could cause problems due to simultaneously sharing system resources with others or having special requirements. The dependability and security, i.e., trustworthiness of a component or a number of correlated components, is dynamically changed in such a system. Furthermore, additional influences on the system have to be considered. For example, to ensure its trustworthiness the system needs to adapt itself accordingly since currently applied trust control mechanisms could be unsuitable against some malicious behaviors or attacks.

Component-Based Software Engineering (CBSE) has many benefits regarding reuse of components and adaptation, but also introduces additional trust concerns. First, we need to ensure the trustworthiness of both isolated and correlated components in various situations. Second, the components should satisfy each other's overall trust requirements during component execution. Consequently, the component-based software system needs a mechanism to ensure performance and establish the system's trust in an autonomic way, even if the internal and external environments change. This creates the need for trust management with regard to software component installation and execution.

Assessment and management of trust is difficult in a component-based software system. First, existing work on trust evaluation is generally system specific, focusing mostly on distributed systems. Additional work is required in order to apply it to component software domains (Sun et al., 2006; Yan and Holtmanns, 2008). Second, trust is influenced by many security and dependability related factors. These factors could be treated differently by different entities (e.g., software components) in different situations due to various expectations from system users. Third, the component-based software system should effectively adapt itself to changing system context in order to ensure trust. Context is hard to comprehensively model due to its complexity, especially in a component-based software system. This introduces additional challenges for autonomic trust management with context awareness (Yan, 2007).

5.3.2.2 Existing Trust Models of Components Based Software System

Recently, trust has been recognized as an important factor for component-based software system. A number of interesting solutions have been proposed to ensure its trustworthiness. Herrmann developed a special reputation system based on the experiences of component users and a third trusted party's certificate to reduce the expense of evaluating a component (Herrmann, 2001, 2003). He applied Subjective Logic with uncertainty support to aggregate users' trust opinions and discount a recommendation with the trust value of its recommender.

Zhou et al. constructed a framework to dynamically reconfigure different qualities in CBSS from the view of trust. A five-layer trust management framework was proposed to satisfy

various QoS demands of different users. This framework provides common trust management facilities for components. It also supplies components for dynamic (re)configuration of multi trust-properties according to predefined policies. It relies on a system user to customize his/her trust evaluation function. This is usually time-consuming, user friendless, and prone to errors. In addition, based on the current system's competence this solution cannot evaluate the manageability of trust. Thus, it lacks flexibility and intelligence to predict cross-influence of various trust control mechanisms on different trust properties. In the next section we will introduce an autonomic trust management for component-based software system proposed by Yan and Prehofer (2011). It solves the problems mentioned above.

5.3.2.3 Autonomic Trust Management for a Component-Based Software System

Yan and Prehofer (2011) adopted a holistic notion of trust, which includes availability, reliability, integrity, safety, maintainability, and confidentiality, depending on the requirements of a trustor. Hence, trust is defined as the trustor's assessment on how well the observed behavior or performance, measurable by the above-specified Quality Attributes (QAs) of a trustee, meets the desired standards for an intended purpose. They developed a trust control model based on Fuzzy Cognitive Maps (FCMs), which suitably represents the causal relationships that exist among trust, its related properties (i.e., QAs), and trust control mechanisms. They assumed several trust control modes, each of which contains a number of trust control mechanisms or operations, e.g., encryption, authentication, hash code based integrity check, access control mechanisms, duplication of process, man-in-middle solutions for improving availability, etc. A control mode can be treated as a special configuration of trust management provided by the system.

They further proposed an autonomic trust management solution for component-based software systems focusing mainly on system runtime, as shown in Fig. 5.2. In this procedure, trustworthiness prediction is a mechanism to anticipate the performance or feasibility of applying control modes. It predicts the trustworthiness values supposing application of some control modes before deciding to initiate them. Trust control mode selection is a mechanism to select the most suitable trust control modes based on the prediction results. Trust assessment is conducted based on the trustor's criteria by evaluating the trustee entity's quality attributes. Particularly, the quality attributes of the entity can be controlled or improved by applying a number of trust control modes, especially at system runtime.

For a trustor, the trustworthiness of its specified trustee can be predicted by supposing that various control modes are adopted by the system. Based on the prediction results, a suitable set of control modes could be selected to establish the trust relationship between the trustor and the trustee. Furthermore, a runtime trust assessment mechanism evaluates the trustworthiness of the trustee by monitoring its behavior according to the trustor's criteria. According to

www.elsevierdirect.com

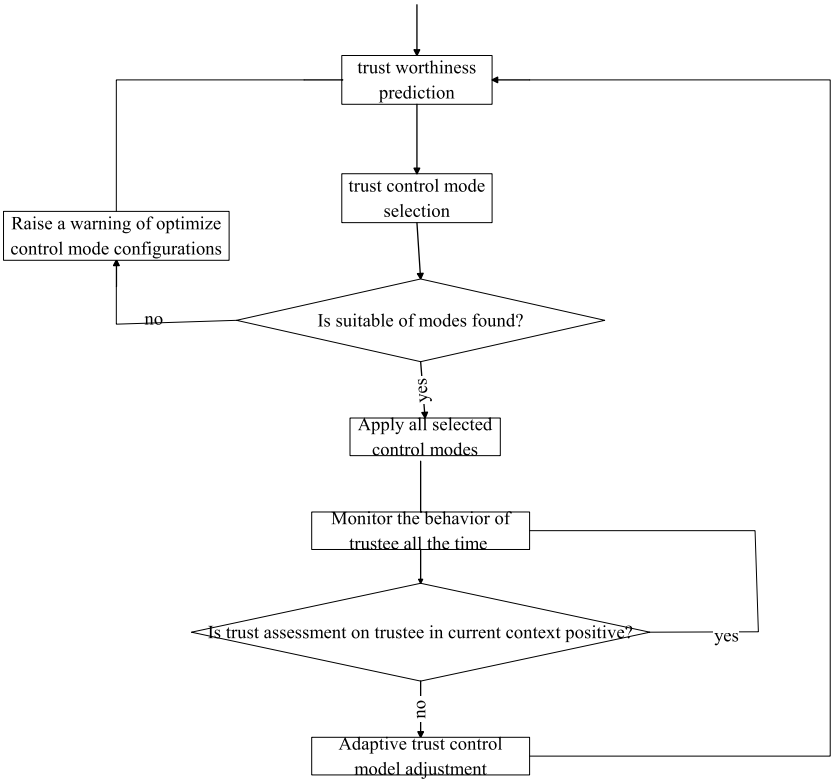


Figure 5.2: An autonomic trust management procedure at runtime.

the runtime trust assessment results in the underlying context, the system conducts trust control model adjustment in order to reflect the real system context if the assessed trust value is below an expected threshold. This threshold is generally set by the trustor to express its expectation on the assessment. Then, the system repeats the procedure. Obviously, the context-aware adaptability of the trust control model is crucial to reselect suitable trust control modes to conduct autonomic trust management.

5.3.3 Trust Evaluation on Mobile Applications

5.3.3.1 Challenges of Mobile Application Trust Management

With the vigorous development of mobile technologies, a mobile device has become an indispensable part of our social life. The mobile device is evolving as an open platform to execute various kinds of applications. Mobile applications are software packages that can be installed

www.elsevierdirect.com

and executed in a mobile device, for example, a mobile email client to access emails in a mobile phone. Generally, mobile applications developed by various vendors can be downloaded for installation.

However, mobile applications could be malicious, buggy, running unexpectedly or bringing a security hole to mobile devices. They may intrude user devices or cause bad usage experiences. Unscrupulous providers and advertisers could insert unsolicited advertisement into the mobile applications, which could even steal the personal information of the users. Due to the above reason and the sharp increase of the number of mobile applications, mobile app trust attracts special attention. Which mobile application is trustworthy for a user to purchase, download, install, execute and recommend becomes a crucial issue. Therefore, a convinced way is demanded to evaluate user trust in mobile apps and generate reputation of theirs.

5.3.3.2 Existing Trust Evaluation Models of Mobile Applications

The trustworthiness of mobile applications relates to their dependability, security, and usability (Avizienis et al., 2004), as well as popularity (Yan, Dong, Niemi & Yu, 2013). Many reputation systems of applications evaluate application trust based on the number of downloads. Obviously, this way is totally inaccurate since 26 percent of mobile apps downloaded in 2010 were used only once. In this section, we will firstly introduce several existing trust evaluation models.

Many systems rely on users to provide feedback for reputation generation, which lack considerations on the means to gather experiential evidence for effective trust evaluation. For example, the trust and reputation mechanism proposed by Pan, Feng, Xianlong & Jian is a complementary approach that analyzed collected recommendations from past users to evaluate software quality. It collects recommendations based on a user's social network and weights information according to recommenders' expectation and capability. However, it may not be appropriate or convenient to request user feedback, especially for a mobile user. This is because the user may be bothered by such a request during usage. Usage experience could be negatively influenced. Moreover, user interface design for feedback requests extra design efforts, which may cause additional challenges for mobile devices with small displayers.

Another issue is that different users may apply different scales in the feedback, which may cause confusion, even attacks. Li, Helou and Gillet proposed a trust-based rating prediction approach for recommendation in Web 2.0 collaborative learning social software. Trust network was exploited in the rating prediction scheme and a multi-relational trust metric was developed in an implicit way. The approach was evaluated using a data set of collaborative learning social software. This approach evaluated the quality of user-generated contents in an open learning environment, and therefore facilitated providing personalized recommendations and guidance.

www.elsevierdirect.com

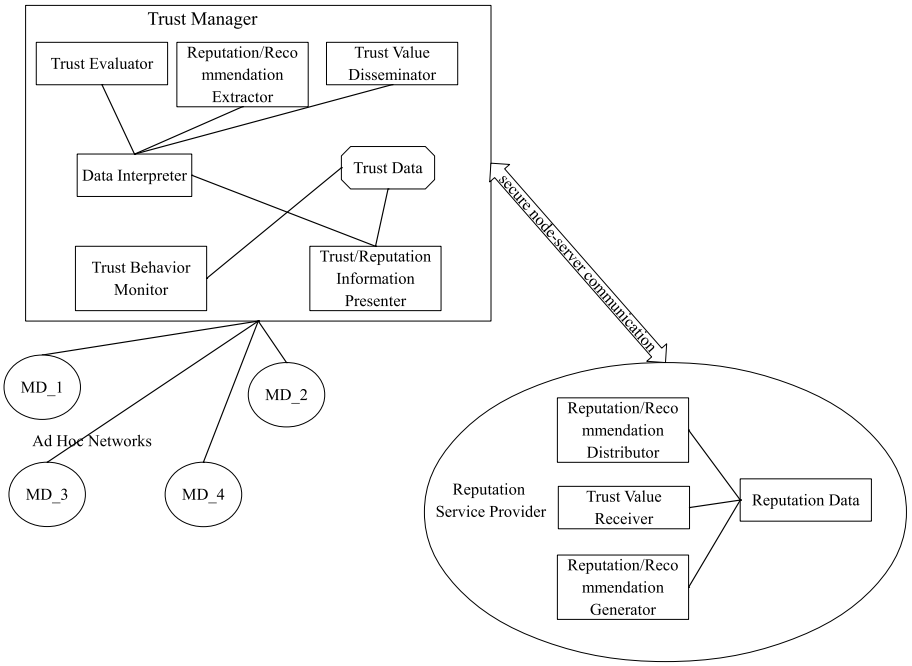


Figure 5.3: TruBeRepec system structure.

An effective method to solve these problems is observing trust behaviors directly during mobile application usage to automatically collect evidence for trust evaluation in a uniformed norm, e.g., TruBeRepec presented by Yan, Zhang and Deng (2012). It explores trust in the view of human trust behaviors and generates reputation and provides recommendations based on trust behaviors. We will briefly introduce this trust model in the next section.

5.3.3.3 A Trust-Behavior-Based Reputation System for Mobile Applications: TruBeRepec

Obviously, trust plays an important role in application consumption and usage because it helps users overcome perceptions of uncertainty and risk and engages in trust behaviors. The trust behavior is a user's actions to depend on an application or believe the application could perform as expected. However, a user's trust in a mobile application is highly subjective. It is built up over time and changes with the use of the application due to the influence of many factors.

TruBeRepec is a trust-behavior-based reputation system for mobile applications, as can be seen in Fig. 5.3 (Yan, Zhang and Deng, 2012). It is designed to overcome the challenges of existing reputation systems by providing sound usability and unifying the credibility of user

feedback. It was developed based on a model of trust behavior for mobile applications explored through a large-scale user survey.

The trust behaviors of mobile app consist of three categories:

- Using Behavior (UB) relates to normal application usage, which can be reflected mainly by elapsed usage time, number of usages, and usage frequency;
- Reflection Behavior (RB) concerns usage behaviors after a user confronts application problems/errors or has good/bad usage experiences;
- Correlation Behavior (CB) is correlated to a number of similar functioned mobile applications.

All above types of trust behaviors contribute to the generation of individual user trust in a mobile app.

The client software "Trust Manager" of TruBeRepec can be installed in a number of mobile devices (MD_k, $k = 1, \ldots, K$). The trust manager contains Trust Behavior Monitor that monitors trust behaviors and inputs statistical data about UB, RB and CB into a secure storage (Trust Data), which is located inside the device platform and has a secure channel to communicate with the behavior monitor and Trust/Reputation Information Presenter. The statistical data can be accessed by Data Interpreter for (a) individual trust evaluation regarding a specific application by Trust Evaluator; (b) data dissemination to send local trust information and vote applications to reputation service provider (RSP) or other devices by Trust Value Disseminator; (c) reputation/recommendation extraction to get mobile applications reputation information and/or application recommendations from the RSP or other devices by Reputation/Recommendation Extractor. Particularly, the Trust Evaluator can also generate application reputation and recommendation at the user's device based on collected information from other mobile devices, e.g., through an ad hoc network. The Data Interpreter is a secure mechanism to access the user's usage statistical data from the Trust Data since these data are private information. Only authorized data interpreter mechanisms can access and unseal the protected usage information. The reputation/recommendation extraction can be tailored based on the mobile user's preference, either a reputation extraction policy or a recommendation extraction policy, or both. In addition, Trust/Reputation Information Presenter is applied to show trust/reputation information to the user in order to aid his/her application usage.

In the RSP, Trust Value Receiver receives individual trust information and votes automatically or by request from the mobile devices. Reputation/Recommendation Generator generates application reputations and recommendations for mobile users. Herein, the reputation could be generated based on all users' usage statistics. But due to a privacy concern, we apply another approach to aggregate the individual trust values based on UB, RB, and CB in each mobile device and send the aggregation result to the RSP for generating application reputation and

www.elsevierdirect.com

recommendations. The reputation/recommendation information about each mobile application is saved in a secure storage (Reputation Data) in the RSP. This information can be retrieved and distributed to the mobile devices through Reputation/Recommendation Distributor. It receives reputation retrieve requests and provides application reputations and recommendations to the requestors.

5.3.4 Mobile Malware Detection

Another important aspect of trust management in mobile platform is mobile malware detection. As the mobile device market gained momentum, thousands of mobile applications have been created and distributed to users via online app stores for providing various services. The relevant security risk is the proliferation of mobile malware. In fact, the trusted computing base of mobile platforms is currently, to some extent, similar to that of applications running in desktops, opening an avenue for security breaches, which leads to the stringent security requirements.

5.3.4.1 Evolution and Classification of Malware

Adopting the definition in some literatures, we describe malware as "a generic term that encompasses viruses, Trojans, spywares and other intrusive code" that harms computing systems. Malware for smart devices has rocketed over in the past few years, evolving from relatively simple apps causing annoyance to complex and sophisticated pieces of code designed for profit, sabotage or espionage.

At beginning, by mobile malware mimicked strategies in PC malware, it was sought to inflict damage over user information or corrupt system files to compromise devices. Then the rise of featured mobile phones brought about various distinctive infection vectors, which can propagate themselves. In recent years, the high development of devices with improved sensing and networking capabilities has caused more novel threats. They monitor and exfiltrate user location data, and some other private information through compromised sensors. What's more important is that they use many methods to camouflage themselves and circumvent detection.

For a better understanding of the functionality of malware, we classify malware according to its distribution and infection feature, from self-propagation mechanisms based on vulnerabilities and misconfigurations, to tricking users into installing malware by means of social engineering.

Trojan Horses

A Trojan horse is the malware embedded by its designer in an application or a system. The application or the system appears to perform some useful function, which conducts some

unauthorized action, e.g., capturing a user's keystrokes and sending this information to a malicious host.

Viruses

A computer virus is the code that replicates by inserting itself into other programs, i.e., a virus needs an existing host program in order to cause harm. For example, in order to get into a computer system, a virus may attach itself to some software utility, and its activation relies on the launch of the host.

Worms

A worm replicates itself by executing its own code independently of any other programs. The worm spreads via network connections with the goal of infecting as many systems connected to the network as possible.

Backdoor

A backdoor is a method of secretly bypassing normal authentication in an application or a system, and then getting access to it illegally. The backdoor is often used for securing unauthorized remote access to a computer, or obtaining access to plaintext in cryptographic systems.

Botnet

A botnet is a number of Internet-connected computers communicating with other similar machines, in which components located on networked computers communicate and coordinate their actions by Command and Control (C&C) or by passing messages to one another. The botnet is used to send spam email or participates in Distributed Denial-of-Service (DDoS) attacks.

Other Categories

Undeniably, there are many other malware categories, e.g., grayware that intends to steal user information with a "kind" appearance.

5.3.4.2 Malware Detection and Analysis

The mainstream malware detection methods are classified as Static Analysis and Dynamic Analysis combined with identification methods: anomaly-based, signature-based, and specification-based identification. The Static Analysis uses disassemble technologies to decompile the application source codes to find out malicious signature codes. The Dynamic Analysis collects the application runtime data to find out whether the app executes with malicious behaviors. The taxonomy of detection techniques can be classified into three general types by combining detection and identification methods.

www.elsevierdirect.com

Anomaly-Based Detection

Anomaly-based detection usually occurs in two phases: a training phase and a detection phase. During the training phase, a detector attempts to learn normal behaviors. The detector could be learning the behavior of the host or the processes, or a combination of both during the training phase. A key advantage of anomaly-based detection is its ability to detect zero-day attacks, which are attacks previously unknown. The two fundamental limitations of this technique are its high false rate and the complexity involved in determining what features should be learned in the training phase.

In dynamic anomaly-based detection, information gathered from the program's execution is used to detect malicious codes. The detection phase monitors the program during its execution, checking for inconsistencies with what was learned during the training phase.

In static anomaly-based detection, characteristics about the file structure of the program under inspection are used to detect malicious codes. A key advantage of it is detecting malware without carrying program execution on the host system.

Signature-Based Detection

Signature-based detection attempts to model malicious behaviors and uses them to detect malware. The collection of all these models represents signature-based detection's knowledge. The model of malicious behaviors is often referred to as the signature. Ideally, a signature should be able to identify any malware exhibiting the malicious behavior specified by the signature. Signatures require a repository that represents all the knowledge it has. The signature-based method uses its repository and compares the process with the known signatures for a match. One of the major drawbacks of the signature-based detection is that it cannot detect zero-day attacks.

Dynamic signature-based detection is characterized by using solely information gathered during the execution of the process to decide its maliciousness. It looks for behavior patterns that would reveal the true malicious intent of a program.

Static signature-based detection is characterized by examining the program for sequences of code (signatures) that represent the malicious behaviors. The analysis and determine process without executing code is the major advantage. But this method cannot detect malware appears during app execution.

Specification-Based Detection

Specification-based detection is a type of anomaly-based detection that tries to address the rate of typical high false alarm associated with aforementioned techniques. In general, this detection attempts to approximate the requirements for an application or a system. The training

www.elsevierdirect.com

phase is the attainment of some rule set, specifying all the valid behaviors that any program can exhibit on protected systems. The main limitation of specification-based detection is that it is often difficult to specify completely and accurately the entire set of valid behaviors a system could exhibit.

Dynamic specification-based detection uses the behaviors observed at runtime to determine the maliciousness of an executable. During the detection phase, static specification-based detection uses the structural properties of the process to determine malware.

In recent years, a number of approaches have been proposed to detect malware on mobile devices. Even though all detection systems are strongly interrelated, because some techniques are more versatile, they are used more often. Others are used mainly for certain detection systems. Besides, both static analysis and dynamic analysis are used for both device and market protection. It is a trend that the complexion system is combining various techniques to achieve advanced protection on mobile platform.

5.4 Further Discussions

5.4.1 Open Issues and Challenges

Trust management in mobile platforms concerns a number of issues related to the security, dependability and usability of the mobile platforms. At present, the literature still lacks a comprehensive study on how to ensure mobile platform trust in a holistic way. Past studies covered the foundational platform layer (e.g. mobile trusted computing platform – MTCP), the middleware layer (e.g., trust management for component software), and the application layer (e.g., mobile app reputation systems and mobile malware detection). However, there are still a number of crucial issues that are still open for further investigation.

First, MTCP has not been widely used. It is applied for ensuring system software and providing a trusted execution environment. But literature still lacks studies on using it to ensure the trust of third party mobile apps. The fast growth of mobile app market and speedy app shipping make it challengeable to use MTCP to detect mobile malware in practice. This fact makes mobile platform become insecure due to the intrusion of the third party mobile apps and potential attacks from mobile and wireless network communications.

Second, it still lacks effective mobile platform middleware that can support app collaboration and cooperation in a trustworthy and secure manner. App isolation or independent execution could make mobile computing resources consumed uneconomically, which requests renovation on mobile platform architecture and mobile operating systems.

www.elsevierdirect.com

Third, collecting user data and feedback for mobile app reputation generation could intrude user privacy. How to solve this problem and meanwhile still ensure the accuracy, efficiency and robustness of the reputation generation is an interesting research issue that is worth our exploration. In addition, how to generate personalized app recommendation with privacy preservation is a signification research problem that challenges our future research.

Fourth, current mobile malware detection technologies cannot detect malware at app runtime. They are generally not effective for finding mobile malware occurred during app execution. Due to limited computing and storage resources at the mobile device, it is hard to achieve runtime malware detection. This is because malware detection needs to monitor mobile app running behaviors, collect a big sum of data and perform data analysis. Performing all above seems impossible in the mobile device, which challenges future research. One way is to outsource this to a cloud service provider. However, a new issue about privacy is introduced if the cloud service provider is curious on user privacy, such as personal preference and personal routine activities. How to overcome the above problems is an interesting research topic.

Fifth, user device authentication in a usable way has not been solved very well. Password input and fingerprint based authentication still need users to use their hands, which is not convenient in many situations, e.g., driving, frequent screen saving, working, etc. How to improve the usability of mobile device authentication and ensure expectable level of security is still a practical and challengeable issue worth our study.

5.4.2 Future Research Trends

Future research on the trust management in mobile platforms requests a holistic trust management framework that should cover all the layers of a mobile platform in a collaborative way. First, the MTCP should support the trustworthiness of the middleware of the platform. Thus, it is possible for the middleware to manage and maintain the trust of installed apps, adjust computing resources to ensure application performance and monitor mobile app behaviors for malware detection. Second, mobile malware detection research should focus on solving two issues. One is how to effectively fuse or aggregate data collected during app execution in order to detect malware in an efficient way in the platform. The other is how to preserve user privacy if runtime malware detection is outsourced to cloud. Third, usable and secure user-device authentication should be researched to replace current approaches in order to provide more advanced user experiences.

5.5 Conclusions

In this chapter, we firstly introduced the basic knowledge of trust and review the fundamental techniques of trust modeling and trust management. Then, we overviewed a number of fun-

www.elsevierdirect.com

damental technologies of trust management in mobile platform, which include mobile trusted computing platform, trust management on mobile software components, reputation system for mobile applications, and mobile malware detection. Furthermore, we discussed a number of open issues with regard to each layer of the mobile platform and proposed future research directions.

Acknowledgments

This work is sponsored by the National Key Foundational Research and Development on Network and Space Security, China (grant 2016YFB0800704), the NSFC (grants 61672410 and U1536202), the Ph.D. grant of the Ministry of Education, China (grant 20130203110006), the Project Supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016ZDJC-06), the 111 project (grants B08038 and B16037), and Academy of Finland (Grant No. 308087).

References

Aberer, K., Despotovic, Z., 2001. Managing trust in a peer-to-peer information system. In: Proceedings of the ACM Conference on Information and Knowledge Management (CIKM), pp. 310–317.

Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C., 2004. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing 1 (1), 11–33.

Balakrishnan, V., Varadharajan, V., 2005. Designing secure wireless mobile ad hoc networks. In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA 2005), vol. 2, pp. 5–8.

Bigley, G.A., Pearce, J.L., 1998. Straining for shared meaning in organization science: problems of trust and distrust. Academy of Management Executive 23, 405–421.

Blaze, M., Feigenbaum, J., Lacy, J., 1996. Decentralized trust management. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 164–173.

Boon, S., Holmes, J., 1991. The dynamics of interpersonal trust: resolving uncertainty in the face of risk. In: Hinde, R., Groebel, J. (Eds.), Cooperation and Prosocial Behavior. Cambridge University Press, Cambridge, UK, pp. 190–211.

Corritore, C.L., Kracher, B., Wiedenbeck, S., 2003. On-line trust: concepts, evolving themes, a model. International Journal of Human-Computer Studies, Trust and Technology 58 (6), 737–758.

England, P., Lampson, B., Manferdelli, J., Peinado, M., Willman, B., 2003. A trusted open platform. IEEE Computer 36 (7), 55–62.

Felten, E.W., 2003. Understanding trusted computing – will its benefits outweigh its drawbacks. IEEE Security & Privacy 1 (3), 60–62.

Gambetta, D., 2000. Can we trust trust? In: Gambetta, Diego (Ed.), Trust: Making and Breaking Cooperative Relations, electronic edition. Department of Sociology, University of Oxford, pp. 213–237. Chapter 13.

Grandison, T., Sloman, M., 2000. A survey of trust in internet applications. IEEE Communications and Survey 3 (4), 2–16.

Herrmann, P., 2001. Trust-based procurement support for software components. In: Proc. Fourth Int'l Conf. Electronic Commerce Research, pp. 505–514.

Herrmann, P., 2003. Trust-based protection of software component users and designers. In: Proc. First Int'l Conf. Trust Management, pp. 75–90.

Jøsang, A., 1999. An algebra for assessing trust in certification chains. In: Proceedings of the Networking. Distributed System Security Symposium, vol. 20(6), pp. 839–845.

Jøsang, A., 2001. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 9 (3), 279–311.
Kosko, B., 1986. Fuzzy cognitive maps. International Journal Man-Machine Studies 24, 65–75.
Li, X., Valacich, J.S., Hess, T.J., 2004. Predicting user trust in information systems: a comparison of competing trust models. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences-Track, p. 80259b.
Liu, Z., Joy, A.W., Thompson, R.A., 2004. A dynamic trust model for mobile ad hoc networks. In: Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS 2004), pp. 80–85.
Maurer, U., 1996. Modeling a public-key infrastructure. In: Proceedings of the European Symposium of Research on Computer Security. In: LNCS, vol. 1146, pp. 325–350.
Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995. An integrative model of organizational trust. Academy of Management Review 20 (3), 709–734.
McKnight, D.H., Cummings, L.L., Chervany, N.L., 1998. Initial trust formation in new organizational relationships. Academy of Management Review 23, 473–490.
McKnight, D.H., Choudhury, V., Kacmar, C., 2002. Developing and validating trust measures for e-commerce: an integrative typology. Information Systems Research 13 (3), 334–359.
Mui, L., 2003. Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks. Doctoral dissertation. Massachusetts Institute of Technology, pp. 452–457.
Muir, B.M., 1994. Trust in automation: part I. Theoretical issues in the study of trust and human intervention in automated systems. Ergonomics 37, 1905–1922.
Muir, B.M., Moray, N., 1996. Trust in automation: part II. Experimental studies of trust and human intervention in a process control simulation. Ergonomics 39, 429–460.
Novák, V., Perfilieva, I., Močkoř, J., 1999. Mathematical Principles of Fuzzy Logic. Kluwer Academic, Dodrecht. ISBN 0-7923-8595-0.
Pearl, J., 1988. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference.
Raya, M., Papadimitratos, P., Gligory, V.D., Hubaux, J-P., 2008. On data-centric trust establishment in ephemeral ad hoc networks. In: IEEE INFOCOM, pp. 1912–1920.
Reiter, M.K., Stubblebine, S.G., 1998. Resilient authentication using path independence. IEEE Transactions on Computer 47 (12), 1351–1362.
Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C., 1998. Not so different after all: a cross-discipline view of trust. Academy of Management Review 23 (3), 393–404.
Shafer, G., 1976. A Mathematical Theory of Evidence. Princeton University Press.
Stylios, C.D., Georgopoulos, V.C., Groumpos, P.P., 1997. The use of fuzzy cognitive maps in modeling systems. In: Proc. Fifth IEEE Mediterranean Conf. Control and Systems. Retrieved from http://med.ee.nd.edu/MED5/PAPERS/067/067.PDF.
Sun, Y., Yu, W., Han, Z., Liu, K.J.R., 2006. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications 24 (2), 305–317.
Tan, Y., Thoen, W., 1998. Toward a generic model of trust for electronic commerce. International Journal of Electronic Commerce 5 (2), 61–74.
TCG, 2003. TCG TPM Specification v1.2. https://www.trustedcomputinggroup.org/specs/TPM/.
Theodorakopoulos, G., Baras, J.S., 2006. On trust models and trust evaluation metrics for ad hoc networks. IEEE Journal on Selected Areas in Communications 24 (2), 318–328.
Wang, Y., Varadharajan, V., 2005. Trust2: developing trust in peer-to-peer environments. In: Proceedings of the IEEE International Conference on Services Computing, vol. 1, pp. 24–31.
Xiong, L., Liu, L., 2004. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering 16 (7), 843–857.
Yan, Z., 2007. Trust Management for Mobile Computing Platforms. Doctoral dissertation. Dept. of Electrical and Communications Engineering, Helsinki Univ. of Technology. ISBN 9789512291205.

Yan, Z. (Ed.), 2010a. Trust Modeling and Management in Digital Environments: From Social Concept to System Development. IGI Global.

Yan, Z., 2010b. Security via trusted communications. In: Stavroulakis, P., Stamp, M. (Eds.), Handbook on Communications and Information Security. Springer, pp. 719–746.

Yan, Z., 2013. Trust Management in Mobile Environments – Usable and Autonomic Models. IGI Global, Hershey, Pennsylvania, USA.

Yan, Z., Holtmanns, S., 2008. Trust modeling and management: from social trust to digital trust. In: Subramanian, R. (Ed.), Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions. IGI Global, pp. 290–323.

Yan, Z., Prehofer, C., 2011. Autonomic trust management for a component based software system. IEEE Transactions on Dependable and Secure Computing 8 (6), 810–823.

Yan, Z., Zhang, P., Deng, H.R., 2012. TruBeRepec: a trust-behavior-based reputation and recommender system for mobile applications. Journal of Personal and Ubiquitous Computing 16 (5), 485–506.

Yan, Z., Dong, Y., Niemi, V., Yu, G., 2013. Exploring trust of mobile applications based on user behaviors: an empirical study. J. Appl. Soc. Psychol. 43 (3), 638–659.

Zhou, M., Mei, H., Zhang, L., 2005. A multi-property trust model for reconfiguring component software. In: Proceedings of the Fifth International Conference on Quality Software, QAIC2005, pp. 142–149.

CHAPTER 6

Security Issues of In-Store Mobile Payment

Xingjie Yu, Su Mon Kywe, Yingjiu Li

Contents

6.1 Introduction 116

6.2 Background on In-Store Card Payment 118

6.2.1 Magnetic Stripe Payment Cards 118

6.2.2 EMV Payment Cards 119

6.3 In-Store Mobile Payment Network Models 120

6.3.1 Overview of In-Store Mobile Payment Services 120

6.3.2 Network Model of PTB Payment Services 122

6.3.2.1 Token Provision 122

6.3.2.2 Token Usage 123

6.3.3 Network Model of STB Payment Services 124

6.4 Issues Related to Token Service Provider 125

6.4.1 Role of Token Service Provider 125

6.4.2 Security Challenges 126

6.4.2.1 ID & V Methods 127

6.4.2.2 Token Assurance 128

6.4.2.3 Domain Restriction Controls 128

6.4.2.4 Token Vault Secure Storage 129

6.5 Issues Related to Mobile Payment Service Provider / Token Requestor 129

6.5.1 Security Issues of Token Requestor 129

6.5.2 Security Issues of Mobile Payment Service Provider 130

6.5.2.1 Service Account Credential Security 130

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00006-1
Copyright © 2018 Elsevier Inc. All rights reserved.

6.5.2.2 Payment Credential Security 131
6.6 On-Device Level Issues 132
6.6.1 Payment Card Emulation 133
6.6.1.1 Secure Element (SE)-Enabled Card Emulation 133
6.6.1.2 Host Card Emulation (HCE) 135
6.6.1.3 Comparison Between SE and HCE 137
6.6.2 User Authentication 138
6.6.2.1 Non-biometric User Authentication 139
6.6.2.2 Biometric User Authentication 140
6.6.2.3 Free Authentication Transaction 141
6.7 Conclusion 141
References 142

6.1 Introduction

Instead of transacting with cash, cheques, or credit cards, an increasing number of consumers start using mobile devices to make in-store payment. In-store mobile payment brings new entities, such as mobile payment service provider and mobile device, into the traditional payment system. Although these two entities have access to users' sensitive payment credentials (e.g., payment card information, payment account information), they are not reliable. For instance, mobile devices are susceptible to various external threats bearing the risk of payment credentials disclosure. To mitigate the risk, most mobile payment services replace payment credentials with non-sensitive payment tokens. The use of payment tokens introduces two new entities, Token Service Provider (TSP) and Token Requestor (TR), into in-store mobile payment. Unsurprisingly, these new entities also introduce additional security issues and challenges. This chapter focuses on the security issues related to the new entities in in-store mobile payment.

We first introduce two types of mobile payment services, Payment-Token-Based (PTB) and Service-Token-Based (STB). A PTB payment service replaces a payment card information, such as Primary Account Number (PAN), with a *payment token*. The token is sent from a mobile device to a Point of Sale (POS) terminal as a user's payment credential. A STB payment service replaces a user's mobile payment service account information, such as username and password, with a *service token*. The mobile payment service provider verifies the service token and sends the user's payment credential to the payment network. We propose network models for both PTB and STB payment services. Our network models reflect the interactions

www.elsevierdirect.com

among various entities of PTB and STB payment services. Based on the proposed network models, we discuss the security issues encountered by each entity. We also explore the design space for addressing these security issues.

TSP is an entity responsible for issuing payment tokens to TR in both PTB and STB payment services. According to EMVCo payment tokenization specification (EMVCo), a standard token service provider performs the following steps: (1) defines and performs identification and verification (ID&V) methods to authenticate the initiator of a token request; (2) provides a token assurance level for a payment token to indicate the confidence on the payment token; (3) defines token domain restriction controls for a payment token to restrict its usage; (4) verifies a payment token in transaction authorization process; (5) operates a secure token vault to store the mapping between payment tokens and the payment cards. We identify security issues encountered in each step. After that, we provide suggestions for token service providers to offer enhanced security in the token issuance and authorization. For instance, we suggest TSP to implement data encryption strategies to prevent unauthorized access to token vault secure storage and implement data redundancy strategies to prevent corruption of information.

TR is an entity which registers with a TSP and requests for payment tokens in both PTB and STB payment services. Based on EMVCo payment tokenization specification, we identify the following major security requirements for a TR. First, a TR is required to register with TSPs and comply with their proprietary registry requirements, systems, and processes. Moreover, in ID&V steps, TR should verify the basic payment card information, such as Card Verification Number (CVN) and bill address, and provide the validation evidence to TSP. In addition, once a payment token is issued to a TR, the TR should provision the payment token in a secure location. In most cases, mobile payment service provider acts as TR.

Mobile payment service providers are responsible for managing users' service account and payment credentials. Due to the differences in transaction authorization process, the security issues of mobile payment service providers in PTB payment are different from that in STB payment. In PTB payment, the service account management processes, including user registration and user account life-cycle management, are similar to other traditional client–server services. However, in STB payment, the mobile payment service providers are required to ensure the secure generation, transmission, and verification of service tokens. In the authorization process of a PTB transaction, a payment token is directly sent from a user's mobile device to a POS terminal. Hence, the mobile payment service provider should securely store payment tokens on users' mobile devices or in a back-end cloud server which distributes payment tokens to mobile clients in real-time or at given time intervals. In STB payment, the user's payment card information may be sent as the user's payment credential to the payment network. Therefore, in this case, the mobile payment service provider should securely keep

www.elsevierdirect.com

users' payment cards information in its database. We also expose the implications of the existing solutions, such as dynamic secure token schemes and secure QR code schemes, which are used to protect the service tokens.

We identify two main security issues on mobile devices: card emulation and user authentication. First, in PTB payment, card emulation techniques enable a mobile device to emulate any contactless smart card when tapped on POS terminal. Hence, we analyze the security risks of Secure Element (SE)-enabled card emulation and Host Card Emulation (HCE) and compare their differences. Second, we investigate the existing user authentication schemes in both PTB and STB payments on mobile devices, including non-biometric user authentication, biometric user authentication, and free authentication schemes. Non-biometric user authentication schemes require users to memorize passwords, but do not require additional dedicated hardware support on mobile devices. Biometric authentication schemes free users from remembering passwords. However, some inherent limitations, such as the difficulties in recognizing biometric signals, affect usability. Some mobile payment services provide better user experience by allowing users to make payment without user authentication. We analyze the attacks against such authentication schemes, including exhaustive attacks, dictionary attacks, shoulder-surfing attacks, and some sophisticated attacks. We also explore existing solutions to mitigate these attacks.

The next section introduces the background on in-store card payment. Section 6.3 describes the network models of PTB and STB payment services. Section 6.4 highlights the security issues of TSP based on EMV tokenization specification. Section 6.5 explains the security issues of TR and mobile payment service provider. Section 6.6 clarifies the security issues related to mobile devices. Section 6.7 concludes this chapter.

6.2 Background on In-Store Card Payment

In this section, we introduce magnetic stripe cards and describe the authorization process of a transaction involving a magnetic card. We also explain about EMV cards and discuss the advantages of EMV cards over magnetic stripe cards.

6.2.1 Magnetic Stripe Payment Cards

A magnetic stripe card is a type of cards capable of storing data on a band of magnetic material on the cards (Pedia, W. Magnetic stripe card). On the back of each card is a magnetic strip very similar to a piece of cassette tape. It stores information on three tracks. Track one contains specific bank information such as account number, a holder's name, expiration data, and security codes. Track two contains general bank industry information with a Card Verification

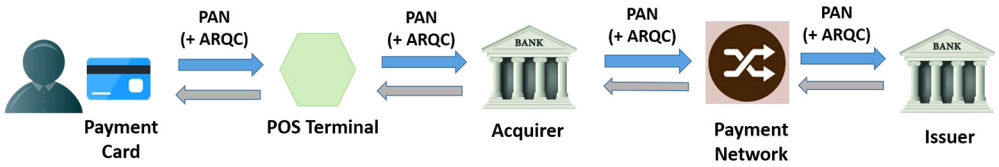


Figure 6.1: Traditional in-store card payment.

Number (CVN). Track three is generally not used (McNamara). Data stored on the magnetic strip are unprotected and never change.

Fig. 6.1 illustrates the authorization process of a magnetic stripe card transaction. When a magnetic payment card is swiped through a magnetic card POS terminal, the static data (e.g., PAN) on the magnetic strip are transmitted to the POS terminal. The POS terminal then forms an authorization request using the received card data. The authorization request is then sent to an acquirer (i.e. acquiring bank), routed to the appropriate payment network (e.g., Visa and MasterCard), and finally delivered to a card issuer (i.e. issuing bank) for authentication and authorization.

After receiving a transaction authorization request, the issuer authenticates the card based on the static card data contained in the authorization request. To verify that the individual with the card is the actual cardholder, the issuer may also verify a PIN provided by the cardholder at the POS terminal. PIN verification is mandated in most debit transactions (e.g., Nets, UnionPay) and some credit transactions (e.g., UnionPay). In addition to PIN verification, an issuer can further authenticate the cardholder by using out-of-band authentications, such as sending a one-time passcode to the legitimate cardholder via SMS or calling the cardholder for additional verifications. After the card is verified as genuine and the cardholder is authenticated as legitimate, the issuer further verifies whether there are enough funds in the payment account to pay for the transaction. Once the issuer finally approves or rejects the transaction, the authorization decision is transmitted to the acquirer via the payment network and sent back to the POS terminal.

6.2.2 EMV Payment Cards

EMV cards are smart cards, which store their data on integrated circuits instead of magnetic stripes (Pedia, W. Emv). They are also called chip cards or IC cards. EMV takes its name from Europay, MasterCard, and Visa, the original three credit card brands that developed it in 1994. MasterCard reported that over 1.2 million U.S. merchant locations have EMV-enabled terminals and are accepting chip card payments by March 2016 (MasterCard). Moreover, Visa

www.elsevierdirect.com

estimated that 50% of merchant locations will be enabled by the end of 2016 (Smart Card Alliance, EMV and Parking).

The logic behind EMV card transaction authorization processes is not radically different from magnetic stripe card transactions. Like magnetic stripe card transactions, the authorization process of an EMV card transaction includes multiple steps such as card authentication and cardholder authentication (ALLIANCE). Hence, the network model shown in Fig. 6.1 also works for EMV card payment transactions.

Contrary to magnetic stripe cards, EMV chip cards have the processing power that allows them to manage risk and perform cryptographic computations dynamically. In the authorization process of an EMV transaction, dynamic data, such as a digital signature, are used to authenticate a card, rather than the static data used in magnetic stripe card transactions. In an EMV card transaction, a chip embedded in an EMV card encrypts data (e.g., amount of the purchase, the transaction time, and a terminal-generated unpredictable number) provided by the card and the POS terminal. The encryption is performed with symmetric keys securely stored on the card for generating a unique authorization request cryptogram (AQRC). This cryptogram is finally sent to and authenticated by the issuer as part of the authorization request together with static card data (e.g., PAN). The usage of dynamic cryptograms in EMV card transactions mitigates the risk of counterfeit fraud and skimming that are normally encountered in magnetic stripe card transactions.

6.3 In-Store Mobile Payment Network Models

In this section, we provide details of the two types of in-store mobile payment services, Payment-Token-Based (PTB) and Service-Token-Based (STB). We also propose the network models of their transaction authorization processes. Our network models reflect the typical interactions among entities involved in PTB and STB payment services.

6.3.1 Overview of In-Store Mobile Payment Services

Most mobile payment services use tokenization technique. Tokenization technique replaces the sensitive credentials with non-sensitive tokens to prevent the leakage and counterfeit of users' credentials. Depending on the type of tokens sent by mobile devices, mobile payment services can be classified into two groups: Payment-Token-Based (PTB) and Service-Token-Based (STB). In a PTB payment service, a mobile device transmits a *payment token* that replaces a payment card's information (e.g., PAN) to a POS terminal. In an STB payment service, a mobile device uses a *service token* that replaces a user's mobile payment service account information (e.g., username and password). Table 6.1 summarizes typical mobile

www.elsevierdirect.com

Table 6.1: Payment-token-based and service-token-based mobile payment services.

Payment-Token-Based Mobile Services		Service-Token-Based Mobile Services	
Payment Service	**Mobile Device Compatibility**	**Payment Service**	**Mobile Device Compatibility**
Apple Pay	iPhone 6/ 6+/6s/6s+/ Apple Watch	PayPal	iOS 7.0+/ Android 4.0+/ Win Phone 8.1/10
Android Pay	NFC-enabled, Android 4.4+	Dash	iOS 7.0+/ Android 2.3.3+/
Samsung Pay	Galaxy S6/S6 edge/S6 edge+/ S6 active/Note 5	Wechat Pay	iOS 7.0/ Android 2.3+/ Win Phone 8/8.1/10
UOB Mighty	NFC-enabled, iOS 8.0+/ Android 4.3+	Alipay	iOS 7.0+/ Android 2.3+/ Win Phone 8/8.1/10

payment services in these two categories. In both types of payment, users are required to pre-install mobile payment apps, such as mobile wallets, when checking out in stores.

In a PTB payment service, a user is not required to open a mobile payment app to make the payment. The user just unlocks the device and the mobile payment app immediately runs in the mobile OS. After the user places the device near a merchant's POS terminal, the mobile payment app running in the mobile OS automatically communicates with the POS terminal and completes the purchase.

In an STB payment service, a user is required to open a mobile payment app and perform certain operations to check out. A user first presents a payment code, such as QR code, shown in the mobile payment app to a merchant's terminal. After the terminal scans and receives a service token encoded in the payment code, it forms a transaction authorization request using the service token and merchant's ID. The request is then sent to the mobile payment service provider. Alternatively, a user can provide the merchant's ID and confirm the transaction details in the mobile payment app. Then the mobile payment app forms a transaction authorization request using the service token and merchant's ID, and sends the request to the mobile payment service provider. There are different methods for a user to provide the merchant's ID in the mobile payment app. For example, a user of Alipay scans a merchant's payment code that has the merchant's ID encoded using Alipay Wallet; a user of Dash Pay chooses a merchant's ID from a list of available merchants in Dash mWallet (i.e., Dash Pay's mobile app for in-store payment), or taps on a merchant's Dash reader with a Near Field Communication (NFC)-enabled phone to get the merchant's account ID.

PTB and STB payment services have different requirements on the capacity of mobile devices and POS terminals. PTB payment services require mobile devices to automatically

www.elsevierdirect.com

communicate with POS terminals at the cashier. Hence, mobile devices and POS terminals need specific technologies to build a communication channel. For example, Apple Pay and Android Pay require NFC-enabled mobile devices and POS terminals. Samsung Pay supports both NFC and Magnetic Secure Transmission (MST). Therefore, Samsung Pay users can pay at traditional magnetic POS terminals with MST Samsung phones. On the other hand, most STB payment services are available on mobile devices without NFC or MST. Users' service tokens and merchants' IDs can be transmitted in other ways.

6.3.2 Network Model of PTB Payment Services

There are two steps involved in a PTB transaction. First, a payment token is generated and issued to a user through a token provision process. Second, a payment token is used as the user's payment credential in the token usage process. The latter step is also referred to as the transaction authorization process, since users' payment credentials are used for authorization. Fig. 6.2 describes the network model of PTB payment, which involves both token provision and token usage processes.

6.3.2.1 Token Provision

Token provision is a process that a token service provider (TSP) issues a payment token for a specific PAN and for a specific purpose, domain, or device. The token provision process consists of the following steps:

1. A user adds a payment card in a mobile payment service and provides the account information of the payment card (e.g., PAN, CVN, and expiry data) to a mobile payment service provider.
2. The mobile payment service provider performs as a TR and submits the account information to TSP in a token request message.
3. The TSP forwards the token request to the card issuer for authorization if the card issuer does not operate as the TSP. Theoretically, any organization, such as a payment network (e.g., VISA and MasterCard), a card issuer, a mobile payment service provider, or a third party, can operate as TSP. If the TSP is operated by the card issuer, the token request will be directly routed to the card issuer from the TR via payment network.
4. The issuer authenticates the identity of the cardholder (i.e., the user of the mobile payment service) and the validity of the payment card. It then approves or rejects the token provision request.
5. With the issuer's approval, TSP replaces the PAN of the payment card with a payment token and shares the payment token with the TR for mobile payment.

www.elsevierdirect.com

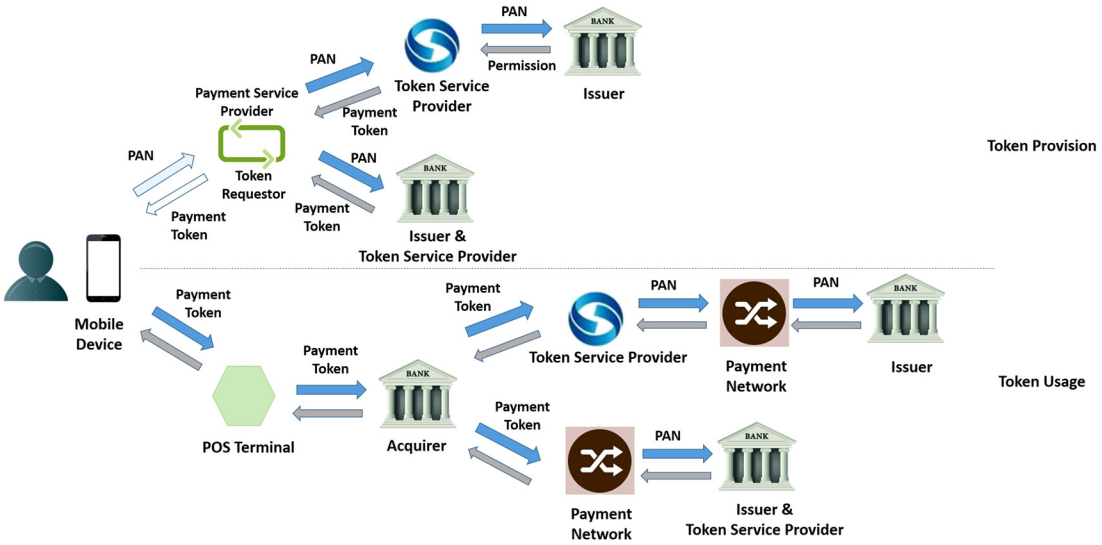


Figure 6.2: The network model of PTB payment.

The same PAN may associate with multiple payment tokens provisioned from the same or different TRs. A cardholder may register the same payment card with multiple mobile payment service providers. Each mobile payment service provider may request for multiple payment tokens for the same card from different TSPs.

6.3.2.2 Token Usage

When a user makes PTB payment, the user's mobile device passes a payment token to the acquirer via the POS terminal as part of an authorization request. In some cases where the TSP is performed by the issuer, the authorization request is directly routed from the acquirer to the issuer via payment network for verification, de-tokenization, and authorization. If the TSP is performed by a payment brand or a third party, the transaction authorization process has the following steps:

1. A user holds his/her mobile device near a POS terminal.
2. The mobile payment service app (i.e., mobile wallet) receives a transaction request sent by the POS terminal and prompts the user to authorize the transaction with his/her credential (e.g., fingerprint, passcode).
3. After verifying the user's identity, the mobile payment service app chooses the user's default card and transmits a payment token and associated transaction data (e.g., a transaction-specific cryptogram) to the POS terminal.

www.elsevierdirect.com

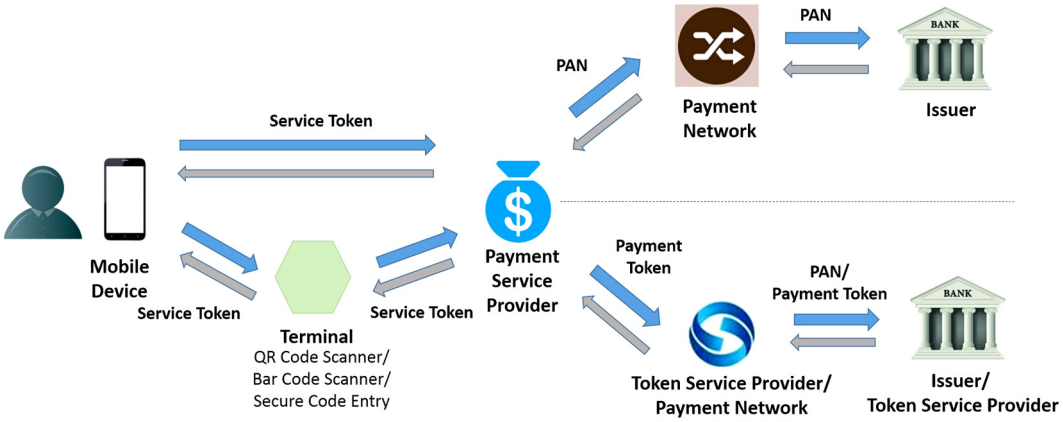


Figure 6.3: The network model of STB payment.

4. The transaction data and payment token are forwarded to an acquirer, and then sent to the corresponding TSP for verification and de-tokenization.
5. Only if the payment token is verified as valid, the TSP maps the payment token to the PAN, inserts the PAN into the authorization request, and sends it to the card issuer for authorization.
6. The issuer accepts or declines the transaction and sends its response back to the TSP.
7. The TSP then maps the PAN back to the payment token and sends the payment token in an authorization response back to the merchant's terminal via the acquirer.

In either token provision or token usage, the TSP and TR should collaborate to ensure the security of a tokenization-based payment system. We clarify the security requirements for a TSP in Section 6.4 and the security requirements for a TR in Section 6.5.1.

6.3.3 Network Model of STB Payment Services

Fig. 6.3 shows the network model of STB payment. In the authorization process of an STB transaction, a service token which is generated from the information of a user's service account is sent by the mobile device as the user credential. The service token may be sent to the merchant's terminal from the user's mobile device, and then routed to the mobile payment service provider in an authorization requestor for validation and authorization. Alternatively, the mobile device may directly send the service token to the mobile payment service provider through an Internet connection. In the latter case, the merchant's ID should also be included in the transaction authorization request sent from the mobile device.

After receiving the transaction authorization request, the mobile payment service provider maps the service token in the request to the user's service account. It then sends the payment credential of the user's default payment card to the issuer for authorization. Depending on whether the mobile payment service provider has registered as a TR of a TSP or not, the user's payment credential may be a payment token or the payment card information (e.g., PAN).

If the mobile payment service provider performs as a TR, the process of token provision follows the steps introduced in Section 6.3.2.1. The mobile payment service provider requests payment tokens for the user's payment card from a TSP. In the process of transaction authorization, the mobile payment service provider sends the user's payment token as the user's payment credential to the TSP. The TSP then verifies the payment token, maps the payment token to the PAN, and sends the PAN to the issuer for transaction authorization.

Otherwise, if the mobile service provider has not registered with any payment token service, in the process of transaction authorization, it directly sends the user's payment card information (e.g., PAN) as the user's payment credential to the issuer for transaction authorization. In this case, the mobile payment service provider needs to keep users' sensitive payment card information in its database, which raises the risk of card information disclosure. We discuss the countermeasures for the mobile payment service provider to mitigate this risk in Section 6.5.2.2.

6.4 Issues Related to Token Service Provider

In this section, we first explain the role of TSP in payment systems. We then clarify the security challenges for a TSP, and analyze the corresponding solutions provided in the EMVCo payment tokenization specification.

6.4.1 Role of Token Service Provider

Currently, TSPs are mainly operated by payment card networks (e.g., Visa, MasterCard) and a few other large card issuers. Visa announced its Visa Token Service (VTS) as part of the broader Visa Digital Solutions (VDS) in September 2014 (Visa Inc.). MasterCard also launched its MasterCard Digital Enablement System (MDES) as a TSP in September 2014 (MasterCard Inc.). Apple Pay, Android Pay and Samsung Pay support VTS and MDES to provide in-store mobile payment through VISA and MasterCard.

The payment card networks have some advantages in operating as TSPs due to their experience in payment card provision and strong security. To use a payment token issued by a TSP

www.elsevierdirect.com

in transaction authorization, both a merchant's terminal and the card issuer need to communicate with this TSP. Since card payment networks have already collaborated with a large number of merchants and card issuers, it might be more efficient for them to create and link a payment token to the cardholder's PAN, receive the payment token from a merchant's terminal and pass the PAN to the card issuer. From the perspective of communication security, the existing transmissions between card networks and card issuers are dedicated communication channels that are constantly monitored for possible intrusion. The data are encrypted in transmissions (Marianne Crowe, Susan Pandy, D. L. S. M.). Hence, the potential to compromise the channels and the sensitive data (e.g., PAN) is relatively low.

EMVCo payment tokenization specification (EMVCo) published by EMVCo is now widely used as an industrial standard of payment tokenization. Theoretically, any organization can be a TSP, if it provides the functions required by EMVCo payment tokenization specification. Therefore, in this section, we analyze the security challenges encountered by a TSP based on the requirements specified in EMVCo payment tokenization specification.

As the industrial standard, the current version of EMVCo payment tokenization specification needs to be improved. First, it provides guides and requirements for payment tokenization systems in a relatively high level. To achieve standardization of every module in payment tokenization system, the next version of EMVCo payment tokenization or other future industrial standards should provide more specific clarity around technical details. Second, the next version of EMVCo payment tokenization or other future industrial standards should not only maintain compatibility with the existing payment infrastructures, but also extend existing specifications to maintain consistency with the development of mobile payment technologies.

6.4.2 Security Challenges

As the authorized party for token issuance, a TSP should ensure that a payment token is issued to a legitimate TR for a legitimate cardholder. Particularly, at the time a payment token is issued, a TSP should (1) define and perform identification and verification (ID&V) methods to verify if the token request is initiated by a legitimate cardholder; (2) provide a token assurance level of a payment token to the card issuer, indicating the confidence level of the payment token to PAN binding; (3) define token domain restriction controls to restrict the usage of the payment token.

During a transaction authorization process, a TSP should (1) verify the payment token, (2) map the payment token to the PAN, (3) send the PAN in a transaction authorization message to the card issuer for account-level validation and authorization, and (4) map the PAN back to the payment token in any response messages sent back to the acquirer. To prevent frauds with a compromised payment token, a TSP should verify the payment token by strictly executing

domain restriction controls. Moreover, to ensure a secure de-tokenization and tokenization, a TSP should operate a secure token vault to store the mappings between tokens and their corresponding PANs as well as other attributes of payment tokens, such as token expiry date and TR's ID.

6.4.2.1 ID & V Methods

ID&V steps are critical parts of the token issuance process. They ensure that a legitimate cardholder initiates the request of replacing a PAN number with a payment token. When issuing a payment token, TSP must define the types of ID&V methods. There are four examples of ID&V methods defined by EMVCo specification (EMVCo): (1) account verification, (2) TSP risk score, (3) TSP risk score with TR data, and (4) card issuer authentication of the cardholder. Their details are described below:

- Account verification includes the basic verification of a payment card. Examples are Card Verification Number (CVN) validation and address verification. The account verification method is either initiated by the TR and reported to the TSP or directly initiated by the TSP. If the account verification is taken by the TR, the TSP should require the TR to provide verifiable evidence of the verification result.
- Token service risk score is calculated from a risk-based assessment performed by the TSP. It is normally based on the risk management system and authentication data.
- In addition to risk score, the TSP can use other types of authentication data to prevent token fraud. They include account age and history, bill or ship addresses, contact information, IP address, device ID and other device information and geolocation provided by TRs. For example, to improve the security of the ID&V or risk-decision process, Apple Pay allows TSPs to collect more data about the enrollment process. It includes information about the mobile device or the iTunes account.
- Cardholder verification can be carried out by the card issuer to enhance the security of binding between the payment token and PAN. After receiving a token authorization request from a TSP, the card issuer can verify the cardholder through dynamic authentication data, such as 3-D Secure Access Control Service (Wiki Pedia, 3-D Secure), one-time password (OTP), activation code, or other shared secret between the card issuer and the cardholder. Authenticating the cardholder with static authentication data is not advisable, since replay attacks can be performed. Moreover, the card issuer should deliver the shared secret (e.g., OTP and activation code) to the cardholder through an out-of-band channel. This is to ensure that the authentication data is shared only between the card issuer and the cardholder.

To issue a payment token, one or a combination of several ID&V methods can be applied. ID&V steps can be performed by not only the TSP, but also the TR or the card issuer.

www.elsevierdirect.com

6.4.2.2 Token Assurance

When requesting the card issuer to authorize a token to PAN binding, a TSP should provide a token assurance level for a payment token. The token assurance level indicates the TSP's confidence level of the payment token to PAN binding. The TSP needs to transmit the token assurance level and token assurance data to the card issuer as a part of an authorization request. The token assurance levels allow a card issuer to measure where the transaction may fall in their risk category and to decide the approval of the token request.

Token assurance level is determined based on the type of the ID&V process. Different ID&V methods result in different token assurance levels. According to EMVCo payment tokenization specification, the token assurance level can range from no assurance to high assurance, depending on the strength of the ID&V methods applied.

The token assurance level should be decided based on a trade-off between security and user experience. Some TRs, TSPs or card issuers may want to increase the token assurance level by implementing more ID&V methods. However, the more ID&V methods are incorporated, the more details are required from the cardholder. This may cause a negative user experience. Even worse, this may cause a loss in competition, since the cardholder may not need to provide the additional authentication information when registering the same payment card with other TRs or TSPs.

6.4.2.3 Domain Restriction Controls

TSPs are responsible for designing and executing domain restriction controls to ensure the appropriate usage of payment tokens. During the registration process, the TSP works together with the TR to define and implement domain restriction controls that meet the TR's needs to restrict the usage of payment tokens. For example, domain restriction controls could specify POS entry modes and merchant identifiers, e.g., country, region, different norms and markets, consumer demographics, customer profiles, levels of sophistication of customer base, loyalty, and average spend of the consumer. Domain restriction controls can also be created to limit token value, transaction volume or type of use (e.g., tokens can/cannot be used for digital goods), create expiration time frames, and add other elements.

In transaction authorization process, TSPs should strictly execute domain restriction controls to reduce the impact of fraud from a compromised payment token. For example, in a transaction where a token cryptogram generated from the mobile device along with POS entry mode serve as the domain restriction control fields, the TSP verifies the cryptogram to validate the integrity of the transaction.

www.elsevierdirect.com

6.4.2.4 Token Vault Secure Storage

The TSP should implement a token vault to maintain the established payment token to PAN mapping (EMVCo). Other attributes of a token that are used for transaction authorization are also kept in the token vault. Any malicious breach of the token vault would likely result in a major erosion of consumer confidence in the payment system since tokenization is supposed to make the overall payment card system more secure. Hence, the token vault must have extremely high levels of security to prevent data disclosure and ensure instantaneous data accessibility.

Consequently, TSPs, just like other secure storage providers, are responsible for preventing unauthorized access to confidential data and accidental or intentional destruction, infection or corruption of information. Data encryption and strong access control are the most common security practices used to prevent unauthorized disclosure of sensitive data. On the other hand, to ensure service availability against accidental or intentional system errors or data destruction, data redundancy that holds the same piece of data in several separate places is widely used in secure storages. Hence, TSPs should deploy appropriate data encryption and data redundancy strategies to ensure secure storage for payment tokens and related data.

6.5 Issues Related to Mobile Payment Service Provider / Token Requestor

As we discussed in Section 6.3, in in-store mobile payment, the role of TR is only operated by the mobile payment service provider. In particular, a PTB service provider always acts as a TR, and an STB service provider may act as a TR in some cases. Consequently, any mobile payment service provider that performs as a TR should address the security issues of a TR. Given that, we analyze the security issues of a TR together with the security issues of a mobile payment service provider in this section. We first clarify the security responsibilities of a TR based on EMVCo payment tokenization specification. We then analyze the security issues of a mobile payment service provider. The issues include the security of service account credentials and payment credentials.

6.5.1 Security Issues of Token Requestor

Disclosure of users' payment credentials results in fraud transactions. To prevent this, a mobile service provider of PTB payment must perform as a TR and request payment tokens for users' payment cards in token provision processes. Alternatively, a mobile service provider of STB payment may perform as a token request registering token service from a TSP. In this

www.elsevierdirect.com

case, the mobile payment service provider sends the user's payment token to the TSP for authorization during the transaction authorization process. Any mobile payment service provider that performs as a TR should take the security responsibilities of a TR.

Based on EMVCo payment tokenization specification, we outline the major security responsibilities of a TR as follows:

First, a TR is required to register with TSPs and comply with their proprietary registry requirements, systems, and processes (EMVCo). When registering a token service, the TR should provide rules of token domain restriction controls to the TSP. The token domain restriction controls submitted by the TR will be used by the TSP to establish appropriate token domain restriction controls for the TR. After successful registration with a TSP, the TR will be assigned with a TR ID. With the assigned TR ID, the TR can implement the specified token service API. After that, the TR can initiate payment token requests in accordance with the processes and technologies specified within the API.

Moreover, as we mentioned in Section 6.4.2.1, a TR plays an important role in ID&V steps. The TR could perform account verification with basic verification of payment card valid, such as CVN validation and address verification. In this case, the TR should send the validation evidence to the TSP. If other ID&V methods are required for issuing a payment token, the TR is required to provide verification data to the TSP, such as account age and history, bill to/ship addresses, IP address, device ID/information, geolocation, and transaction velocity.

In addition, once a payment token is issued to a TR, the TR should keep the payment token in a secure location in the token provision process. In PTB payment, payment tokens are directly passed to the terminals from users' mobile devices. Hence, for a TR performed by a PTB payment service provider, it is better to locate payment tokens in a secure storage on the user's mobile device or a secure cloud-based storage, which is detailed in Section 6.6.1. Unlike PTB payment service providers, an STB payment service provider that performs as a TR should store payment tokens in its database. This is because, in STB payment, a mobile payment service provider only receives service tokens from users' mobile devices in transaction authorization requests. Hence, there is no need to keep the payment tokens on users' mobile devices which are vulnerable to various known threats.

6.5.2 Security Issues of Mobile Payment Service Provider

6.5.2.1 Service Account Credential Security

All mobile payment service providers are responsible for managing their users' service accounts, such as user registration, user account life-cycle management, and service account credential storage. In a PTB payment service, the service account management is similar to

other client–server services. Hence, no new issue on the security of service account credential has been brought to the mobile payment service provider.

However, in an STB payment service, service tokens that replace users' service account information are used as users' service account credentials in transaction authorization requests sent from mobile devices. The usage of service tokens requires the service provider to ensure secure generation, transmission and authentication of the service tokens.

A service token should contain the basic service account information, such as username and password. Besides that, to prevent replay attacks using a disclosed service token, the service token should also contain dynamic data. Dynamic service tokens are currently applied in mainstream STB payment services, such as Alipay and PayPal. As a simple example, a dynamic service token could include user account's basic information and a time stamp. In this case, when verifying a received service token, the service provider can compare the time stamp contained in the service token with the time of the transaction authorization request. More information may also be included in a service token, such as geolocation, mobile device ID and other information. Correspondingly, this information can be verified by the mobile payment service provider as part of user validation.

In some cases where the service token is not generated under encryption, a malicious attacker, such as a malicious merchant, may extract a user's basic account information from his/her previous service token. Then, the attacker can generate a counterfeit service token by merging dynamic data and initiate a transaction with this counterfeit service token. To prevent such attack, the service token should be generated by encrypting both the basic service account information and dynamic data. The encryption key is secret with the user's mobile payment app and the payment service provider. Therefore, the attacker who intends to forge a service token must steal the encryption key through attacking the user's mobile device or the payment service provider's storage. This significantly increases the difficulty of forging service token.

In the current market, the most popular way to pass a service token from a mobile device to a mobile payment service provider is to scan a QR code on a merchant's terminal. The service token is encoded in the QR code, and the QR code is shown in the mobile payment application. A QR code can be generated under industrial standards that cover the encoding of data as QR codes. Alternatively, a QR code can also be generated under a scheme customized by a payment service provider. Compared to customized QR code, a QR code generated under industrial standards requires fewer modifications on merchants' terminals.

6.5.2.2 Payment Credential Security

In a PTB payment service, payment tokens are used as users' payment credentials. Due to the usage of payment tokens, a PTB payment service provider does not save any information

www.elsevierdirect.com

of users' payment cards in its database or on users' mobile devices. Alternatively, the PTB payment service provider should securely store payment tokens in a cloud storage or on users' mobile devices, which are detailed in 6.6.1.

In an STB payment service, if the mobile payment service provider has not registered with any token service, it needs to store users' payment cards information in its database. In this case, to prevent fraud transactions caused by the disclosure of payment cards information, the STB service provider could replace the payment cards information with secure tokens in its storage.

Unlike payment tokens which replace sensitive payment card information in transaction authorization processes, secure tokens that are used to replace the sensitive payment card information contain a non-sensitive token value for data-at-rest or after payment authorization process has begun. These secure tokens are also referred to as post-authorization tokens (Marianne Crowe, Susan Pandy, D. L. S. M.).

Some industrial standards have been published to guide the generation and usage of secure tokens in mobile payment. Secure token models for Point-of-Sale (POS) and e-commerce have existed since the mid-2000s, driven primarily by the issuance of the PCI SSC Data Security Standard (PCI-DSS) in 2004, which defines business requirements for protecting cardholder data (PCI Security Standards Council, 2016). The intent of the PCI SSC 2011 Tokenization Guidelines (PCI SSC) is to use tokens to secure and protect sensitive information (i.e., low value token), not to create a token to replace a payment credential used during a financial transaction (i.e., high value token) and processed over a payment network. American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X9 has also developed tokenization specifications for bank card payment industry use in ANSI X9.119 standard (ANSI ASC X9, ANSI ASC X9.119). The ANSI X9.119 is written by X9 F6 work group to address tokens used after initial payment authorization, such as when an acquirer provides tokenization services to merchants. Through deploying a security tokenization system under these standards, the mobile payment providers can effectively decrease fraud exposure of sensitive payment cards information.

6.6 On-Device Level Issues

PTB payment uses card emulation techniques, which allow the mobile devices to directly communicate with POS terminals like normal payment cards. In this section, we introduce two mainstream card emulation techniques: secure element-enabled card emulation and host card emulation. We analyze the security challenges in implementing each technique and comment on the solutions to address these challenges. Moreover, in most in-store mobile payment services, user authentication schemes are used as the primary on-device protection to prevent

illegitimate users from accessing the payment services. Hence, we also give a comprehensive comparison of user authentication schemes on mobile devices.

6.6.1 Payment Card Emulation

In PTB payment, card emulation technology enables a mobile device with NFC applications to emulate any contactless smart card when tapped on POS terminal (Smart card alliance, Host Card Emulation (HCE) 101). Currently, two types of card emulation technology are widely used in mobile payment services: secure element (SE)-enabled card emulation and Host Card Emulation (HCE). Mobile payment services that apply SE-enabled card emulation technology store the card emulation applet and payment credentials in an SE which is a tamper-resistant smart card module. On the other hand, HCE services store the payment credentials and related data at somewhere other than an SE, e.g., in the cloud or in a Trusted Execution Environment (TEE) of the mobile device.

6.6.1.1 Secure Element (SE)-Enabled Card Emulation

The Secure Element (SE) is defined by GlobalPlatform as "a tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities" (GlobalPlatform).

GlobalPlatform is a technical organization that develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology (Wiki Pedia, GlobalPlatform Wiki). GlobalPlatform has been working on the standardization of supporting SEs in the contactless environment since 1999. It has published some specifications to guide the implementations and managements of SEs, e.g., GlobalPlatform Card Specification v2.3 (Wiki Pedia, GlobalPlatform Card Specification v2.3) and Management of Multiple Contactless Secure Elements v2.0 (Wiki Pedia, Requirements for NFC Mobile: Management of Multiple Contactless Secure Elements v2.0). These specifications have already been supported by most manufacturers.

Mobile payment services based on SE-enabled card emulation require hardware SEs on mobile devices. A hardware SE includes a microcontroller CPU, an operating system, different types of memory (ROM, EEPROM, and RAM), and cryptographic engines. An SE stores data in security domains that adhere to GlobalPlatform specifications. Each service provider is assigned with a specific domain, which is protected by cryptographic keys to prevent unauthorized access. The level of protection and assurance offered by the SE allows mobile payment

www.elsevierdirect.com

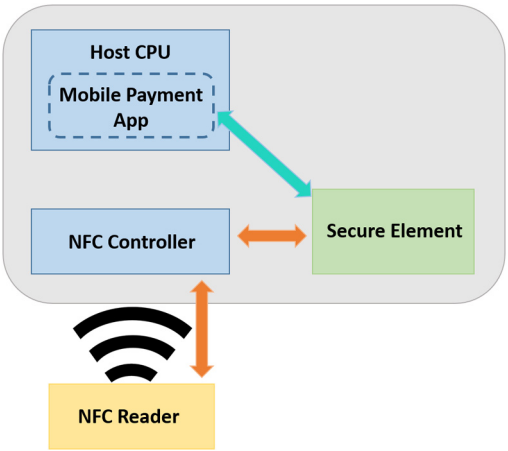


Figure 6.4: NFC communication in SE-based mobile payment services.

service providers to store a payment token on mobile devices, exactly like storing payment card information on physical cards.

SE can reside in an embedded secure smart card chip on a mobile device, on the Subscriber Identity Module (SIM) or Universal Integrated Circuit Card (UICC), or on a secure digital (SD) card that can be inserted into the mobile phone. Embedded SEs can only be deployed by mobile device manufacturers, while SEs on SIMs and UICCs can only be deployed by the mobile network operators. Therefore, a mobile service payment provider must cooperate with the third party, such as a mobile device manufacturer or a network operator, who can deploy and control the SE chip. This makes it cumbersome for a mobile payment service provider to distribute and manage the payment services in an embedded SE.

Fig. 6.4 illustrates the communication between a mobile device and a POS terminal in SE-based mobile payment. In SE-based card emulation, an NFC card emulation applet is running in the SE. The SE itself communicates with the NFC POS terminal. Therefore, no Android application is involved in the transaction at all. When a user holds his/her mobile device over an NFC-enabled POS terminal, the NFC controller in the mobile device routes all data from the terminal directly to the SE. After the transaction authorization process, the mobile payment application running on the mobile OS can directly query the SE for the transaction status, and then notify the user about the status.

Generally, in an SE-based mobile payment service, an SE is responsible for communicating with: (1) the NFC controller, and through it, with contactless readers to perform transactions; (2) user-interfacing mobile payment applications running on the mobile OS; and (3) the credential provisioning infrastructure called the Trusted Service Manager (TSM), if appropriate (Smart card alliance, Host Card Emulation (HCE) 101).

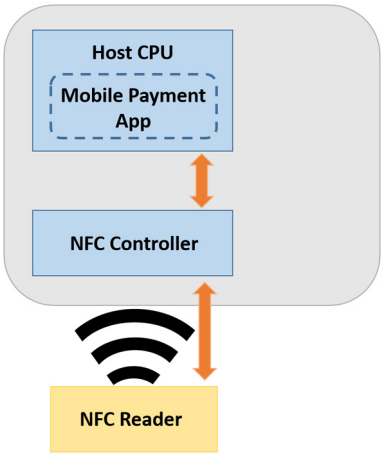


Figure 6.5: NFC communication in HCE-based mobile payment services.

6.6.1.2 Host Card Emulation (HCE)

Android 4.4 introduces a card emulation method, called Host Card Emulation (HCE), that does not involve a secure element (Google Inc., Host-based Card Emulation). HCE is a software architecture that provides an exact virtual representation of various electronic identity (access, transit, and banking) cards using only software (Wiki Pedia, Host Card Emulation). It enables mobile applications running on supported operating systems to offer payment services independently of hardware-based SEs and third party issuers of the secure chips.

Fig. 6.5 illustrates how host-based card emulation works. In an HCE-based mobile payment service, when a user holds his/her mobile device over an NFC-enabled POS terminal, the NFC controller in the mobile device directly routes all data from the terminal to the host CPU on which Android applications are running.

The HCE architecture in Android is based around Android *Service* components, which are known as HCE services. In Android OS, an HCE service that handles NFC transactions is associated with a certain mobile payment application. When the user taps a mobile device to an NFC-enabled POS terminal, the Android system first identifies which HCE service the POS terminal actually wants to talk to. Then, the communication is routed from the POS terminal to the HCE service running in the host CPU. After that, the HCE service passes transaction information, such as payment credentials, to the POS terminal to complete the transaction.

However, this HCE service does not care where the payment credentials (e.g., payment tokens and other cryptographic keys used to generate the dynamic cryptogram) are stored. It just makes sure that the payment data is safely transported to the NFC controller and out to the

www.elsevierdirect.com

NFC reader. In an HCE-based payment service, payment credentials may be stored: (1) in the host OS on the mobile device, (2) in the cloud, (3) in a TEE on the mobile device, or (4) in an SE. The location of credentials should be decided based on a trade-off between flexibility and security.

In an HCE-based mobile payment service, payment credentials can be hosted in the local mobile payment application. It has made mobile payment services available on mobile devices that are not equipped with an SE. However, host storage is considered as the least secure option, and is not permitted by the Visa and MasterCard HCE specifications without the use of additional software security tools. Payment credentials stored in the local application may be exposed by physical storage analysis or malware resident on the device. Even worse, an attacker who has rooted an Android device can access all data stored on the device including payment credentials and related cryptographic keys.

To reduce the risk of exposing payment credentials from the local payment application, additional software security tools, such as tamper-proofed software and white box cryptography, can be applied. For example, payment credentials can be hidden in the mobile payment application using white box cryptography. The white box cryptography prevents the keys from being retrieved even if the original source code is available.

Sensitive payment data can also be stored in the cloud. The HCE service can connect with a back-end server in the cloud in real-time or at given time intervals and retrieve credentials to exchange with the POS terminal. To improve the security of the data stored in the cloud, the cloud should deploy a hardware security module (HSM), which functions like an SE on a mobile device.

Although real-time retrieval of payment credentials from the cloud is possible, it is an unlikely option. This is because network latency may result in a poor user experience or even worse, the Internet connection may not be available when a user purchases in-store. To avoid request a payment token from the cloud in real-time, a few limited use payment tokens can be stored on the mobile device. This technology is now supported by Android Pay. In particular, a few payment tokens with limited use capability (e.g., limited expiry time and transaction value) can be derived from a master payment token stored in the cloud. They are then distributed to a user's mobile device and refreshed from the cloud after being used. However, in this solution, limited use payment tokens are still stored in the local application and are exposed to security threats on the mobile device.

Compared to standard mobile OS, TEE provides a more secure solution for sensitive computation, such as generating dynamic cryptogram, and payment credential storage on the mobile device. Samsung Pay provides HCE-based mobile payment services using TEE. The TEE, composed of software and hardware, is a secure area of the main processor in a smartphone

or any connected device. The TEE is isolated from the standard mobile OS. It securely stores keys and implements the main cryptographic operations within the boundaries of the secure execution environment. Hence, the TEE offers a level of protection against software attacks originating from the mobile OS. GlobalPlatform specifications describe how applications can securely reside in the TEE, including how to interface trusted applications with the TEE, and how to communicate between applications running on the mobile OS and trusted applications residing in the TEE.

Although the TEE delivers a higher level of security than what the standard mobile OS offers, it still does not provide the same security level as an SE. A major advantage of an SE is the tamper-resistance. Hence, a hybrid model that stores payment credentials in an SE can also be used in an HCE-based mobile payment service. However, even an HCE-based mobile payment service that stores payment data in an SE is still less secure than an SE-based mobile payment service where both sensitive data and programs (applets) are deployed on a tamper-resistant hardware isolated from the host OS.

6.6.1.3 Comparison Between SE and HCE

HCE eliminates the dependence on hardware SE, introducing entirely new business plan considerations for PTB payment service providers. Although HCE offers greater flexibility than SE-enabled card emulation, it brings obvious disadvantages on security due to the less secure implementations.

Comparisons on some security issues between SE-enabled card emulation and HCE are given below:

- **Credential storage options.** In SE-based mobile payment, payment credentials are stored inside SEs and are highly tamper-proof. In HCE-based mobile payment, the location of credentials should be decided based on a trade-off between flexibility and security as discussed in Section 6.6.1.2.
- **Approach for managing payment credentials.** Payment credential are managed through Trusted Service Manager (TSM) infrastructure in an SE. In HCE-based mobile payment, payment credentials are directly managed by the payment application. Once additional risk mitigation techniques are applied in HCE-based payment services, the complexity of the payment credentials management grows.
- **Risk of malware attack.** In an SE-based mobile payment service, the execution of payment data is completely isolated from the mobile OS in the transaction authorization process. In an HCE-based payment service, the mobile payment application that resides in an open and connected mobile OS is subject to malware attacks like any other mobile applications on the mobile device.

www.elsevierdirect.com

Table 6.2: Comparison on user authentication methods.

Mobile payment service	User authentication method
Apple Pay	Fingerprint; PIN code
Android Pay	PIN code; gesture passcode
Samsung Pay	Fingerprint; PIN code
Alipay	PIN code;gesture password;password-free;voice
Wechat Pay	PIN code

6.6.2 User Authentication

User authentication on mobile devices plays an important role in preventing fraud transactions initiated by illegitimate users. User authentication methods supported by mainstream mobile payment services are summarized in Table 6.2.

In PTB payment, payment applications automatically run in the OS after users unlock their mobile devices, and then communicate with POS terminals when users check out. To unlock mobile devices, users should be authenticated locally on mobile devices, e.g., swiping a fingerprint, and entering a PIN.

In STB payment, a mobile payment service provider is required to verify a user's service account credential (i.e., service token) contained in a transaction authorization request. To decrease the burdens on the mobile payment service provider to manage users' service accounts, Fast Identity Online (FIDO) architecture provides an approach for online mobile payment service providers to authenticate users locally on mobile devices. The usage of FIDO architecture can also mitigate the risk of the disclosure of users' service account credentials on communication channels.

FIDO Universal Authentication Framework (UAF) protocol uses public key cryptography techniques to provide online authentication. The user registers his/her mobile device to the online service (e.g., mobile payment service) by selecting a local authentication mechanism such as swiping a fingerprint, looking at the camera, speaking into the mic, entering a PIN, etc. The client device stores the user's credential information such as biometric authentication data locally on the user's device. Then, the user's device creates a new key pair, retaining the private key on the device and registering the public key with the online service. Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. Once the user passes the local authentication, the client device proves possession of the private key to the service by signing a challenge. The server validates the signature using the registered public key. PayPal is the first mobile payment service provider to use the fingerprint verification functionality in the Galaxy S5 handset launched in 2014 with FIDO Ready software (FIDO Alliance).

www.elsevierdirect.com

6.6.2.1 Non-biometric User Authentication

In non-biometric user authentication schemes, a user provides an alphanumerical or graphical password on a user interface as user credential. Alphanumerical passwords (which are also referred to text-based passwords) are one of the most widely used methods for user authentication on mobile devices. In most mobile payment services, to provide a desirable user experience, users are allowed to enter a short PIN code as their user credentials for transaction authorization. However, the short PIN codes are weak and vulnerable to many known attacks, such as exhaustive attacks, dictionary attacks, and shoulder-surfing attacks.

As a more user-friendly alternative to text-based passwords, graphical passwords systems have been proposed and applied on mobile devices. These schemes are motivated by psychology research results suggesting that the human brain is particularly well-suited to remember graphical information (Standing et al., 1970). Currently, Android's Unlock Pattern scheme (i.e., referring to gesture passcode in Table 6.2) is the most deployed graphical password in Android OS. It is designed by modifying Pass-Go (Tao and Adams, 2008) with minor adoptions to accommodate for the size of mobile devices. In the Android's Unlock Pattern scheme, a user is required to draw a pattern on a 3×3 grid (i.e., a sequence of lines connecting the dots) as his/her secret for authentication. However, a research (Uellenbeck et al., 2013) published in 2013 indicates that the security offered by the scheme is lower than the security of only three-digit randomly-assigned PINs for guessing 20% of all passwords.

Since people are prone to carry and use mobile devices everyday and everywhere, even in crowded places, both alphanumerical and graphical password schemes on mobile devices are vulnerable to shoulder-surfing attacks, in which a password entered on a user interface is observed or recorded by a nearby adversary. There are two types of shoulder-surfing attackers. The shoulder-surfing attackers of the first type are weaker adversaries (e.g. cognitive shoulder-surfing (Roth et al., 2004)) whose capabilities are restricted to a human. They do not have any automatic recording device and rely only on manual tools, such as paper and pencil. Hence, such adversaries are not able to capture the complete interaction between user and server (Roth et al., 2004). A replay-based shoulder-surfing attack against the graphical password systems without recording devices was analyzed in Dunphy et al. (2010). The shoulder-surfing attackers of the second type are stronger adversaries who are equipped with automatic recording devices, such as a concealed camera, to capture the complete interactions between user and server. Thus, such adversaries may analyze and recover the underlying password from the user's inputs after recording sufficient rounds of authentication (Li et al., 2015b).

Although some non-biometric authentication schemes which are resilient to shoulder-surfing attacks are proposed in academia (see examples in Renaud and Maguire (2009), Renaud and Olsen (2007), Wang et al. (2013)), these schemes still cannot completely mitigate the risk of shoulder-surfing attacks on mobile devices. Biometric user authentication might be a practical solution to thoroughly address shoulder-surfing issues.

www.elsevierdirect.com

6.6.2.2 Biometric User Authentication

The release of Android 4.0's face unlock system at the end of 2011 (Google Inc., Introducing Android 4.0) and the iPhone 5S' Touch ID system two years later (Google Inc., Using Touch ID on the iPhone) has suddenly brought biometric authentication to wide deployment on mobile devices. As shown in Table 6.2, biometric user authentication mechanisms have been supported by major mobile payment service providers. Besides the authentication methods summarized in Table 6.2, ECG signals captured and analyzed on smartbands can also be used to authenticate users in mobile payment. For example, MasterCard has cooperated with Nymi smart band in Canada to authenticate a user for in-store purchases only based on the ECG signal detected by the user's Nymi smart band (Al Sacco). When a user checkouts at a POS terminal that supports NFC and MasterCard's PayPass, Nymi band authenticates the user based on his/her ECG signals and transfers the authentication result to the POS terminal.

Biometric authentication schemes free the users from remembering passwords, thus they can bring a more desirable user experience compared to traditional non-biometric authentication methods. However, some inherent limitations still pose negative effects on the usability of biometric authentication. First, the recognizability of biometric signals still needs to be improved. For examples, the accuracy of face recognition authentication suffers in dark environment (Trewin et al., 2012), the accuracy of voice recognition authentication is greatly affected by accents (Lei et al., 2013), and the accuracy of fingerprint authentication is barely satisfactory with dirty hands (Bhagavatula et al., 2015). In addition, subtle issues in deployment, like the height of face scanners and the hygiene of fingerprint scanners, also have a major impact on user perception and therefore adoption (Maple and Norrington, 2006). Moreover, some biometric authentication methods require additional dedicated hardware supports increasing costs of production, such as a fingerprint scanner on a mobile device or a wearable smart band, which negatively affects their deployment.

Although biometric authentication schemes are resistant to shoulder-surfing attacks, they are still vulnerable to some sophisticated attacks. For example, in authentication systems based on voice-recognition, synthetic speech generated from synthesis systems (Masuko et al., 2000; De Leon et al.) or voice conversion techniques (Stylianou et al., 1998; Stylianou, 2009) can be used to modify an impostor's voice to sound like that of the claimed speaker to attack the voice recognition system. For another example, static face-recognition systems could be fooled by a photograph/video that contains a legitimate user's face (Furnell and Evangelatos, 2007). In response to such a potential threat, a dynamical face-recognition system that authenticates a user by measuring the consistency between device movement data from the inertial sensors and the head pose changes from the facial video captured by the built-in camera has been proposed in Li et al. (2015a). Besides these known attacks to biometric authentication

systems, more efforts should be made to explore the potential attacks on biometric authentication schemes, especially in some certain environment, and eventually propose more secure biometric authentication schemes to mitigate the risk of these potential attacks.

6.6.2.3 Free Authentication Transaction

To simplify user's payment process, some mobile payment services allow users to check out in-store without user authentication. For example, Dash mWallet supports in-store payment without PIN on iOS and Android phones; Apple Pay allows users to pay via iWatch by double clicking the side button; Alipay supports users to make payment without entering PIN in some retailers.

Although these free authentication schemes provide good user experience, they increase the risks of frauds initiated by an unauthorized user. Mobile payment service providers can reduce such risks by applying strong risk management models which validate a user by analyzing his/her consumer behaviors, such as store location and purchase time. In addition, the amount of the purchase should be limited in free authentication purchases. The limitation on the amount of the purchase is already widely used in traditional credit card payment without PIN. Besides that, to detect unauthorized payments in time, mobile payment service providers should notify their users about transaction details via e-receipts.

Mobile payment service providers can also try to implement user authentication systems which authenticate users without users' interactions or perceptions. For example, Alipay has cooperated with Mi Band to authenticate a user of Alipay by validating the device ID of the user's Mi Band (Emma Lee). Before making in-store payment, a user needs to connect his/her Mi Band's device ID with his/her Alipay account. When purchasing in a store, the user just places the Mi Band near the phone. Then, the Mi Band connects to the phone via Bluetooth, and the Alipay Wallet installed on the phone extracts the Mi Band's device ID. Payments can be processed only when the Mi band's device ID pairs with its pre-set Alipay account.

6.7 Conclusion

This chapter discusses the security issues arising from the new entities introduced into the payment system by in-store mobile payment, and analyzes the solutions to address these issues.

In current mobile payment services, tokenization is the key component for preventing fraud transactions resulted from payment credentials disclosure. TSPs should comply with the EMVCo payment tokenization specification to improve the security of token issuance and authorization. In particular, as the authorized party for token issuance, a TSP should ensure

www.elsevierdirect.com

that a payment token is issued to a legitimate TR for a legitimate cardholder by defining and performing ID&V methods, token assurance schemes, and domain restriction controls. Besides that, to offer secure tokenization and de-tokenization during transaction authorization, a TSP should securely store the payment token to PAN mappings in a token vault which could prevent data disclosure and ensure instantaneous data accessibility.

Any mobile payment service provider that performs as a TR should take the security responsibilities of a TR. When registering with a TSP, a TR should comply with the TSP's proprietary registry requirements and honestly provide sufficient information, e.g., token domain restriction controls, for registration. In the token provision process, the TR should cooperate positively with the TSP, and store the issued payment tokens in a secure location.

In STB payment, a mobile payment service provider should ensure the secure generation, transmission, and verification of the service tokens. If the mobile payment service provider has not registered with any token service, to prevent the disclosure of the sensitive cards information, it could replace the sensitive payment card information with a non-sensitive token value for data-at-rest or after payment authorization process has begun. In PTB payment, the usage of payment tokens requires the PTB payment service provider to securely store payment tokens in a cloud storage or on users' mobile devices.

Among all on-device designs, card emulation is basically the cornerstone of mobile payment. We introduce two mainstream card emulation techniques, SE-enabled card emulation and HCE, and give a comparison on the security between these two techniques. The implementations of card emulation should consider both security requirements and hardware/software costs. User authentication on mobile devices is a significant step to prevent illegitimate access in mobile payment services. We give a comparison on the usability and security among the existing non-biometric, biometric, and free authentication schemes. It still remains a wild design space for user authentication schemes to satisfy specific security requirements in mobile payment environment and provide good user experience.

Overall, a positive collaboration among all participants in the payment system should be valued and achieved to secure in-store mobile payment.

References

Al Sacco. Nymi Band uses your heartbeat to secure mobile payments. [EB/OL]. http://www.cio.com/article/2969293/wearable-technology/nymi-band-uses-your-heartbeat-to-secure-mobile-payments.html.

ALLIANCE, S. C. Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization. In: Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization.

ANSI ASC X9. ANSI ASC X9.119. [EB/OL]. http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.119-2013.

Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F., Savvides, M., 2015. Biometric authentication on iPhone and Android: usability, perceptions, and influences on adoption, In: Proc. USEC.
De Leon, P.L., Pucher, M., Yamagishi, J. Evaluation of the vulnerability of speaker verification to synthetic speech.
Dunphy, P., Heiner, A.P., Asokan, N., 2010. A closer look at recognition-based graphical passwords on mobile devices. In: Proceedings of the Sixth Symposium on Usable Privacy and Security. ACM, p. 3.
Emma Lee. Xiaomi Wristband Supports Mobile Payment Enabled by Alipay. [EB/OL]. http://technode.com/2015/04/02/xiaomi-wristband-supports-alipay/.
EMVCo. Technical framework. In: EMVCo Payment Tokenisation Specification.
FIDO Alliance. The FIDO Alliance Announces First FIDO Authentication Deployment. [EB/OL]. https://fidoalliance.org/the-fido-alliance-announces-first-fido-authentication-deployment-%E2%88%92-paypal-and-samsung-enable-consumer-payments-with-fingerprint-authentication-on-new-samsung-galaxy-s5/.
Furnell, S., Evangelatos, K., 2007. Public awareness and perceptions of biometrics. Computer Fraud & Security 2007 1, 8–13.
GlobalPlatform. GlobalPlatform made simple guide: secure element. [EB/OL]. https://www.globalplatform.org/mediaguideSE.asp.
Google Inc. Host-based Card Emulation. [EB/OL]. https://developer.android.com/guide/topics/connectivity/nfc/hce.html.
Google Inc. Introducing Android 4.0. [EB/OL]. http://www.android.com/about/ice-cream-sandwich/. Accessed October 2014.
Google Inc. Using Touch ID on the iPhone. [EB/OL]. http://support.apple.com/kb/ht5883.
Lei, X. Senior, A.W. Gruenstein, A. Sorensen, J., 2013. Accurate and compact large vocabulary speech recognition on mobile devices, in: INTERSPEECH, pp. 662–665.
Li, Y., Li, Y., Yan, Q., Kong, H., Deng, R.H., 2015a. Seeing your face is not enough: an inertial sensor-based liveness detection for face authentication. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 1558–1569.
Li, Y., Yan, Q., Deng, R.H., 2015b. Leakage resilient password systems: attacks, principles, and usability. In: Leakage Resilient Password Systems. Springer, pp. 1–28.
Maple, C., Norrington, P., 2006. The usability and practicality of biometric authentication in the workplace. In: The First International Conference on Availability, Reliability and Security, 2006. ARES 2006. IEEE, p. 7.
Marianne Crowe, Susan Pandy, D. L. S. M. Is payment tokenization ready for primetime? Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta, BetterBuyDesign.
MasterCard. Mastercard sees continued momentum in U.S. EMV adoption. [EB/OL]. http://newsroom.mastercard.com/press-releases/mastercard-sees-continued-momentum-in-u-s-emv-adoption/.
MasterCard Inc. MasterCard Digital Enablement Service (MDES): Making Digital Payments Happen. http://newsroom.mastercard.com/2014/09/10/mastercard-digital-enablement-service-mdes-making-digital-payments-happen/.
Masuko, T., Tokuda, K., Kobayashi, T., 2000. Imposture using synthetic speech against speaker verification based on spectrum and pitch. In: INTERSPEECH. Citeseer, pp. 302–305.
McNamara, J. EMV Chip Card Security Vs. Magnetic Stripe Card Security. [EB/OL]. https://pos.toasttab.com/blog/emv-chip-card-magnetic-stripe-card-security.
PCI Security Standards Council, 2016. Payment Card Industry (PCI) Data Security Standard V3.2. [EB/OL], APR 2016. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1468994844566.
PCI SSC. Information Supplement: PCI DSS Tokenization Guidelines. [EB/OL]. https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.
Pedia, W. Emv. [EB/OL]. https://en.wikipedia.org/wiki/EMV.
Pedia, W. Magnetic stripe card. [EB/OL]. https://en.wikipedia.org/wiki/Magnetic_stripe_card.
Renaud, K., Maguire, J., 2009. Armchair authentication. In: Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology. British Computer Society, pp. 388–397.

Renaud, K., Olsen, E.S., 2007. Dynahand: observation-resistant recognition-based web authentication. Technology and Society Magazine, IEEE 26 (2), 22–31.
Roth, V., Richter, K., Freidinger, R., 2004. A pin-entry method resilient against shoulder surfing. In: Proceedings of the 11th ACM Conference on Computer and Communications Security. ACM, pp. 236–245.
Smart Card Alliance. EMV and Parking. [EB/OL]. http://www.smartcardalliance.org/downloads/EMV-and-Parking-White-Paper-FINAL-May-2016.pdf.
Smart card alliance. Host Card Emulation (HCE) 101. [EB/OL]. http://www.smartcardalliance.org/downloads/HCE-101-WP-FINAL-081114-clean.pdf.
Standing, L., Conezio, J., Haber, R.N., 1970. Perception and memory for pictures: single-trial learning of 2500 visual stimuli. Psychonomic Science 19 (2), 73–74.
Stylianou, Y., 2009. Voice transformation: a survey. In: IEEE International Conference on Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE, pp. 3585–3588.
Stylianou, Y., Cappé, O., Moulines, E., 1998. Continuous probabilistic transform for voice conversion. IEEE Transactions on Speech and Audio Processing 6 (2), 131–142.
Tao, H., Adams, C., 2008. Pass-go: a proposal to improve the usability of graphical passwords. IJ Network Security 7 (2), 273–292.
Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., Ben-David, S., 2012. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In: Proceedings of the 28th Annual Computer Security Applications Conference. ACM, pp. 159–168.
Uellenbeck, S., Dürmuth, M., Wolf, C., Holz, T., 2013. Quantifying the security of graphical passwords: the case of Android unlock patterns. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, pp. 161–172.
Visa Inc. Visa Launches Innovative Token Service. [EB/OL]. http://investor.visa.com/news/news-details/2014/Visa-Launches-Innovative-Token-Service/default.aspx.
Wang, Z., Jing, J., Li, L., 2013. Time evolving graphical password for securing mobile devices. In: ASIA CCS'13 Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. ACM, pp. 347–352.
Wiki Pedia. 3-D Secure. [EB/OL]. https://en.wikipedia.org/wiki/3-D_Secure.
Wiki Pedia. GlobalPlatform Card Specification v2.3. [EB/OL]. http://www.globalplatform.org/specificationscard.asp.
Wiki Pedia. GlobalPlatform Wiki. [EB/OL]. https://en.wikipedia.org/wiki/GlobalPlatform.
Wiki Pedia. Host Card Emulation. [EB/OL]. https://en.wikipedia.org/wiki/Host_card_emulation.
Wiki Pedia. Requirements for NFC Mobile: Management of Multiple Contactless Secure Elements v2.0. [EB/OL]. http://www.globalplatform.org/specificationscard.asp.

CHAPTER 7

Blockchain – From Public to Private

Roy Lai, David LEE Kuo Chuen

Contents

7.1 Introduction 146

7.2 Terminology 146

7.3 Overview of the Bitcoin Blockchain 147

7.4 Characteristics of Blockchain 149

7.4.1 Distributed Consensus Protocols 149

7.4.2 Liveness and Safety 149

7.4.3 No Correlation Between Nodes Failures 149

7.4.4 Resiliency 150

7.4.5 Types of Fault 150

7.4.6 Synchrony 151

7.4.7 Authentication and Non-repudiation 152

7.4.8 Scalability and Performance 154

7.4.9 Turing-Complete 155

7.4.10 Smart Contracts 155

7.4.11 Smart Contract Oracle 157

7.5 Types of Blockchains 157

7.5.1 Token-Based Consensus Protocol Blockchains (With Mining) 157

7.5.1.1 Ethereum 158

7.5.1.2 Proof-of-Stake 158

7.5.2 Token-Based Consensus Protocol Blockchains (Without Mining) 159

7.5.2.1 Tendermint 159

7.5.2.2 Ripple Protocol Consensus Algorithm (RPCA) 160

7.5.3 Token-Less Blockchain Technologies 160

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00007-3
Copyright © 2018 Elsevier Inc. All rights reserved.

7.5.3.1 Practical Byzantine Fault Tolerance (PBFT) 161
7.5.3.2 Hyperledger 161
7.5.3.3 R3 Corda 162
7.6 Conclusion 162
7.6.1 Step 1: Decide if Blockchain is the Right Solution for the Problem 162
7.6.2 Step 2: Assess the Benefits and Caveats 163
7.6.3 Step 3: Assess the Technical Design Considerations 164
7.6.4 Step 4: Assess the Functional Design Considerations 164
7.6.5 Step 5: Assess the Non-functional and Operational Considerations 165
7.6.5.1 Identity and Key Management 165
7.6.5.2 Privacy and Confidentiality 165
7.6.5.3 Existing Systems Integration and Interoperability 165
7.6.5.4 Regulations 166
7.6.5.5 Production Rollout and Testing 166
7.6.5.6 Operational Readiness 166
Appendix 1: The Six Layers of Blockchain 167
Appendix 2: Notable Blockchain and Distributed Ledger Technologies 171
References 176
Notes 177

7.1 Introduction

The term "blockchain" originally refers to the underlying technology used in implementing the Bitcoin protocol and network based on a paper published by Satoshi Nakamoto in 2008. The present-day use of this term generally refers, in a broad stroke, to a myriad of nascent distributed ledger technologies that are either associated with or evolved from the invention of Bitcoin. This writing seeks to provide the readers with some guidance on technological considerations when deciding to apply blockchain for commercial use.

7.2 Terminology

Terminology means everything in the world of blockchain where technologies are largely nascent and standard authoritative definitions seldom exist. Blockchain terms oftentimes are

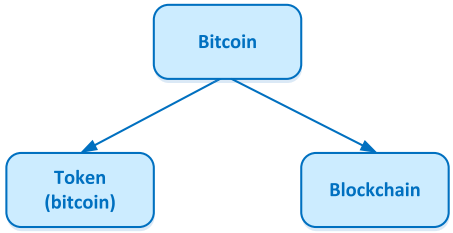
highly contextual and it is often helpful to know the historical and evolutionary path of the technology to make sense of its purpose.

- The term **blockchain** was originally used for describing the distributed record keeping system used by the Bitcoin protocol but is now generally used to describe any distributed ledger technologies that are inspired from the Bitcoin's blockchain design. The term Distributed Ledger Technology (DLT) or Replicated, Shared Ledger refers to a distributed record keeping system that is append-only and secured by means of consensus protocols. This writing will use Blockchain to refer to DLT as well as blockchain because it is still a more prevalently adopted nomenclature in spite that some DLT do not use a blockchain model at all.
- The term **private blockchain** (permissioned ledger) refers to Blockchain that requires authentication of participant identities and authorization of participant's permission-level of access on the Blockchain. This writing will use Private Blockchain to refer to Permissioned Ledger as well.
- The term **public blockchain** (permissionless ledger) refers to Blockchain that does not require approval or authorization for access.

7.3 Overview of the Bitcoin Blockchain

This section aims to give an overview on the major concepts utilized in the original Bitcoin blockchain design. At the same time, it serves as a frame of reference for comparison purposes in subsequent sections of this writing.

- **Bitcoin** (uppercase "B") refers to the protocol and the network based on a paper written by Satoshi Nakamoto in 2008 (Nakamoto, 2008). The **bitcoin** (lowercase "b") cryptocurrency is implemented using the Bitcoin protocol and released in January 2009. The term **blockchain** gained prominence in 2014 when the industry attempted to decouple the technology from its token that is often characterized as a currency of choice for drugs and other illegal trades.



- Bitcoin is not the first attempt at creating a digital currency and the challenge largely lies in solving the so-called **Double-Spend** problem. Unlike physical objects, digital currency

www.elsevierdirect.com

is just data. It can be copied and sent to two different recipients at the same time. This is not difficult when using a central authority but Bitcoin is the first that successfully solves this problem in a fully decentralized manner. Thus, there is no single point of failure in Bitcoin's design as compared to a centralized one.

- Because Bitcoin network is designed to be publicly accessible by anyone without need for identification or permission, it must withstand a kind of problem called **Byzantine Generals' Problem (Lamport et al., 1982).** The Byzantine General's Problem assumes that there will be an unknown number of participants that are expected to misbehave and attempt to subvert the network. Byzantine General's Problem is often used in classical computer science to describe the challenges faced by distributed systems in achieving consensus over unreliable communication links.
- To solve this problem, Bitcoin must maintain a distributed record keeping system and a consensus protocol that can withstand the double-spend and byzantine general's problem:
  - The distributed record keeping system (**blockchain**) is designed in such a way that is constantly appending new blocks of validated records to the end of its chain. The chain can only grow and blocks cannot be removed or amended once confirmed and appended. Each new block is cryptographically chained to the previous block using a block hash derived from the combined hash of the list of records and the hash of the previous block along with a number called the **nonce**.
  - The consensus protocol (**Proof-of-Work** or **PoW**) is designed in such a way that requires all nodes on the network to compete for the reward of adding a block of records to the end of the chain. This competition involves the search for a nonce by sheer brute-force use of processing power such that the resulting block hash is lower than the target set by the network. The system also defines a fixed block frequency which determines the average amount of time the winning node will take to find such a nonce.
- Because there is a chance that different nodes may find the correct result almost simultaneously, the blockchain may **fork**[1] temporarily and parallel chains can co-exist temporarily. When such an event occurs, the nodes will only pick the longest[2] chain.
- This creates an incentive model whereby the winning node that adds a block to the blockchain gets rewarded with the digital tokens – bitcoins. In order for an attacker to subvert the network, not only must it compete for the right to add a block but must also compete to produce the longest chain. This is how it dis-incentivizes attacks by making it economically unfeasible for malicious actors to spawn multiple nodes in order to game the system (known as **Sybil attack**).

7.4 Characteristics of Blockchain

Because Blockchain is an umbrella term, it is easy to confuse the scope of its function. This section aims to identify the common characteristics and assumptions among various types of blockchains.

7.4.1 Distributed Consensus Protocols

Although Proof-of-Work has probably garnered the most fame from Bitcoin's success, it is hardly the only or the best consensus protocol (and strictly speaking not a distributed consensus protocol in the traditional sense) in existence. It is designed to address a very special use case under a very unique set of operating conditions and may not be that applicable beyond the bitcoin use case.

Distributed consensus protocols have been an area of research in the realm of distributed systems for over more than a decade. The only problem is that most of this research has never made it to a global scale like Bitcoin and operating within a highly asynchronous environment like the Internet.

7.4.2 Liveness and Safety

All consensus protocols are designed to guarantee either one or two of these properties under different conditions.

Safety means nothing bad will happen during execution. Usually this refers to the consensus protocol's ability to prevent the overwriting or corruption of a previous validated state.

Liveness means something good will eventually happen. Usually this refers to the consensus protocol's ability to guarantee message sent from the sending node will eventually reach the destination node.

7.4.3 No Correlation Between Nodes Failures

This is a key assumption in most consensus protocol such that a single vulnerability discovered in the protocol implementation will not jeopardize the entire system. In practice, it is achievable by introducing diversification into the network by means of using different implementations of code (N-version Programming), different operating systems platform (operating systems diversity), or different types of hardware.

www.elsevierdirect.com

7.4.4 Resiliency

Resiliency is a design measurement of consensus system. It is based on the maximum number of adversary nodes that the protocol is designed to tolerate in order to guarantee safety and liveness under different fault conditions. For instance, a resiliency of 100% means the protocol is able to guarantee safety and liveness for any number of adversary nodes. A resiliency of 33% means the protocol is able to guarantee safety and liveness if the number of adversary nodes does not exceed 33% of the total number of nodes.

7.4.5 Types of Fault

All consensus protocols are designed to help the system of nodes to agree on one single value. This is not an issue under normal conditions. However, when the nodes are not behaving the way they are expected to behave, then the system may become difficult to terminate in agreement. That is why understanding the types of fault and trade-offs available it is important to choose the required consensus protocol. There are two major types of faults we are generally concerned with: Fail-Stop Fault and Byzantine Faults.

Fail-Stop Fault. Describes the most basic types of fault which means that the system will stop the moment it runs into an error. This is a less difficult problem to deal with because it is relatively easy to detect. This type of fault does not include data corruption fault or node collusion; those faults fall under the Byzantine category.

- **Paxos (Lamport, 1998)** is the most established consensus protocol for this type of faults. It is a leader-based consensus protocol that was developed more than 15 years ago and is notoriously complex to implement as it is designed to handle all cases of non-Byzantine faults. Paxos always guarantees safety, which means that it will always converge to one value (no forks) and the value will eventually reach all nodes. However, in asynchronous systems, Paxos cannot guarantee it will continue to make progress with more than 50% failures. Paxos is being used by Google's Chubby service (Burrows, 2006) and Microsoft's Autopilot cluster management service.
- **RAFT** is a more recent consensus protocol that is also leader-based and is gaining popularity due to its simpler implementation and fewer moving parts than Paxos. One of the key difference is in the leader selection process. RAFT only selects the leaders from among the recent servers whereas Paxos allows the selection of leaders across all nodes.

Byzantine Fault. Describes the super class of all faults that includes fail-stop faults as well as malicious faults where results can be arbitrary due to data corruption, code error, node collusion and other forms of attacks. This is the hardest type of fault to catch because it is difficult to discern an honest node from an adversary node based on the result from one node alone.

www.elsevierdirect.com

The solutions designed to work with Byzantine Faults are known as Byzantine Fault Tolerance (**BFT**) systems. BFT is applied in aircraft and submarine systems and is applicable in low network latency environment but is typically at an extremely high-end cost.

- Traditional approach to solving Byzantine Fault involves the use of **State Machine Replication (Lamport, 1978).** One popular implementation of this technique called **Practical Byzantine Fault Tolerance** (PBFT) was introduced by Castro and Liskov in 1999 (Castro and Liskov, 1999). Because BFT systems were very expensive to build, they were only practical in critical real-time systems where Byzantine faults can result in very expensive failures (e.g. aircraft, submarine, space craft, etc.). PBFT shows that a solution can exist in a more conventional setting utilizing commodity hardware, over Internet with acceptable performance and being able to guarantee liveness and safety up to 33% resiliency.
- The Bitcoin blockchain is designed specifically to address Byzantine faults. Bitcoin Proof-of-Work (PoW) was commonly assumed to require 50% of adversary nodes in order to for the network to be subverted (also known as 51% attack) but it has been shown that only 25% are actually required (Eyal and Sirer, 2013). However, because of the sheer scale of Bitcoin compared to traditional systems, the resiliency is robust enough as demonstrated in practice.
- Since Bitcoin, several Proof-of-Work types, token-based or blockchain inspired consensus protocol hybrids have been developed. For instance, BitShares created the first Proof-of-Stake consensus protocol.
- Tendermint is a token-based BFT consensus protocol developed by combining Proof-of-Stake consensus protocol with DLS algorithm which assumes partial synchrony of network.
- Hyperledger is a token-less BFT consensus protocol developed by combining PBFT design with blockchain.
- Ripple Protocol Consensus Algorithm (RPCA), a token-based BFT consensus protocol that does not depend on the blockchain design, has a resiliency of 20% but provides a strong safety guarantee.

7.4.6 Synchrony

The consensus protocol depends heavily on the ability of the system to keep time. It has been proven that if the nodes of a distributed system have no bound on the time it takes for a message to be sent across to another node or that relative difference in processing speed between two nodes, then there is always a chance that the system cannot converge in consensus. This is because there is no way to tell whether it is due to process failure, slow processing, or network latency. This is called the FLP Impossibility Proof which is named after its inventors

www.elsevierdirect.com

Fischer, Lynch and Patterson who published a paper in 1985 called the "Impossibility of Distributed Consensus with One Faulty Process". This was a major breakthrough as it resolved a decade-long debate in the distributed systems circle over how consensus can be achieved in a fully asynchronous environment.

As a result, we can conclude that:

- In a synchronous environment, it is possible to find solutions that can guarantee consensus as long as the number of failures is less than the resilience level that the consensus protocol is designed to tolerate.
- In an asynchronous environment, however, it is not possible to find a solution that can guarantee consensus even with a single failure.

Because the Impossibility Proof cannot be circumvented, therefore it is a matter of relaxing the asynchronous requirement and finding the condition for achieving consensus with the number of failure nodes it can tolerate.

- Bitcoin Proof-of-Work (PoW) achieves a weak form of synchrony by controlling the block frequency and timestamp. The block timestamp is considered valid if its value lies between the median timestamp of the last 11 blocks on the chain and two hours after the network-adjusted time. If this is not valid then the block will not make it onto the chain. It was also shown that the Proof-of-Work protocol can provide strong consistency guarantee in an asynchronous network under known conditions (Pass et al., 2016).
- Dwork, Lynch and Stockmeyer published a paper in 1988 titled "Consensus in the Presence of Partial Synchrony". It illustrates a way, known as DLS algorithm, to circumvent the Impossibility Proof by assuming a partial synchrony environment. DLS is adapted by Tendermint's consensus design (Kwon, 2014) for use with blockchain with Proof-of-Stake.
- PBFT does not require synchrony for safety but requires synchrony to provide liveness. This basically means that each node will constantly resend messages upon timeout and message will eventually reach the other node as long as less than 33% of the nodes are malicious. PBFT is adapted for use by Hyperledger.
- Ripple Protocol Consensus Algorithm (RPCA) maintains a strong synchrony by requiring all validators nodes to submit candidate set of transactions within 2 seconds in order for the set to be proposed for committing into each validator's ledger. If validator does not receive any submission, the wait time is extended to 20 seconds.

7.4.7 Authentication and Non-repudiation

Authentication plays quite a significant role in BFT systems. According to Lamport, it is shown that a consensus can converge for any number of Byzantine nodes if they are authen-

ticated and the messages are unforgeable (non-repudiation). Without these conditions, no solution exists that can only tolerate more than 33% of Byzantine nodes. This is because the effect of Byzantine failure is more severe when it is unable to identify the erring node from the messages.

In practice, all blockchains can be divided between what is public (permissionless) and private (permissioned). Blockchains are highly use-case-specific technologies and the perceived lineage of private blockchain from public blockchain is perhaps what caused the most confusion. Private and public blockchains have very little in common apart from the concept that both are designed to provide shared record keeping access driven by participants' consensus and the option of running smart contracts.

Public blockchain assumes that anyone from the public Internet can join or leave the blockchain network without any need for providing forms of identification or asking for permission. In order for this to work, the design has to assume that altruism has no part to play and all actors are driven by incentives derived from the network. Proof-of-Work rewards miners with tokens as incentives that can be traded in the real-world for value. It creates a disincentive for any actor to subvert the network because the cost of real-world electricity investment will outweigh any gains that can be derived out of it. Mining for tokens is intrinsically an important part of public blockchain.

- Authentication is not used, therefore most classical distributed systems algorithms that require nodes to be known ahead of time will not work.
- Environment is assumed to be public Internet and therefore consensus protocols that assume synchronous environment will not work.
- Environment is assumed to be public Internet and anonymous, therefore susceptible to Sybil attacks and consensus protocols that cannot handle Byzantine failures are not applicable.
- Environment is assumed to be public Internet and can reach out to millions of users, therefore consensus protocols that assume a small LAN-based setting will not work.

Private blockchain assumes that all actors on the network are known and trusted; belonging to a controlled membership. These actors can be individuals such as employees and customers or organizations such companies or departments within companies. They conduct businesses by entering into contracts and agreements without the need for artificially created intrinsic incentives derived from the network. They are subjected to human rules and regulations as well as liabilities and obligations that are legally enforceable in the real world. Because the envi-

www.elsevierdirect.com

ronment is controlled and more sanitized, the conditions are more favorable for State Machine Replication based systems.

- Environment assumes members are known and access is permission-able, therefore solutions can be found to guarantee convergence of consensus with any number of malicious nodes.
- Environment assumes members are known and access is permission-able, therefore use of token mining to create an intrinsic incentive model is not required, and solution for a better performance can achieved.
- Private blockchain networks are for members only and participants are required to seek approval for access. A central authority (or group) may be required to perform the identity verification and approval of membership.
- Private blockchains may require different levels of access needs to be crafted for different roles of usage. For instance, to participate in consensus, to read or create a transaction, to execute a smart contract, all may require different sets of permissions to be authorized for the participant. A central authority (or group) may be required to perform permission review and approval.

In the appendix, we have given another way to classify blockchain with six different layers. The first three layers are common to all blockchains and decentralized ledger systems (DLS). The last three layers are optional. However, each layer has different choices and it is much like a menu choice for anyone who wishes to create a new blockchain or a DLS. Readers who wish to have a different perspective may read Appendix 1.

7.4.8 Scalability and Performance

Distributed consensus protocols are generally inversely proportional when it comes to scalability and performance. When the protocol can cater for high performance, it generally cannot scale very well. When the protocol can scale very well, it cannot achieve high performance (Vukolić, 2015). Scalability and performance is a topic of active research in consensus protocols.

- Bitcoin blockchain has a performance bottleneck from consensus latency of 60 minutes and a throughput of seven transactions per second (TPS) based on a block size of 1 MB which is a far cry from global credit card transaction average throughput (VISA, 2015) of 2000 TPS (with a peak of 56,000 TPS). Strictly speaking, Bitcoin does not cater for consensus finality because there is no way to tell in theory if the block will ever reshuffle on the chain due to forking. The only way to solve this is to reduce the chance of its happenings to an exceedingly small probability. It is therefore conventional to wait for six rounds of confirmations to ensure transactions are irreversible. Blockchain latencies arise as a

result of this consensus latency which is by design. This performance bottleneck may be overcome in the short term by increasing the block generation frequency for 10 minutes to a smaller time or using larger block size than 1 MB. However, performance increase will trade off against security risks and benefits are largely incremental – there will be no end to the debate on the correct block size.

- Traditional approach of consensus protocol such as PBFT is typically designed for use cases around distributed databases or filesystems at a relatively small scale of 10–20 nodes based on State Machine Replications and is unproven to work at large scale like Bitcoin. It requires the nodes to be authenticated and identified ahead of time and not designed for use cases like Bitcoin or other public blockchains where participating nodes can join or leave at will without need for any permissions. As such, it can achieve high performance and some in the order of few tens of thousands of transactions per second and limited only by network latencies. However, because all nodes must participate in the consensus, when the number of nodes is to increase, the amount of resources required for coordination and increase in message size may become a substantial impact especially when operated over the public Internet. At this point, such protocols are likely to scale only within physically near premises.

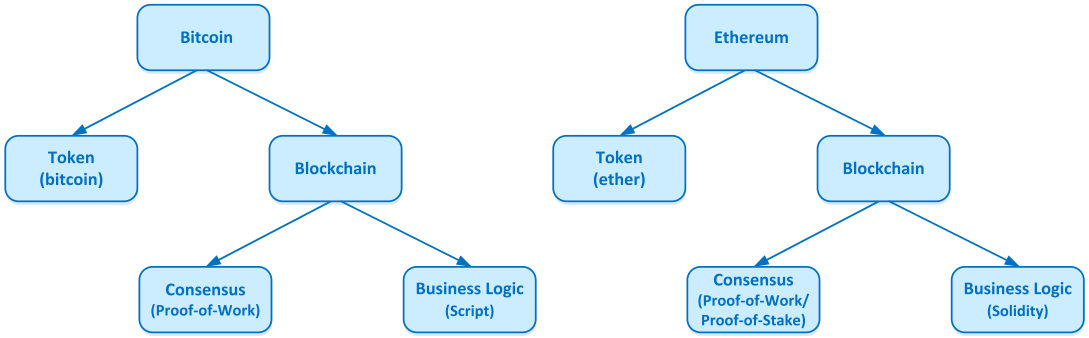
7.4.9 Turing-Complete

The Bitcoin blockchain contains a rudimentary form of programming language called Script. Script expressions use reverse Polish notation and are processed using stacks and postfix algorithm. The results arising from Script operations are only limited to Boolean output, that is, either true or false. The Script language used in Bitcoin is also known as a non-Turing Complete language. Turing Completeness is a mathematical concept and is a measure of the computability of a programming language. A non-Turing Complete language basically means that the language is designed without complex constructs such as loops and conditions which limits its ability to create general purpose programs. In Bitcoin's case, this is by design as it avoids the risks of bad programming such as infinite loop from bringing down the entire network.

7.4.10 Smart Contracts

If the Bitcoin blockchain were to be created with a Turing Complete language instead of Script, it might open up a whole world of new possibilities. This is the motivation behind the experiment called Ethereum which began as a proposition for Bitcoin 2.0. Ethereum provides developers with its own Turing Complete language called Solidity and is essentially a globally distributed computing platform. Ethereum makes it easier to implement business logics that run on the blockchain called Smart Contracts, a concept originated since 1997.

www.elsevierdirect.com



As with Blockchain terms in general, there is no standard definition of Smart Contract. Given that Ethereum is the most known Smart Contract platform in existence to date, it is fitting to use Ethereum's definition which defines it as "a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated". While Bitcoin blockchain can be used to create Smart Contract as well, it will be very difficult to use an analog to writing software applications using calculators (which was what reverse Polish notations were famously used for).

If Bitcoin can be described as a disintermediary of the central monetary system, then one way to look at Smart Contract is as a disintermediary of lawyers. However, this is not practical in business world since legal entities are governed by actual human laws and require human interpretations and enforcements. **Ricardian Contracts**, originally proposed for bond instruments to be issued as contracts that are both human and machine readable, is another trend taken up by some start-ups to create enforceable "Smart Legal Contract" in bridging the on-chain and off-chain contracts.

Smart contracts are especially necessary for private blockchain to be useful.

- This is because the need for business logic processing for enterprise usage is a lot higher than for public individuals.
- Enterprise businesses also have a heavy reliance on off-chain enterprise application such as accounting, human resource, payroll and other enterprise resource planning systems to support the operations of the business. On top of that, most business enterprises may also have in-house developed proprietary applications used within their business processes.
- Therefore, there is little utility value for the use of blockchain unless business processes can operate across on-chain and off-chain logic. This is where private block chain starts

to behave a lot more like a middleware than database for enterprise applications integration.

- This, however, is not a straightforward affair because to maintain a consistent state of the blockchain, the smart contract logic must be deterministic and all nodes must converge at the same result from execution using the same input parameters. This is the reason why individual nodes cannot pull data directly from external sources. If the external source happens to be nondeterministic, for example a service that returns random number after each call, then every node will receive a different result even though they make the same call with the same input at the same time.

7.4.11 Smart Contract Oracle

Hence the need for an **Oracle** as a gateway to provide a single view. In the case of public blockchain like Ethereum, ecosystems can be created around Oracles such as Oraclize. However, doing so creates a trust dependency on the Oracle on a public blockchain which potentially goes contrary to the original zero trust intent. For a private blockchain, the security aspect is more manageable because the Oracle is authenticated and permissioned. Microsoft's implementation of private blockchain called Bletchley (at this point) makes use of off-chain code components called "Cryptlets" that run in a secure container and data is accessed by smart contracts via event hooks.

7.5 Types of Blockchains

This section explores the different other forms of Blockchains that utilize distributed consensus protocols besides Proof-of-Work by classifying them as either token-based or token-less. This section does not aim to be exhaustive as the evolution of consensus technology is advancing at an incredible pace. It is designed to be illustrative for the purpose of exploring the differences between the various consensus protocols, both old and new, so as to identify the characteristics and conditions where one may work better than the other.

7.5.1 Token-Based Consensus Protocol Blockchains (With Mining)

Proof-of-Work (PoW) enlists the help of friendly nodes to secure it through mining while making it extremely costly for malicious nodes to launch an attack. This creates an incentive model that makes token-based consensus protocols suitable for application in the public blockchain space. However, not all token-based consensus protocols use tokens for incentive purpose; some protocols, such as Ripple, use tokens for servicing of transaction fees

www.elsevierdirect.com

whereas Ethereum's purpose for Ether is to provide the gas necessary for operating smart contracts.

7.5.1.1 Ethereum

- Ethereum is a global decentralized application platform used for the development and operation of smart contracts. It was launched to much fanfare in July 2014 supported through initial coin sale of 60 million Ether (Ethereum's token) valued at around $18 million. A complete discussion on Ethereum is out of scope for this issue and readers are encouraged to refer to the reference for more details. The following illustrates some of the core concepts used in various versions.
  - **Frontier** is the first major release and beta release of Ethereum launched on the 30th July 2015 which is a bare-bone implementation with the primary focus on supporting the mining of Ether. Ethereum uses Proof-of-Work, but unlike Bitcoins, it is a variant designed to be more memory-intensive than processor-intensive which renders most ASIC mining rig unsupportable for Ethereuo prevent network centralization and remove unfair advantage from mining pools with specialized hardware.
  - **Homestead** is the second major and officially stable release of Ethereum launched on the 14th March 2016 (Pi Day) and the focus is on providing essential support for smart contract development as well as support for future compatibility of code upgrades without requiring hard forks. Major part of Homestead is centered around the Ethereum client development. To ensure client diversity, there were at least eight different clients developed to support Homestead implemented using different programming languages on different platforms.
  - **Metropolis** (not released yet) can be described as a release to make Ethereum more user-friendly to layman rather than developer-centric to encourage mainstream adoption.
  - **Serenity** (not released yet) planned to replace existing Ethereum Proof-of-Work with Proof-of-Stake consensus protocol called Casper (Zamfir, 2015), like Tendermint that requires miners to put up a bond to participate in consensus which is essentially a bet on the block that will be included next. The incentive is such that it encourages the miner to drive towards convergence of consensus rather than betting against it and losing the deposit.

7.5.1.2 Proof-of-Stake

Proof-of-Stake (**PoS**) consensus protocol, first implemented by Peercoin, depends on market forces instead of sheer processing power to secure the network. The concept gener-

ally involves increasing the chance of a node's success in minting new digital tokens in proportion with the number of digital tokens already owned by the node. The rationale is that the more digital tokens a node owns, the more vested interest the node will have in securing the network. To launch an attack, the attacker will need to acquire enough digital tokens to succeed. This results in price hike for the token, making the attack economically unsustainable. Even if the attack were to succeed, the damage from the attack will create a devaluation of the tokens resulting in substantial economic loss to the attacker.

Comparing with Proof-of-Work, Proof-of-Stake has the advantage of securing the network without using processing power as a deterrent of attack, and lowers the barrier of entry by removing advantages associated with using specialized hardware.[3] On the flip-side, there is no penalty to miners for voting on all the chains when a fork arises which can result in the network not able to reach consensus (**Nothing at Stake**). Proof-of-Stake are also exposed to the kind of attacks impossible on Proof-of-Work designs. For instance, for Proof-of-Stake design, it is a possible to perform **a long-range attack** in which the longest fork can be replaced by a chain reconstructed from the genesis block. This cannot happen in Proof-of-Work as attacker can only rely on sheer use of energy in order to subvert the longest fork. Proof-of-Stake is also rarely implemented on its own as this will result in a permanent advantage to the richest stakeholder.

Because of these reasons, several variants of Proof-of-Stake design are in existence or in development stage today and it is difficult to validate their theoretical pros and cons at this moment:

- Peercoin (King and Nadal, 2012) uses Proof-of-Work for bootstrapping in its initial design called "ppcoin" and Proof-of-Stake which combines the number of unspent digital tokens with the number of days it is held by the node called the "*Coin Age*". The probability of successfully mining a digital token is based on the Coin Age.
- Bitsharesnt of Proof-of-Stake called the *Delegated Proof-of-Stake* (*DPoS*) that relies on the concept of "witnesses" that is voted in by stakeholders on regular intervals to prevent network centralization.

7.5.2 Token-Based Consensus Protocol Blockchains (Without Mining)

7.5.2.1 Tendermint

Tendermint (Kwon, 2014) forms a class of its own by blending traditional State Machine Replication algorithm (DLS algorithm) (Dwork et al., 1988) that assumes partial synchronicity of the network with a *deposit-based Proof-of-Stake* incentive model.

www.elsevierdirect.com

As a result of this combination, a token-based consensus protocol is created without the need for mining. The protocol requires validators to put up a bond deposit that determines the validators' voting power in order to participate in the consensus process. Since Tendermint requires a 2/3 majority of validators' combined voting power for a block in order for it to be committed, therefore a fork can only happen when some nodes double-sign a block. Validators are deterred by having their bond deposit forfeited if they perform a double sign.

When compared against PBFT, another State Machine Replication implementation, Tendermint has slightly lower performance but better security due to the use of Round-Robin-based leader election over every round as compared to PBFT's design of Sticky-Leader approach where leader is only elected upon failure. Tendermint is designed with peer-to-peer in mind, can cater to nodes joining or leaving at will, and uses Bittorrent-based message broadcast algorithms.

7.5.2.2 Ripple Protocol Consensus Algorithm (RPCA)

The Ripple Protocol Consensus Algorithm which was developed by Ripple Lab in 2014 is another token-based consensus protocol without the use of mining. Strictly speaking, Ripple do not use blockchain for its design but is frequently considered as part of blockchain family. It uses a distributed record keeping system that only keeps track of the final ledger balance. This is unlike blockchain that tracks the entire transaction history. It adopts its native token called XRP which in this case is not meant for incentive purposes and which was originally used to facilitate transaction payment and as a bridging currency between fiat currencies in illiquid markets. RPCA has made some highly explicit design choices optimizing it for speed and real-time cross-border remittance, clearing and settlement. RPCA consensus is based on all validators proposing a set of transactions it received in its open ledger to all the validators it is connected within a 2-second window. Several rounds of voting are executed to identify transactions that show up in each validator's proposal often enough until the transaction achieves 80% of votes to be confirmed into the Validators ledger.

7.5.3 Token-Less Blockchain Technologies

Token-less consensus protocols are used mainly in private blockchains and largely make use of classical State Machine Replications traditionally used in replicated database design.

One key reason is that private blockchains are governed by business agreements established between identified parties network and do not require the use of token as a defense mechanism against Sybil attack. This is the reason why most private blockchains do not rely on mining or Proof-of-Work consensus protocols.

Distributed database designs are based on the premise that participants are authenticated and numbers are known ahead of time and cannot cater to unknown participants joining or leaving at will. This fits very well in the context of private blockchains since members must be authenticated anyway. So why not simply use distributed databases instead? That is because distributed databases are typically designed to be centrally owned or administered where blockchain provides the option for decentralized administration even though there is a centralization of membership. One important aspect of private blockchain is that the newer generations of blockchains can generally support the use of smart contracts.

7.5.3.1 Practical Byzantine Fault Tolerance (PBFT)

PBFT is a distributed consensus protocol that works by requiring all clients in the network to be authenticated and authorized to send transactions to the validators. The validators have access to a public key infrastructure that supports the identity and digital certificates management. Each validator is a replicated state machine with a leader being chosen as the primary and the rest of the replicas as backups. The clients only send transactions to the primary and only the primary can broadcast messages to the backups. The primary is replaced when it is suspected to have failed (consecutive timeout). Each backup upon processing the messages will send the result to the original client. Client confirms transaction is complete when it receives 33% of the same result from all the nodes.

7.5.3.2 Hyperledger

Linux Foundation's Hyperledger Project is a result of combining the codebase from IBM, Digital Asset Holdings, and Blockstream to create a fabric to support different implementations of distributed ledger technologies and it aims to go beyond financial use cases. Like most modern private blockchains, Hyperledger is designed with the decoupling of core blockchain features in mind and supports pluggability of different distributed consensus protocols such as PBFT. It also supports the creation of smart contracts called chaincode written in Golang with support for other languages like Java in the pipeline. Hyperledger supports the use of Unspent Transaction Output (UTXO) approach adapted from Bitcoin where balance is derived from past transaction records. The other approach is to use the account model which keeps track of the account balance directly. One key aspect central to Hyperledger

www.elsevierdirect.com

design is the support for complex identity management with built-in certificate authority systems.

7.5.3.3 R3 Corda

Corda is a distributed ledger platform for recording and processing financial agreements developed by R3 (Brown, 2016); it has a design geared towards enforceability by human laws where "distributed ledgers are those reliant on legal institutions" (Swanson, 2015a). Unlike Hyperledger but similar to Ripple, Corda is specialized for use cases applicable to the financial sector only. Here are some high-level notable features of Corda. Unlike most smart contracts, Corda is designed to be both executable by programming logic and enforceable by human law inspired by Ricardian Contract (Clack et al., 2016). Traditionally consensus protocol involves validation of at ledger level whereas Corda maintains transaction privacy whereby validation is only performed by parties involved in the same transaction. Supervisory observer nodes such as financial authority participation can be included for carrying our audit activities. To work in a bank setting, Corda is designed to work with universal financial messaging standards such as ISO20022. For more details, readers are encouraged to read the Non-Technical White Paper called "Corda: An Introduction".

In Appendix 2, we have given more technical details for notable blockchains and DLSs for those readers who wish to have an overview.

7.6 Conclusion

In conclusion, Bitcoin and blockchain technologies are not general-purpose problem solving tools and are unlikely to be applicable to solving most problems most of the time. However, in problems that blockchain can be used to solve, it solves exceedingly better than any known approach – Bitcoin is by far the best use case of blockchain. Finally, by pulling together the characteristics, caveats, and properties, this section describes an approach that business can use for analyzing blockchain for a commercial use.

7.6.1 Step 1: Decide if Blockchain is the Right Solution for the Problem

Since there are much hypes around blockchain, it is necessary to have an objective view on understanding if blockchain is the right tool for the problem on hand. Most approaches today

start by asking what kind of problems that blockchain can solve and try to identify the cases used for. The more effective approach should be based on understanding the unique properties of blockchain, followed by an understanding of the problem domain. Finally, conclude if the problem domain can be solved only based on the properties of blockchain.

Properties	Types of Requirements	Benefits
Immutability of Record	• When content can be verified at the source by some form of authorities before permanently etched onto blockchain. • When large number of different stakeholder types are involved.	• Provenance Tracking: Since it is immutable, the authenticity of the content is preserved and can be used to track assets. • Reconciliation: Speed-up reconciliation processes between multiple participants because everyone is using the same ledger and reducing duplication and inconsistencies. The caveat is that confidentiality and privacy should be preserved and only shared with relevant transacting parties. • Auditability: Being the single version of truth also implies that records are trusted source for audit purpose. • Do not require centralized party: Suitable for situation where centralized party may not be possible due to special circumstances such as cross-border payments, sovereign ownerships, etc. • Centralized method not effective or too expensive. The caveat is that this is relative to the cost and risk of change from centralized to decentralized approach.
Single Version of Truth	• When excessively complicated reconciliations are involved. • When high deficit of trust with centralized systems exists. • When centralized party involvement is not feasible. • When data is allowed to be resided outside the country.	
Dis-intermediation of trust	• When the loss of service can result in high impact systemic failure. • When cost of end of fully redundant network incurs prohibitive cost. • When cloud infrastructure is acceptable and allowed by regulatory policies.	

7.6.2 Step 2: Assess the Benefits and Caveats

After ascertaining that blockchain is a possible solution for the problem on hand, the next step is to determine whether the technology is worth adopting and understanding the caveats that come with it.

www.elsevierdirect.com

Benefits	Caveats
Provenance Tracking	• For physical assets, this assumes that the identity of the assets is physically immutable as well. • The proof of ownership for off-chain asset may require legal legitimacy in the court of law. • Blockchain is not a file system and needs to be supplemented by off-chain storage. • The immutability property holds true only when risk of collusion is low.
Reconciliation	• Confidentiality and privacy have to be preserved and accessible only by relevant transacting parties. • Blockchain is not consistent and finality may be a concern when low latency transactions are involved, especially when combined with straight-through processing. This is especially important when nodes are spread globally and connected asynchronously.
Auditability	• Trustable source for audit depends on proving that the consensus process itself involved is tamper-proof.
Lack of trusted third party	• Will be less of a technical issue but more of how legal and contractual obligations are structured between counterparties with the lack of third party.
Cost of centralized systems	• The benefit to change must outweigh the cost and risk of change. There may be too much legacy and baggage to change a centralized system introducing new operational risks whereas an underperforming centralized system with a lack of strong centralized support capabilities may be more effectively replaced by DLT.

7.6.3 Step 3: Assess the Technical Design Considerations

Once the assumptions are defined and acceptable, the technical design considerations involving what features to choose for DLT will become a major part of most consultancy work as illustrated in Section 7.4.

7.6.4 Step 4: Assess the Functional Design Considerations

Business logic involved in the development of blockchain can reside on-ledger (e.g. smart contracts) but usually a large part of it may reside off-ledger (e.g. application and front-end layer) since integration with existing enterprise subsystems can be required (1-way events out of the blockchain, or 2-way events in and out of the blockchain involving oracle). The design of on-ledger and off-ledger business logic cannot be taken in isolation without overall assessment of the business process flow.

www.elsevierdirect.com

7.6.5 Step 5: Assess the Non-functional and Operational Considerations

Challenges and roadblocks to blockchain implementations are largely not technical in nature (for instance legal, business processes, corporate policies, etc.) and present an area that is highly underexplored in most blockchain discussions. Non-technical challenges should be identified and countermeasures identified before implementation, less creating a solution that cannot be practically supported.

7.6.5.1 Identity and Key Management

- Key Management is an important aspect of blockchain operations. Considerations should include the management of private keys involved in the operation such as the use of an HSM or hardware key and the solution in the event of loss of keys, process involved in applying for new keys, and how public key is made aware of the network.
- There must be a mechanism to facilitate the association between the key and user identity. User identity certification process must be established such as through the use of Certificate Authorities.

7.6.5.2 Privacy and Confidentiality

- Maintaining anonymity of transaction counterparties on the network is an important aspect for business operations.
- Details of a transaction such as volume and size of transactions cannot be revealed to any other participants on the network apart from the transaction counterparties.
- Failure to do so can result in legal liabilities or competitions gaining access to business intelligence relating to your business performance.

7.6.5.3 Existing Systems Integration and Interoperability

- Implementing a blockchain for an organization must involve a way that facilitates integration with supporting infrastructures and their existing legacy systems. For instance, a software adaptor integrating the blockchain to the enterprise messaging infrastructure.
- The placement and development of oracle to provide access for instance to reference data used in the business logic processing will be an important integration consideration as it can pose a single point of failure even though the blockchain has mitigated this risk.
- Existing systems may be following a messaging standard such as ISO20022 for new financial messaging standard or ISO8583 for legacy and card-based messaging standard. DLT will need catering for these standard formats to ease integration and adoption.

www.elsevierdirect.com

7.6.5.4 Regulations

- Certain regulations may not allow banking data to be stored outside the regulated regions.
- In a centralized system, the centralized operator and technology providers can be held liable for systems failure and liquidated damages. In a decentralized system, the liability ownership has to be established clearly as roles and responsibilities of an ecosystem may be shared.
- Governance. A centralized system has clearly defined governance frameworks; however, for a decentralized system, the governance framework, policies, and regulations may not have an existing precedence to follow and may require a redesign.
- There may be some form of federated decision body making up the validator nodes and a form of policies should be drafted to determine the level of rights and access for members participations.

7.6.5.5 Production Rollout and Testing

- Testing will be an extremely important element of operation support that needs to take into consideration the integration aspect of on-chain and off-chain logic.
- Non-functional testing involving various node failure exception scenarios should be performed. Proof of consistency and finality should also be tested under heavy load in order to be certain that critical transactions will not be rolled back under the assumed conditions.

7.6.5.6 Operational Readiness

- Change Management and Version Control. It may be necessary to establish guidelines on controlling blockchain software upgrades as well as impact to the off-chain logic.
- Monitoring and Alerts. It will be challenging to ensure the process to maintain the consistency of the blockchain systems' performance and functionality across all locations. Blockchain Infrastructure Monitoring and Alerting is required to ensure that the system is working optimally.
- Batch Jobs and Processes. As blockchain data storage is not suited for analytics and reporting purposes, there is a need to schedule batch jobs and processing to extract data and load data into analytical databases.
- Workflow. As blockchain is new and multiple participants are involved in the operations of the entire system, there is a need to establish best practices and optimal work flow processes.
- Minimum System Requirements. As the blockchain sits on top of a heterogeneous operating environment, there is a need to establish minimum server specifications in order to ensure that smart contract processing is not impacted by one or more participants running underpowered servers or implications from poor network connectivities.

www.elsevierdirect.com

- Rules and By-laws. If an entire industry is concerned, there should be some form of by-law and legally enforceable guidelines prescribing the requirements for membership, level of access, or support obligations.

Appendix 1: The Six Layers of Blockchain

There is another way to understand blockchain by decomposing into six layers. Given the complexity, there are many interpretations of these layers. These layers are not necessarily mutually exclusive. In this Appendix, we look at one of the **classifications of six layers** in accordance to Wan Xiang Blockchain Lab (WanXiang, 2016). The **first three layers are essential** for a blockchain and have implications for cost savings for many institutions in streamlining their process and operations. The **last three layers are not necessary** for a private chain but they enable a lot of new revenue generating ideas. The discussion here is meant to be introductory and not exhaustive. The choice of one layer may necessitate the inclusion of another or it may not because the layers are not mutually exclusive:

1. Data
   - This layer is the underlying data structure and usually is arranged in chain of blocks. The underlying data technology will include **how and when** data are being stored, such as the use of asymmetric public and private keys encryption and time stamping. **Asymmetric cryptography**, also known as **public key cryptography**, uses **public and private keys** to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (i.e., asymmetric). One key in the pair (the group, when more than two) can be shared with everyone and that particular key is called the public key.
   - There are many asymmetric cryptography protocols such as SSH, OpenPGP (including GNU Privacy Guard (GPG)), Secure/Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL)/Transport Layer Security (TLS), and other less favored (not secure) such as RSA that was first used in Lotus Notes 1.0 in 1989. All of them rely on asymmetric cryptography for **encryption and digital signature** functions. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (**authentication**), that the sender cannot deny having sent the message (**non-repudiation**), and that the message was not altered in transit (**integrity**).
   - Asymmetric encryption will deliver confidentiality, integrity, authenticity, and non-repudiability, provided users and systems are certain that a public key is authentic, that it belongs to the person or entity claimed without any tempering or malicious replaced by a third party. Trusted certificate authorities that certify ownership of key

www.elsevierdirect.com

pairs and certificates is the most common approach in a public key infrastructure (PKI). But encryption products, based on the **Pretty Good Privacy** (PGP) model, rely on a decentralized authentication model called a web of trust (Cumulative Trust) that trusts keys that others have signed. PGP relies on individual endorsements of the link between user and public key rather than certificate authorities. PGP is created by Philip Zimmermann (1991) and provides a confidential and authentication service that can be used for electronic mail and file storage application. Basically, the date is encrypted and sent to a known recipient with a digital signature so that the recipient(s) can be sure from whom it is. **OpenPGP**, developed based on PGP in 1998, is more flexible and can use any trust models but **Cumulative Trust** is a more secure and preferred choice.

- A **timestamp** is a sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second. Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. That means that no one – not even the owner of the document – should be able to change it once it has been recorded. It is important that the timestamper's integrity is never compromised. There are a few **time stamping schemes** that are of interest but only two are presented here:
  a. **PKI-based** means that the timestamping token is protected using PKI digital signatures;
  b. **Distributed schemes** require the cooperation of multiple parties to ensure the timestamp is generated.

The PKI scheme conforms to the Internet and International standards RFC3161, ANSI ASC X9.95 and ISO/IEC 18014, while the database system conforms to the ISO/IEC 18014. There are other schemes such as Linked, MAC, Transient Key, Hybrid Linked, and Signed. Most of them conform to the newer X9.95 except for Linked that conforms to both X9.95 and the older ISO/IEC 18014 (Une, 2001). X9.95 has been applied to authenticating digitally signed data for regulatory compliance, financial transactions, and legal evidence. The distributed scheme is not X9.95 compliant. Data-level security requirements are to ensure data integrity against a reliable time source that is provable to any third party.

Blockchain has changed it all in that it enables securely timestamp information in a decentralized and tamper-proof manner with the use of digital signature and hash. Once the digital data is hashed and the resulting hash is incorporated into a blockchain, it serves as **a secure proof of the exact time at which the data existed**. In the case of decentralized ledger and whether the database is editable by some parties, it may amount to tampering with the timestamp that leads to doubts about the integrity of the entire digital database.

www.elsevierdirect.com

2. Network
   - This layer concerns the **P2P networking, data transmission, and verification of data**. Blockchain technology is a self-organized network with peer-to-peer networks communicating with each other. In its simplest form, **P2P network** is created when two or more computers are connected and share resources without going through a centralized server. In a P2P environment, access rights are governed by setting sharing permissions on individual machines and designed around the notion of equal **peer nodes simultaneously functioning as both "clients" and "servers"** to the other nodes on the network.
   - The P2P architecture was popularized by the file sharing system Napster released in 1999. Other P2P file sharing examples are Gnutella, Freenet, Kazaa, Bearshare, Limewire, Scour, Grokster, Madster and eDonkey2000, and many others were brought down, changed, or acquired due to copyright issues. **Unstructured P2P networks** do not impose a particular structure on how nodes are connected to each other but simply connected randomly. It is robust because there is no particular overlay network by design, especially when large numbers of peers are frequently joining and leaving the network. However, its disadvantage is that each search query of a desired piece of data in the network will create high amount of traffic and use more CPU/memory causing flooding. In contrast, in a **structured P2P network**, the overlay is organized into a specific topology, and the protocol ensures that even if the desired piece of data is rare, it can be efficiently located. A **distributed hash table** (DHT) will enable any participating node to efficiently retrieve the information since the hashed information is assigned to a peer and it is known. It is a class of a decentralized distributed system that provides a lookup service similar to a hash table: (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. CAN, Chord, Pastry, IRIS, and Tapestry are protocols and algorithms for P2P DHT. Well-known distributed networks outside the academic that use DHTs include BitTorrent's distributed tracker, GNUnet, Gnutella, G2, eDonkey, Zeronet, the Kad network, the storm botnet, YaCy, and the Coral Content Distribution Network. Other structured P2P protocols are Chord project, Kademlia, PAST storage utility, P-Grid, a self-organized and emerging overlay network, and CoopNet content distribution system. While there are many file sharing protocols, **BitTorrent** (BT) is one of the most common protocols for transferring large files. Using a BT Client on an Internet-connected computer, data files can be sent and received. The program was designed by Bram Cohen in April 2001. Outlined in Leverington (2014), RLPx is a cryptographic peer-to-peer network and protocol suite which provides a general-purpose transport and interface for applications to communicate via a P2P network. RLPx is designed to meet the requirements of decentralized applications and is used by Ethereum.

www.elsevierdirect.com

- Four important issues are self-organizing, cooperation, data availability, and reliability, as mentioned in Oualha et al. (2010). "The main goal of a P2P storage system is of course to guarantee the potential retrieval of data. Since data are not stored in a centralized server and since P2P networks are assumed to be very dynamic, the **stored data should be available even if peers may leave the network**. Data availability can be increased with data redundancy techniques. Data should not only be available at any time but also **preserved in the long term**. Data integrity thus has to be ensured and, in case of errors, a peer should be **able to detect the compromised data**."

3. Consensus
   - This layer concerns the processes of P2P network on agreeing on a single data value. There are a few consensus algorithms for nodes on the network. It determines how the records are chosen, how the records are kept, who keeps the records, how data are propagated and how all these will influence the security and reliability for the whole system. These issues have been discussed in the Chapter and we shall not elaborate any further here. In essence, the fundamental problem of consensus network is to achieve overall system reliability in the presence of several faulty processes and to ensure a certain degree of fault tolerance or resilience. One example of Byzantine Fault Tolerance described in detail in the chapter is Bitcoin. **The Proof of Work** (POW) of Bitcoin is a computationally expensive effort to perform in order that the resulting hash be submitted to the blockchain. The PoW chain is key to overcome Byzantine failures and to reach a coherent global view of the system state. Besides PoW, there are other consensus systems for blockchain, such as Proof of Stake and Delegated Proof of Stake.
   - **(1) To (3) there are essential components of a blockchain that will determine how the entire network functions.** One narrow definition of distributed ledger system is "a network that utilizes cryptocurrency-inspired technology and perhaps even part of the Bitcoin or Ethereum network itself, to verify or store votes (e.g. hashes)". Distributed ledgers system (DLS) in the narrow sense (Swanson, 2015b) are those reliant on legal institutions and as such, a final commonality is the permissioned identity system. However, distributed ledger system can have a much wider interpretation.
4. Incentive
   - This layer concerns the **economic incentives for the agent to act** in their self-interest for building the network. It usually involves issues of how different agents or participants are rewarded and punished. The layer involves the issuance of economic incentives, allocation of reward mechanism, and the governance structure. For the network to function in accordance to the rules and regulation, incentives must be provided for the participating nodes that contribute to its continuity and to punish those

that violate the regulation. Private network may not need this layer given that there are higher authority or off-chain incentives that enable consensus.

5. Contract
   - This layer concerns the different types of scripts, algorithms and smart contracts that are forming the basic blockchain programmable feature. **Smart contracts** are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary (Szabo, 1994). While Bitcoin blockchain has the function to write simple scripts, the Ethereum significantly improved this programming language protocol, with which theoretically one can write and implement applications with any function. If we refer to bitcoin as a global ledger, the Ethereum is then a global computer, with which anyone can upload and execute any kind of applications, and ensure the efficiency at the same time (WanXiang, 2016).
6. Application
   - This layer concerns the **application scenarios and use cases**. It usually involves the blockchain applications built on the first three layers that give potential rise to new business models that generate revenue.

Appendix 2: Notable Blockchain and Distributed Ledger Technologies

Given the discussion above, we shall outline a few prominent blockchains and decentralized ledgers (New Blockchain Finance, 2016; Gao, 2016):

1. **Bitcoin:** https://github.com/bitcoin/bitcoin
   - Bitcoin, created by Satoshi Nakamoto (2008) is the "original" blockchain and the most widely used case of open and permissionless public blockchain. This has been discussed elsewhere (Lee, 2015) in much greater detail and we will not elaborate here. Bitcoin Core is released under the terms of the **MIT license**.
2. **Chain:** https://github.com/chain/chain
   - Chain is a name of the blockchain by the company of the same name. It is designed for industry and finance. The design is for supply chain financing products but allows for digital assets. Its features are a 1-second consensus algorithm, allow for third party to read encrypted information on a need to basis, smart contracts are stored in a readable complete form, flexible data structure for cost savings, allows for easy implementation of KYC and AML. Programming language is GO with Byzantine consensus algorithm, and supports various digital assets. Chain Core Developer Edition is licensed under the terms of the **GNU Affero General Public License Version 3 (AGPL).** The Chain Java

www.elsevierdirect.com

Software Development Kit SDK (/sdk/java) is licensed under the terms of the **Apache License Version 2.0**.

3. **Corda:** Codes to be released
   - Corda is developed by R3 using a DLS originally intended to solve financial sector issues. There are currently over 70 members and there are signs that they may be moving outside the financial sectors towards IoTs. The codes for R3 consortium's Corda blockchain platform will be handed over to the Hyperledger project. The main features for Corda are known to be database sharing on a need to a known basis, decentralized coding and allocation, consensus on trades rather than at the system level, designed to accommodate compliance as a node, trades are agreed bilaterally rather than by consensus from unrelated mass, support different consensus protocols, programmer and legal friendly smart legal contracts (based on Ricardian Contracts) running on Java Virtual Machines, conformance to industry standards, and there are no tokens.
4. **Dragonchain:** https://github.com/dragonchain/dragonchain
   - Dragonchain is a mixture of open and closed blockchain developed by Disneyland for record keeping and trades. Unlike Bitcoins, it has many tokens and allows for many consensus algorithms. The features are easy integration with existing blockchains, designed for developers who are not necessary familiar with cryptography, DLS or blockchains. C/S client servicing and RESTful are integrated, flexible, allow for centralized control, fixed timestamp period with short and high speed blockchain, support different tokens, no basic tokens, easy linkages with other blockchains. Written in Python and support smart contract, it is licensed under the **Apache License, Version 2.0**.
5. **Ethereum:** https://www.ethereum.org/
   - Ethereum is the second most used public blockchain that has an ideal programming environment for smart contracts. Good references are Buterin (2013a, 2013b) and Gavin (2014). While smart contracts can be executed on the Bitcoin protocol, it is cumbersome compared to Ethereum that allows for multiple programming language in the execution of smart contracts. Every contract will have an Ether address and when a transaction is activated with a payment called gas, the contract will be executed, drawn on external information if needed, and return an outcome. Given that the execution has no central authority, the contract is also known as decentralized App.
   - The smart contracts can be written in Solidity, Python, LLL and many other languages. Solidity is an object-oriented language designed for writing contracts in Ethereum and perhaps the first experimental contract-oriented programming language. With Solidity and through the client Mist, contracts are tested and executed.

Given the popularity of Dapps, there are now many Dapps developers such as Truffle, Embark, Meteor, and BlockApps. Blockapps, Net and Embark are now part of the Azure BAAS. Most users will first install the Ethereum Wallet and first get used to the wallet and the smart contract execution. The test net can be used since it does not require to burn your gas or Ether while learning. Once there is familiarity, most will go to the Geth and Node environment, install the Mist client (for testing and smart contract), and activate Geth. After familiarizing with Geth and Solidity compiler, one can test run the Dapps. Web3.js is then used to edit or some will prefer to use Truffle and Embark to develop the app for specific purposes. Those interested in Ethereum Browser Parity and Ethereum Classic, can visit web pages https://ethcore.io/parity.html and https://ethereumclassic.github.io/. Ethereum Classic is a continuation of the original Ethereum blockchain – the classic 'unforked' version that abides by "Code is Law"; free from external interference and subjective tampering of transactions.

- The Core of Ethereum includes the consensus engine, the networking code and any supporting libraries. While committed to be open source, it is unclear what the final open source license will be for the C++ and Go Core even though MIT, MPL and LGPL have been mentioned. For the applications of Ethereum including the Solidity complier, AlethZero and Mix, they will be distributed under the **GNU General Public License**. The middleware of Ethereum, including the JavaScript-based web3.js, the web3 libraries and eth (the command line client) will be distributed under an **Affero license**, likely the LGPL variant of it (https://github.com/ethereum/wiki/wiki/Licensing).

6. **Hyperledger** (http://hyperledger-fabric.readthedocs.io/en/latest/)
   - Linux Foundation's Hyperledger Project is a result of combining the codebase from IBM, Digital Asset Holdings, and Blockstream to create a modular design capable of supporting different implementations of distributed ledger-based solutions for enterprise use. The core of Hyperledger is its application fabric which is its cloud-based middleware for hosting pluggable distributed ledger components such as consensus protocols and smart contracts. Smart contracts in Hyperledger known as chaincode provides language support for Golang and Java. It makes use of Unspent Transaction Output (UTXO) approach adapted from Bitcoin for storage of gross transactions but also provides the use of account model which keeps track of net digital asset balances. One key aspect central to Hyperledger design is its strong support for complex identity management with built-in certificate authority systems. The Hyperledger Project uses the **Apache License Version 2.0** software license.

www.elsevierdirect.com

7. **Microsoft Azure**
   - Microsoft is the first global IT company that adopted blockchain in 2014 through Bitcoin. Microsoft Azure (Microsoft, 2016) was first introduced in November 2015, initially working with Ethereum and then extended to having other partners including ConsenSys, Ripple, Eris Industries, CoinPrism, Factom, BitPay, Manifold Technology, LibraTax, Netki, Emercoin, Multichain and others. Blockchain as a Service (BaaS), through the Azure Cloud Platform, is a sandbox for new technology and services by allowing different partners to experiment. Microsoft has rolled out their own distributed ledger framework called Bletchley. The heart of it is a cloud-based middleware tier that supports the use of "Cryptlets" which is Microsoft's term for the smart contract building blocks. The key advantage that cryptlet brings is its ability to support a built-in for "Oracle" – enabling trusted external request to off-chain services.
8. **Multichain:** Open Source Code to be released
   - Multichain is a blockchain for software for building and developing permissioned chain. It takes two steps to set up and blockchain and another step to link to other blockchains. It uses Proof-of-Work but the multiple mining solves the issue of any miner dominating the activities. It supports Windows, Linus, and Mac Servers and provides a simple API and command-line interface. MultiChain is a fork of Bitcoin Core and will be open source under the **GPLv3 license**.
9. **Openchain:** https://github.com/openchain/
   - Openchain is an open source distributed ledger system developed by Coinprism for large and financial institutions. It is designed for higher Transaction per second (tps), with lower cost and better security with DLS. It is designed for trading and requires signature to ensure trades are legitimate. It can be linked to Bitcoin Blockchain. Written in C# with DNX application, it can support trading across platforms, support smart contracts and suitable for consortium chain. It is licensed under the **Apache License, Version 2.0**.
10. **Qtum:** Codes are not available yet
    - Qtum is designed by the team in China with Value Transfer Protocol that services finance, IoT, Supply chain and social games using DAPP platform. The positioning of Qtum is to allow for compliance monitoring with possibility of third party verification. It introduces the concept of control contract that allows for external data and language verification. Incentive proof of Stake is used as the consensus system. However, in consortium chain, Proof-of-Time integrated with Raft is being used in the consensus system in order to achieve higher speed. It supports EVM/EVM2.0 and smart contract. Ripple: https://github.com/ripple/rippled.

- This is a consensus ledger deigned for financial institutions and XRP is the native token. This is a shared global ledger that is transparent to all. Transactions are cryptographically signed with using ECDSA and Ed25519. Candidate transaction goes through consensus and validation process until the nodes reach a supermajority of a defined percentage, the network will recognize the validated transactions with a new validated ledger. Any rejected transaction will remain a candidate until it is included in a validated ledger. It has been used mainly for cross-currency settlement, FX market making and other institution use cases with enterprise software. Rippled is the reference server implementation of the Ripple protocol and the open source permissively licensed under the **ICS license**.

11. **Sawtooth Lake:** https://github.com/hyperledger/sawtooth-core
    - Sawtooth Lake is a distributed ledger designed for IoT and Financials with versatility and scalability. Sawtooth Lake is Intel's modular blockchain suite and supports both permissioned and permissionless deployments. It includes a novel consensus algorithm, Proof of Elapsed Time (PoET). PoET targets large distributed validator populations with minimal resource consumption. It is a lottery or competition protocol. The second consensus protocol that it uses is Quorum voting, an adaption of the Ripple and Stellar consensus protocols. It is more appropriate for the needs of applications that require immediate transaction finality. Sawtooth Lake has a data model that captures the current state of the ledger, a language of transactions that change the ledger state, and a protocol used to build consensus among participants around which will be accepted by the ledger. More information is available in https://www.hyperledger.org/community/projects.
12. **Stellar:** https://github.com/stellar/stellar-core
    - Stellar was founded by Jed McCaleb, formerly with Ripple and written in C++ with SCP consensus algorithm. It supports smart contract and suitable for public and consortium chains. Unlike Ripple that uses a fixed 80% threshold, Stellar uses Stellar Consensus Protocol with a Proof of Safety. That means that it is "optimally safe" for a given configuration and failure patterns. It allows for flexibility in terms of how nodes configure their quorums. It is explicitly designed to accommodate Byzantine failures and different nodes trusting different subsets of the system (https://www.quora.com/How-do-Ripple-and-Stellar-perform-consensus).
13. **Tendermint:** https://github.com/tendermint/tendermint
    - Tendermint is a consensus protocol engine that is adapted from on a type of Byzantine Fault Tolerance algorithm called DLS (named after its inventors) which assumes partial synchronous communications between nodes. It can support other blockchains and smart contracts (written in different languages) as it is standalone and decoupled; integration with Tendermint is facilitated through its protocol called

www.elsevierdirect.com

the TMSP (Tendermint Socket Protocol). Most popular use of Tendermint is in providing the consensus component to Eris:DB (By Eris Industries). Another up and coming use case of Tendermint is in the implementation of Cosmos (known by its inventor as the Internet of blockchains).

14. **InterPlanetary File System (IPFS)** https://github.com/ipfs/ipfs
    - IPFS combines a distributed hash table based on Kademlia, peer-to-peer file sharing technologies based on bittorent and version control capabilities based on git to create a distributed file system that seeks to connect all computing devices with the same system of files (essentially becoming the Internet file system). Distributed ledger technologies do not support file storages and generally only store the hash of a file that is stored offchain. As such, technologies such as IPFS can provide distributed file storage capabilities that complement the use of distributed ledgers.

This list is not exhaustive and was included as a complete list of notable blockchains and DLSs.

References

Brown, R.G., 2016. The corda non-technical whitepaper [online]. Available at: https://r3cev.com/blog/2016/8/24/the-corda-non-technical-whitepaper.

Burrows, M., 2006. The Chubby lock service for loosely-coupled distributed systems. s.l.: Google Inc.

Buterin, Vitalik, 2013a. Ethereum: a next-generation smart contract and decentralized application platform. http://ethereum.org/ethereum.html.

Buterin, Vitalik, 2013b. Dagger: a memory-hard to compute, memory-easy to verify scrypt alternative. http://vitalik.ca/ethereum/dagger.html.

Castro, M., Liskov, B., 1999. Practical byzantine fault tolerance. In: The Proceedings of the Third Symposium on Operating Systems Design and Implementation, February.

Clack, C.D., Bakshi, V.A., Braine, L., 2016. Smart contract templates: foundations, design landscape and research directions [online]. Available at: https://arxiv.org/pdf/1608.00771.

Dwork, C., Lynch, N., Stockmeyer, L., 1988. Consensus in the presence of partial synchrony. Journal of the Association for Computing Machinery 35 (2), 288–323.

Eyal, I., Sirer, E.G., 2013. Majority is not enough: bitcoin mining is vulnerable. arXiv:1311.0243, November.

Gao, Elwin, 2016. Introduction to Blockchain. http://blog.csdn.net/elwingao/article/details/52412315.

King, S., Nadal, S., 2012. PPCoin: Peer-to-peer crypto-currency with proof-of-stake [online]. Available at: https://peercoin.net/assets/paper/peercoin-paper.pdf.

Kwon, J., 2014. Tendermint: consensus without mining [online]. Available at: http://tendermint.com/docs/tendermint.pdf.

Lamport, L., 1978. Time, clocks, and the ordering of events in a distributed system. Communications of the ACM 21 (7), 558–565.

Lamport, L., 1998. The part-time parliament. ACM Transactions on Computer Systems 16 (2), 133–169.

Lamport, L., Shostak, R., Pease, M., 1982. The byzantine generals problem. ACM Transactions on Programming Languages and Systems 4 (3), 382–401.

Lee Kuo Chuen, David, 2015. Handbook of Digital Currency. Elsevier.

Microsoft, 2016. Introducing project “Bletchley”. https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md#bletchley.

Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system [online].
New Blockchain Finance, 2016. Introduction to 8 new generation of open source blockchain technology. http://mp.weixin.qq.com/s?__biz=MzIzMjEzOTY5OA==&mid=2650415287&idx=2&sn=683ee587cf82533de55f6a293f71243a&chksm=f097fe6ac7e0777c633d6ded80018ef9d46920987f0cc80230e33c2d4f0801c219fab6a04f33&mpshare=1&scene=5&srcid=1030dLeAxOHa6mipk8P8yKS5#rd.
Oualha, Nouha, Önen, Melek, Roudier, Yves, 2010. Secure P2P data storage and maintenance. International Journal of Digital Multimedia Broadcasting, 720251. https://www.hindawi.com/journals/ijdmb/2010/720251/.
Pass, R., Seeman, L., Shelat, A., 2016. Analysis of the blockchain protocol in asynchronous networks [online]. Available at: https://eprint.iacr.org/2016/454.pdf.
Swanson, T., 2015a. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems [online]. Available at: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.
Swanson, Tim, 2015b. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.
Szabo, Nick, 1994. Smart Contract. Copyright©1994 by Nick Szabo, reproduced in http://www.virtualschool.edu/mon/Economics/SmartContracts.html.
VISA, 2015. Visa Inc. at a glance [online]. Available at: https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf.
Vukolić, M., 2015. The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: Proceedings of the IFIP WG 11.4 Workshop – iNetSec 2015, December.
WanXiang, 2016. Six layer model of blockchain. http://mp.weixin.qq.com/s?__biz=MzA3NTg1MjE0Ng==&mid=2649775177&idx=2&sn=3a9b3f04d916c88ef0fc06150fddc5c0&mpshare=1&scene=5&srcid=1031N8BxO7MkfE1q5R3b44sm#rd.
Wood, Gavin, 2014. Ethereum: A Secure Decentralised Generalised Transaction Ledger, EIP-150 Revision. http://gavwood.com/Paper.pdf.
Zamfir, V., 2015. Introducing Casper "the friendly ghost" [online]. Available at: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/.
Zimmermann, Philip, 1991. Why I wrote PGP. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

Notes

1. To be specific, this refers to a blockchain fork. Because Bitcoin and most public blockchain-related projects are open-sourced, the source code can be readily copied and used on a different track of developments which is known as creating a software fork.

2. Nodes will actually pick the most difficult chain.

3. BitFury Group (13 September 2015) "Proof of Stake versus Proof of Work".

www.elsevierdirect.com

CHAPTER 8

Blockchain 101: An Introduction to the Future

Jeff Garzik, Jacob C. Donnelly

Contents

8.1 Two Factors to Achieve Trust 180

8.2 What Problems Do Blockchains Solve? 182

8.2.1 The Perfect Storm of the Permissionless Network 183

8.3 What Problems Do Blockchains Create? 184

8.4 In Conclusion: The 9 Factors of Blockchain 185

References 186

For all its potential to revolutionize finance, healthcare, supply chain, identity, and countless industries, blockchain technology is still very new. If it were a child, it would barely be out of elementary school. Yet, since the concept of a blockchain was first introduced, the field has exploded, with companies and ideas sprouting in every direction.

With this explosion of companies and ideas, there are numerous debates about what a blockchain really is. Questions of private versus public sprout up on a regular basis, with different groups standing strong about what they believe a blockchain to truly be.

If we go back to the very beginning and ask the creator of the first true blockchain, Satoshi Nakamoto, he would say:

> *The block chain is a tree shaped structure starting with the genesis block at the root, with each block potentially having multiple candidates to be the next block.*

In layman's terms, this means that there is an originating block and then each new block builds on the last, creating a taller/longer structure. Because each entity is referred to as

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00008-5
Copyright © 2018 Elsevier Inc. All rights reserved.

a block and they are chained together in perpetuity, it has become common to call them a blockchain.

At Bloq, we view a blockchain as:

> *Distributed, immutable databases that are technological infrastructure.*

This is a key point because along the way, people will present ideas about blockchains that don't *actually* necessitate the technology. At its core, a blockchain is a database that, due to certain written-rules, cannot be changed (immutable) and, if it is deployed properly, is spread-out amongst many computers (distributed).

Ultimately, the blockchain results in every transaction being recorded indefinitely, with every future transaction being rooted to the previous one, such that each transaction can be traced back to the very beginning of the blockchain's creation. Due to this linked nature, a blockchain becomes very easy to audit.

But a chain of every transaction is only as good as the trust people have for that chain. If people believe that the transactions on that blockchain can be changed, no amount of auditing will bring back the trust.

8.1 Two Factors to Achieve Trust

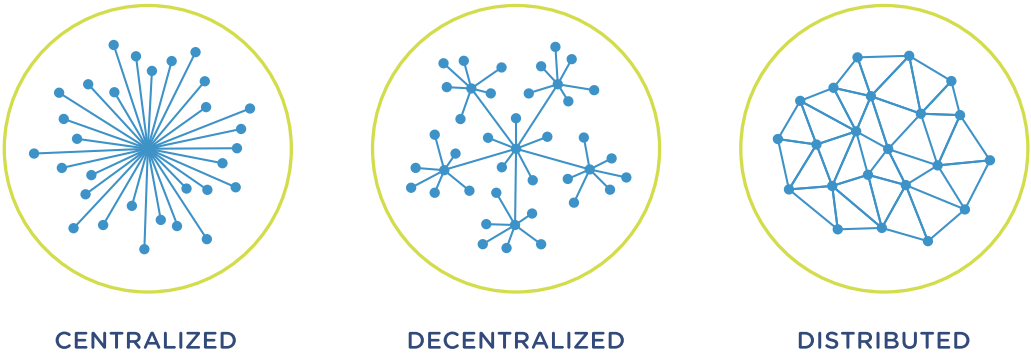
To achieve this trust, two factors are needed: cryptographic integrity and network power.

Cryptographic integrity (Wikipedia, 2016) means that you can provide a proof that you control whatever asset is stored on that specific blockchain—currency, titles, stocks, etc. So long as you have the cryptographic proof, known as a key, you have proof of ownership.

Blockchains rely on what's known as public-key cryptography (Davenport, 2015), which requires the pairing of two keys: public and private. The public key shows what you have without giving control of the assets away. The private key gives that control. Therefore, any person can audit assets on a blockchain simply by analyzing the public keys, but cannot actually act on those assets without the corresponding private key.

The other factor is network power. The more people, or nodes, that are part of the network, the more powerful the blockchain. Nodes are programs that validate transactions and blocks, and relay them throughout the network. In the world of blockchains, power is security.

www.elsevierdirect.com



This network power is providing certainty, through proof of work, to the data in the blockchain through the confirmation of transactions. When a transaction is sent, it broadcasts out to the network and nodes verify their validity. They are then put into a block and attached to the previous one (Stackexchange, 2016).

The problem arises when the network power providing this proof of work is not vast.

Although Ethereum and Bitcoin are two of the largest blockchains, there are hundreds of others that are far smaller and lack this network power. For example, Shift, the first alternative cryptocurrency built using Ethereum's code, has been at risk of a 51% attack for some time. This means that a single individual becomes powerful enough to account for 51% of Shift's total network power, thus allowing that individual to change things on a blockchain.

While we agree that a blockchain is an immutable database, it is only as immutable as it is distributed.

> *FAQ: What is a Miner?*
> *Individuals and companies who help secure a blockchain, paying for electricity and, in return, receiving bitcoin via the mining subsidy and any transaction fees*

Proof of work, ultimately, requires computational resources (electricity) from these nodes. Because electricity is not free, there needs to be some sort of an incentive for node operators. In the world of Bitcoin and Ethereum, this incentive is provided through what's called the "mining subsidy."

In Bitcoin and Ethereum, this subsidy is the release of new bitcoin or ether to the individual who seals the next block of transactions. And because of this subsidy, there is a financial benefit to participate in sealing blocks. Ultimately, this economic benefit leads to the network

power. As bitcoin and ether appreciate in value, more individuals become incentivized to help secure the blockchain, thus allowing the total network powerful to grow.

This subsidy also acts as a disincentive to those with malicious intent. If there is a strong network securing a blockchain, the resources required to alter the blockchain (which gets stronger with each sealed block) become increasingly larger. This is why some have suggested that hacking Bitcoin is worth a $10 billion bounty (Coindesk, 2015).

Ultimately, if the blockchain you're using has both strong cryptographic integrity and securing network power brought about by distribution, you can be confident that the blockchain is immutable.

8.2 What Problems Do Blockchains Solve?

A tool without a use is just a fancy object. Fortunately, blockchains do provide significant utility to many problems.

We've talked about how people have to trust that the blockchain has not been altered in any way. If, for example, someone sends a transaction, but then an individual alters that transaction, faith in the system would be lost. Therefore, its immutable nature is without question.

But what if the blockchain, itself, has not been altered, but the same asset has been sent twice? This is known as the "Double Spend" problem and has made previous versions of digital cash effectively worthless. The "Double Spend" problem is akin to sending a file to one person and then immediately sending that file to another person.

With the blockchain, this becomes impossible. When an asset is transferred, the blockchain records who it came from and who it went to. And with each sealed block, that transaction gains additional verifications, essentially re-confirming that the asset went from point A to point B. While this is absolutely necessary for the transfer of value, such as sending bitcoin to someone, there are numerous other examples of where preventing the "Double Spend" problem is so necessary.

One, in particular, is with land registry. In developed countries, we know who owns a house and it's relatively straightforward. However, in countries that are still developing, a family may have owned a piece of land for generations, but it is very easy for someone to come along and steal it, essentially saying that the family no longer has claim. And, unfortunately, who can argue against that?

Because blockchains don't allow for the chain to be altered, and since the same asset cannot be on the chain twice, the ownership of said land title is crystal clear. There are companies around the world creating robust blockchains that would create this protection for families in developing nations (Chavez-Dreyfuss, 2016).

With the advent of blockchain, the trust moves from the counterparty to the system—the network power.

Another problem that blockchains solve is the need for counterparties. In the past, civilizations have relied on trusted middlemen—banks—to ensure that a transaction is valid. Take, for example, the sale of a share of Apple or Amazon. Today, there are brokers for both the buyer and seller, market makers, and many other entities that are all acting between the buyer and seller of the said share. Each of these individuals is taking a small cut, making an exchange of assets more expensive.

With the advent of blockchains, the trust moves from the counterparty to the system—the network power. Rather than relying on brokers, market makers, etc., now the system acts as the verifier, allowing the seller to trade directly with the buyer. Ultimately, the cost of the trade becomes smaller.

8.2.1 The Perfect Storm of the Permissionless Network

If we go back to our definition of a blockchain, we say that a blockchain is a "distributed, immutable database that is a technological infrastructure." And because the trust moves from the counterparty to the system, what we wind up with is what's known as a permissionless network, a system by which anyone can participate, whether or not they have any sort of previous relationship or identity.

With Bitcoin, anyone can spin up a node and join the network. Anyone can buy a piece of mining hardware and start contributing to the security of the network, attempting to be compensated via the "mining subsidy." The strength of your vote is contingent on how much you provide to the network rather than any predetermined rules.

The Internet acts in the same egalitarian way, whereby developers can participate how they see fit. Blockchains, at least permissionless ones, allow the same outcome, where no single person dictates the outcome of the blockchain.

Because of how open everything is—while still being completely secure and cryptographically sound—options become possible.

One is a mechanism called tokenization. This is where digital currencies, such as a bitcoin, ether, or something else, can be used to represent a specific type of asset (Rosenfeld, 2012). In the future, it will be possible to take a physical piece of property and associate it to a digital token. With that token, it can be traded like a bearer share, physically transferring the ownership of this digital asset. These are sometimes referred to as colored coins, which are simply fragments of a bitcoin (or some other coin) that act as a token of the asset.

www.elsevierdirect.com

This ultimately leads to programmable contracts, otherwise known as smart contracts. These are programs built on these tokens that execute based on a specific set of rules coded into the actual contract (Szabo, 1997). They're identical to a contract one might get drawn up from a lawyer, except they don't depend on a middleman to execute; instead, it can verify that the conditions of the contract have been met and then distribute whatever assets are associated with it (Stark, 2016).

For example, imagine an individual looks to lease a car, which has been tokenized. Both the car lessor and the lessee sign the smart contract with the stipulation that the token will be in the lessee's name under a series of rules. Each time the lessee makes a payment, the smart contract can verify that the funds have been transferred, keeping the token in the lessee's name (Higgins, 2015). But if a payment is missed—or the term of the lease ends—the token automatically transfers back to the lessor. And, if the smart contract is attached to the lock in the car, it can automatically lock the person out and call for someone to pick it up.

8.3 What Problems Do Blockchains Create?

The promise of blockchain technology is only getting started. And over the coming years, there will be umpteen ideas on ways that the technology can be applied. However, the reality is that nothing is without fault. And there are both limitations and drawbacks to blockchains that must be considered.

The primary problem has to do with regulation and how to deal with the applications, smart contracts, and tokens that come from blockchains. There are three problems that entrepreneurs and regulators have been grappling with.

> *"It can become a problem when enterprises are trying to fit a square blockchain into a round use case. In some instances, they just don't fit."*

With smart contracts, the "code of law" might be different than a local jurisdiction's law. Take, for example, the DAO heist, which resulted in over $60 million in ether being stolen (Siegel, 2016). Many have argued that, under the "code of law," the individual that stole the $60 million was in the right due to them exploiting the code. However, many jurisdictions would argue that the individual who stole over $60 million in ether was, in fact, breaking the law. Which is correct: the code of law or the law of the land?

On the digital token side, there are regulatory hurdles. The ease in which a project can raise money through an Initial Coin Offering (ICO) goes against many of the traditional finance

rules. However, many of these projects would not pass the Howey Test, which is the SEC's way of determining whether something should be treated as a security.

But before the Howey Test (FindLaw, 2016) can be administered, it's important to understand whether a digital currency is a security, commodity, true money, or something else? And until that's determined, how can regulators pass functional rules? This results in ambiguity, which can leave many enterprises uncertain about which direction they should go.

[http://consumer.findlaw.com/securities-law/what-is-the-howey-test.html]

And the ultimate problem that blockchains create is that they can be expensive if they are not the right technology for the project at hand. It is natural that everyone is excited about blockchains, but it can become a problem when enterprises are trying to fit a square blockchain into a round use case. In some instances, they just don't fit.

Preventing this brings us back to what Bloq feels is the fundamental definition of a blockchain. If your project requires this, you're on the right track. The definition of a blockchain is:

Distributed, immutable databases that are technological infrastructure.

8.4 In Conclusion: The 9 Factors of Blockchain

Blockchains confound people even after so many years of being in existence. But there are nine factors of blockchains that are important to understand.

1. Trust shifting: Pre-blockchain, the trust was with the middleman. This resulted in increased costs and counterparty risk. Post-blockchain, the trust is with the system. So long as the network power is strong, the risk is low.
2. Decentralization: Another word for distribution; this means that the blockchain is spread out across multiple nodes, making it increasingly difficult to alter the blockchain.
3. Machine-to-Machine Automation: With blockchains and smart contracts, machines can communicate with each other, obviating the need for human intervention entirely.
4. Cryptography / PKI: Through the use of Public-Key Infrastructure, a cryptographic technology which requires both a public and private key, the blockchain is secure while also being open.
5. Permissionless: An individual can start contributing network power to a blockchain at any point without invitation, prior relationship, or any sort of identity.
6. Validity: As each block is sealed, it provides a continuous self-checking and cross-checking mechanism whereby previous transactions become further confirmed. And as more transactions are validated, the historical strength of the blockchain becomes greater.

www.elsevierdirect.com

7. Immutability: So long as the network power to a blockchain is strong, the cost of changing something will prove very costly, providing the trust that the chain is pure.
8. Uniqueness: Digital assets could be easily copied; however, blockchains don't allow this "Double Spend" problem to exist. When an asset is transferred, the recipient can rest easy knowing that the same asset won't then be sent to someone else.
9. Authentication: Everything on the blockchain can be both audited and authenticated, leading to further trust in the system.

It's true that blockchains are the future for so many different industries. And it is also true that only the tip of the iceberg has been exposed with where this technology is going. But recognizing the core function of a blockchain as a distributed, immutable database will provide the groundwork for determining whether this technology is applicable to your project.

References

Davenport, B., 2015. What is multi-sig and what can it do? Retrieved from Coin Center: http://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do, http://ethereum.stackexchange.com/questions/118/whats-the-difference-between-proof-of-stake-and-proof-of-work.

Coindesk, 2015. How bitcoin mining works. Retrieved from coindesk: http://www.coindesk.com/information/how-bitcoin-mining-works/.

Chavez-Dreyfuss, G., 2016. Sweden tests blockchain technology for land registry. Retrieved from Reuters: http://www.reuters.com/article/us-sweden-blockchain-idUSKCN0Z22KV.

FindLaw, 2016. What is the howey test? Retrieved from Findlaw: http://consumer.findlaw.com/securities-law/what-is-the-howey-test.html, https://github.com/trottier/original-bitcoin/blob/master/src/main.h#L1002.

Higgins, S., 2015. Visa debuts bitcoin proof of concept for car leasing. Retrieved from Coindesk: http://www.coindesk.com/visa-docusign-car-lease-proof-of-concept-bitcoin/.

Rosenfeld, D., 2012. Overview of colored coins. Retrieved from: https://bitcoil.co.il/BitcoinX.pdf.

Siegel, D., 2016. Understanding the DAO attack. Retrieved from Coindesk: http://www.coindesk.com/understanding-dao-hack-journalists/.

Stark, J., 2016. Making sense of smart contracts. Retrieved from Coindesk: http://www.coindesk.com/making-sense-smart-contracts/.

Szabo, N., 1997. Formalizing and securing relationships on public networks. Retrieved from First Monday: http://journals.uic.edu/ojs/index.php/fm/article/view/548/469.

Wikipedia, 2016. Data integrity – Wikipedia the free encyclopedia. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Data_integrity.

CHAPTER 9

Betting Blockchain Will Change Everything – SEC and CFTC Regulation of Blockchain Technology

Richard B. Levin[#] **, Peter Waltz**[##]**, Holly LaCount**[##]

Contents

9.1 Introduction 188

9.2 The Paper Crisis and the National Market System 189

9.2.1 The Paperwork Crisis 189

9.2.2 SEC Response 190

9.2.3 Securities Act Amendments of 1975 190

9.3 Blockchain Technologies 193

9.3.1 What Is Blockchain Technology? 194

9.3.2 Blockchain and Traditional Financial Services Technology 194

9.3.3 Restricted and Unrestricted Blockchains 195

9.4 SEC Regulation of Blockchain Technology 196

9.4.1 What Is a Security? 196

9.4.2 Securities Exchanges 197

9.4.3 ATS 198

9.4.4 Broker-Dealers 198

9.4.4.1 Engaged in the Business 199

9.4.4.2 "For the Account of Others" 199

9.4.4.3 Role of Compensation in Analysis 199

[#] Shareholder and the Chair of the FinTech and Regulation Practice of Polsinelli PC.

[##] Attorneys with Polsinelli PC.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00009-7
Copyright © 2018 Elsevier Inc. All rights reserved.

9.4.4.4 Effecting Transactions in Securities 200
9.5 BTC Trading Corp 200
9.5.1 Clearing Agencies 202
9.5.1.1 Clearing Corporations 202
9.5.1.2 Depositories 203
9.5.2 Transfer Agents 204
9.6 CFTC Regulation of Blockchain Technology 205
9.6.1 Introduction 205
9.6.2 Facts 205
9.6.3 CFTC Jurisdiction 207
9.6.4 The Actual Delivery Exception 207
9.6.5 Section 4(a) of the CEA 208
9.6.6 Section 4(d) of the CEA 208
9.6.7 Analysis 209
9.7 Conclusions 211
References 211
Note 212

"Silicon Valley and Wall Street are ***betting... the blockchain... can change... everything...***" (Goldman) Blockchain technologies have the potential to improve the trading of certain types of securities and derivatives and to address the limitations of the current post-trade process by modernizing, streamlining and simplifying the design of the financial industry infrastructure with a shared fabric of common information. (DTCC) There are several aspects of blockchain technologies that offer tremendous opportunities to improve existing processes, including the ability to validate securities transaction and the creation of an immutable record of transactions.

9.1 Introduction

While Blockchain technology has captured the imagination of the financial services industry, the technology will need to overcome a number of challenges before it can be widely adopted. (DTCC) The industry will need to determine whether using the technology is more cost effective than improving existing technology and whether it can overcome its inherent scale and

performance challenges. (Id.) The potential applications of blockchain technologies will also be subject to the rules adopted by regulators including the U.S. Securities and Exchange Commission ("SEC") and the U.S. Commodity Futures Trading Commission ("CFTC").

This chapter provides an introduction to the crisis of the 1960s that spurred the creation of the national market system which then spurred the growth of electronic trading, and the development of financial services technology. This chapter addresses the main features of a blockchain technologies and when blockchain technology platforms must register with the SEC as an exchange, an alternative trading system ("ATS"), a broker-dealer, a clearing agency, or as a transfer agent. Finally, this chapter examines a recent CFTC case that addressed whether a blockchain technology platform must register with the CFTC as a Futures Commission Merchant ("FCM").

To better understand the potential regulation of blockchain technology it is helpful to understand the causes of the development of the current national market system and model for regulation by the SEC.

9.2 The Paper Crisis and the National Market System

From 1934 through 1975, trading, clearance and settlement of securities in the United States was governed by the Securities Act of 1933 (the "Securities Act"), and the Securities Exchange Act of 1934 (the "Exchange Act"). The clearance and settlement of trades was governed by state laws. It was not until the late 1960s that the SEC began focusing on how securities transactions were cleared and settled. (Bergmann, L.)

9.2.1 The Paperwork Crisis

In the late 1960s and early 1970s, securities markets in the United States experienced a back-office crisis (the "Paperwork Crisis") caused by increasing volumes and back-office inefficiencies in processing securities transactions. (Id.) During the Paper Crisis, a brokerage firm used approximately 33 different documents to execute and record a single securities transaction. (Id.) These paper-based transactions slowed processing to the point where exchanges shortened the trading day to alleviate back-office delays. (Id.) Clerical personnel at firms were working day and night to process transactions. (Id.) As the mounds of paper grew, so did the number of errors in handling and recording transactions. (Id.)

The confusion and delays in the back offices of brokers and dealers were magnified by inadequate clearance and settlement facilities, particularly in the over-the-counter market. (Id.) Systems designed for the three million share days of 1960 proved incapable of dealing with

www.elsevierdirect.com

the astonishing volume of thirteen million share days around the end of the decade. (Id.) Operational deficiencies caused fail rates and customer complaints to soar. (Id.) Losses in 1967–1968 caused an unprecedented number of broker-dealer firm failures. (Id.) Approximately 160 New York Stock Exchange ("NYSE") member firms went out of business while others either merged or liquidated. Because the problems confronting the industry were industry-wide and could not be tackled in isolation, few immediate solutions were available. (Id.)

9.2.2 SEC Response

By the early 1970s, Congress examined the back-office crisis and asked the SEC to (1) compile a list of unsafe and unsound practices employed by brokers and dealers in conducting their business, (2) report to Congress on steps being taken to eliminate these practices, and (3) recommend additional legislation that might be needed to eliminate these unsafe and unsound practices. (Id.) In its study, the SEC found:

> ***There is no area of the securities business which offers more opportunity for reducing costs*** *as well as exposure to the kind of disruption which resulted in loss to customers during the 1969–1970 period than the improvement and modernization of the systems for clearing, settlement, delivery, and transfer of securities.* ***It was an archaic method of achieving this simple objective which nearly drowned the financial community in a tidal wave of uncontrolled paper****.*

(NSCC Order)

After extensive studies and hearings, Congress agreed that a fundamental weakness in the U.S. clearance and settlement system was the absence of a mechanism to give direction to, and ensure cooperation and coordination among, the entities engaged in securities processing – clearing corporations, securities depositories, transfer agents, and issuers. (Bergmann, L.) Industry practice combined with a lack of uniformity had failed to effectively support transaction processing in the U.S., and legislation soon followed. (NSCC Order)

9.2.3 Securities Act Amendments of 1975

In 1975, Congress enacted amendments to the Exchange Act finding that: (i) ***the prompt and accurate clearance and settlement of securities transactions is necessary for the protection of investors***; (ii) inefficiency imposes unnecessary costs on investors and intermediaries;

(iii) ***new data processing and communication techniques present opportunities for more efficient, effective, and safe clearing procedures***; and (iv) linking of clearance and settlement facilities, and the development of uniform standards and procedures, would reduce unnecessary costs and increase investor and intermediary protection. (15 U.S.C. § 78q-1(a)(1)(A)-(D))

The Securities Acts Amendments of 1975 (the "Securities Acts Amendments"), made sweeping changes to the federal securities laws, established the national market system and the national clearance and settlement system as they exist today. (15 U.S.C. §78q-1(a)(2)) Congress directed the SEC to, among other things: (i) facilitate the establishment of a national system for the prompt and accurate clearance and settlement of transactions in securities and (ii) end the physical movement of securities certificates in connection with the settlement among brokers and dealers of transactions in securities.

Two basic themes recur throughout the legislative history of the securities processing provisions of the Securities Acts Amendments: (i) prevent another paperwork crisis in the securities industry and (ii) establish a safe, efficient, and modern national clearing and settlement system. Section 17A of the Exchange Act gave the SEC the authority to facilitate: (i) the establishment of a national system for prompt and accurate clearance and settlement in securities and (ii) linked or coordinated facilities for clearance and settlement of related financial products.

Congress instructed the SEC that in developing a national market system, "competition, rather than regulation, should be the guiding force." (Hause Report) ***The SEC is mandated by Congress to facilitate the development of a national market system not to be its chief architect***. In establishing this mandate, Congress identified five criteria to guide the SECs role in the establishment of a national market system:

1. promotion of the development of mechanisms that allows for economically efficient execution of securities transactions;
2. promotion of fair competition;
3. promotion of transparency;
4. improvement of investor access to the best markets; and
5. the development of mechanisms that allow for investors' orders to be executed without the participation of a dealer.

(Section 11A(a) of the Exchange Act)

Congress did not grant the SEC unfettered authority over the national market system. The two "paramount objectives" of the national market system were "the maintenance of stable and orderly markets" and "the centralization of all buying and selling interest so that each investor will have the opportunity for the best possible execution of his order, regardless of where in the system it originates." (Senate Report (1975)) Congress did not instruct the SEC to dictate

www.elsevierdirect.com

the specific elements of a national market system. Rather, Congress chose to rely on an "approach designed to provide maximum flexibility to the [SEC] and the securities industry in giving specific content to the general concept of the national market system." (Id.)

Congress implemented this approach by adding Section 11A to the Exchange Act. Section 11A(a) directs the SEC to facilitate the establishment of a national market system in accordance with specific congressional findings and objectives. Among these findings were that new data processing and communications techniques created the opportunity for more efficient and effective market operations, and that the linking of all markets through such data processing and communications facilities would increase the information available to broker-dealers and investors. Congress stated in 1975 that the SEC would not have:

> ***either the responsibility or the power to operate as an "economic czar" for the development of a national market system***. *Quite the contrary, for a fundamental premise the bill is that the initiative for the development of the facilities of a national market system must come from private interests and will depend upon the vigor of competition within the securities industry...*

(Senate Report)

This is not to say that the SEC does not have an important role in the national market system. As Congress recognized in 1975:

> *Although the [SEC]'s basic role would be to remove burdens to competition which would unjustifiably hinder the market's natural economic evolution and to assure that there is a fair field of competition consistent with investor protection, in situations in which natural competitive forces cannot, for whatever reason, be relied upon, the SEC must assume a special oversight and regulatory role.*

(Id.)

While blockchain technology was not available in 1975, many technologists believe the technology could help the financial services industry accomplish many of the goals of the Securities Acts Amendments. The question for Congress and the industry will be how such technologies should be regulated by the SEC and the CFTC. To understand how blockchain technologies should be regulated, it is helpful to understand the technology.

www.elsevierdirect.com

9.3 Blockchain Technologies

Blockchain is a database structure that can only be updated by appending a new set (or block) of valid transactions to the log of previous transactions. (ECB Paper) As noted by Goldman Sachs in a note to clients:

> *In its most basic form, the* ***blockchain records ownership of bitcoin and transactions involving the crypto currency across a wide network of computers, as opposed to a centralized ledger****. Transactions are signed off by the parties involved using the software, checked by the network or the "crowd," then added to the blockchain – a long string of code that records all activity. Encryption in the software ensures these "blocks" cannot be tampered with or altered. And the decentralized nature means the "crowd" police the whole system.* ***The software cuts out the need for a "trusted middleman" to sit in between parties in a transaction, such as a bank or clearinghouse.*** *This makes transactions quicker, cheaper, and easier when compared to the current systems banks use.*

(Goldman) Many firms in the financial services industry believe blockchain technology can be adapted for use in traditional financial services transactions in a way that "***has the potential to redefine transactions and the back office of a multitude of different industries***. From banking and payments to ... trade settlement ... a distributed shared ledger has the potential to make interactions quicker, less-expensive and safer." (Goldman)

The focus of the financial services industry on blockchain technologies has attracted the attention of the SEC which recently hosted a FinTech Forum that included a panel discussion on blockchain technologies. (SEC FinTech Forum) The SEC has noted:

> *[T]he blockchain... is being tested in a variety of settings, to determine whether it has utility in the securities industry. What utility, if any, would a distributed public ledger system have for transfer agents, and how would it be used. What regulatory actions, if any, would facilitate that utility?* ***How would transfer agents ensure their use of or interaction with such a system would comply and be consistent with federal securities laws and regulations, including the transfer agent rule?***

(Transfer Agent Release)

www.elsevierdirect.com

9.3.1 What Is Blockchain Technology?

The idea of a blockchain was introduced in 2008 as a basis for the virtual currency Bitcoin, which is an example of an unrestricted blockchain.[1] (Nakamoto, S.) Blockchain technology is a distributed list of all transactions across a peer-to-peer network. Blockchain is the technology underlying Bitcoin and other digital currencies, and it has the potential to disrupt a wide variety of business processes. (PricewaterhouseCoopers) The blockchain is "authoritative" because every user agrees on it. (Id.) In some blockchain initiatives there are no central, regulated institutions playing any role in the process. (ECB Paper)

Advocates of blockchain technology believe it could substantially improve the trading, clearance and settlement of securities. (Id.) SEC Commissioner Stein believes "one could imagine a world in which securities lending, repo, and margin financing are all traceable though blockchain's transparent and open approach to tracking transactions." (Stein, K.)

9.3.2 Blockchain and Traditional Financial Services Technology

The technologies used by the financial services industry have developed over time as a network of mutually trusting institutions, with legal agreements and regulations designed to minimize risks, such as operational and counterparty risk, that are not directly related to the business of a securities issuer. (ECB Paper) Each institution trades with accountable and authorized counterparties, under the supervision and oversight of regulators. (Id.)

The adoption of blockchain technology will mean that competing financial institutions will be able to share a common digital representation of asset holdings and keep track of the execution, clearing and settlement of trades outside their legacy proprietary databases, and without the need for a central database management system. (Id.) Blockchain technology will enable users to become peers in a shared database, which they can rely on to record transfers of assets and to perform additional related activities involving multiple parties, such as trading, clearance, and settlement. (Id.)

Blockchain users can propose new transactions and, depending on the blockchain chosen, they can either contribute to validation collectively or have a subset of users responsible for this task. A transaction is validated when a specified proportion of the network's validators have reached a consensus as to its legitimacy. (Id.) Changes to the shared database are then reflected in its digitally signed versions, which users can store locally (either in their entirety or with only a subset of transactions/accounts visible). Users can then extract the updated information they need for conducting their respective businesses from these locally stored databases. (Id.)

Blockchains allow their users to store and access information relating to a given set of assets and their holders in a shared database of either transactions or account balances. (Id.) This information is distributed among users, who could then use it to settle their transfers of, or for example, securities and cash, without needing to rely on a trusted central validation system. (Id.)

In financial markets, the substantial de-materialization of securities and cash has progressively shifted the settlement of a trade from the physical delivery and paper-based recording, to a system of book transfers in digital databases. (Id.) What remains unchanged is the need for an authoritative "golden record" of holdings to be kept by specific financial market infrastructures, and for intermediaries involved in the settlement process to update their individual databases by communicating with the other institutions involved, at the different levels of post-trading, in order to be able to reflect the changes in each other's records. (Id.) The high cost of this type of reconciliation process has led many market players to consider distributed ledgers as an alternative to central validation systems – currently one per institution (internal records of outstanding positions) or per cluster of institutions (e.g. interoperable market infrastructure) – to keep their reciprocal records updated. (Id.)

Blockchains allow their users to reach consensus on a particular version of the distributed ledger, in particular on the sequential order of transactions. (Id.) This means that there cannot be any doubt as to the users' respective holdings. (Id.) Central validation is replaced in a blockchain by a set of cryptographic solutions and economic incentives that combine to prevent illicit updates and reconcile discrepancies. (Id.) The ledger produced can thus be considered authoritative, although its management is shared among users with conflicting incentives. (Id.)

9.3.3 Restricted and Unrestricted Blockchains

Blockchains can be divided into those which are restricted and those which are unrestricted. (Id.) Restricted blockchains are closed systems whose members are identified and accountable entities. (Id.) Updates to the blockchain can only be proposed and validated by authorized participants. (Id.) In unrestricted blockchains, by contrast, any entity can access the database and, depending on the specific validation method used, may be able to contribute to updating the ledger or to submit spam transactions to cause a denial of service. (Id.)

In a restricted blockchain the identity of participants is known, at least by its governance body. (Id.) This implies that any wrongdoer can be identified and his misbehavior can be punished in the case of future activity in the ledger. (Id.) Restricted blockchains also expose the conduct of any participants in the blockchain network to the set of rules and law-enforcement measures that typically apply to off-ledger activity. (Id.) By definition, users of unrestricted

blockchains cannot be held accountable outside the distributed ledger for their activity in the network. (Id.)

While blockchain technologies may be well suited to accomplishing the goals of the Securities Acts Amendments, the laws that regulate securities and commodities are not designed to regulate such innovative technologies.

9.4 SEC Regulation of Blockchain Technology

As noted by Commissioner Stein, "creative uses of blockchain are still in their infancy... [and] a lot of questions will need to be answered." (Stein, K.) Echoing Commissioner Stein's comments, SEC Chair White has noted: *"[b]lockchain technology has the potential to modernize*, ***simplify, or even potentially replace*** *current trading and clearing and settlement operations*." (White, M.J.) However, as White noted in the same speech:

> ***One key regulatory issue is whether blockchain applications require registration under existing [SEC] regulatory regimes, such as those for transfer agents or clearing agencies****. We are actively exploring these issues and their implications. [The SEC's] Advanced Notice of Proposed Rulemaking and Concept Release on transfer agent regulations... asked for public comment on the use of blockchain technology by transfer agents and how such systems fit within federal securities regulations.*

(Id.)

While there is tremendous potential for blockchain technology in the financial services industry, it is less clear how regulators in the United States will treat platforms that use blockchain technology in the financial or securities sectors. It is unclear if those platforms must register with the SEC as an exchange, an ATS, a broker-dealer, a clearing agency, or a transfer agent. Before regulators can address this issue, they must better understand in what instances blockchain technology involves transactions in securities.

9.4.1 What Is a Security?

The definitions of a "security" under the Securities Act and the Exchange Act are virtually identical and each is broad enough to include the various types of instruments that are used in commercial marketplaces that one might suspect to fall within the ordinary concepts of a security. (Securities Act and Exchange Act) This would include common instruments like

stocks, bonds, and notes, as well as the various collective investment pools and common enterprises devised by persons seeking to generate profits from the efforts and investments of others (i.e. investment contracts and instruments commonly known as securities).

The definition of a "security" under U.S. securities law does not include blockchain technology. However, the SEC has argued that investments in Bitcoin-related schemes that make use of blockchain technology are investment contracts – a contract, transaction, or scheme involving: (i) an investment of money, (ii) in a common enterprise, and (iii) with the expectation that profits will be derived from the efforts of the promoter or a third party. (BTC Trading Corp and Howey).

Assuming in certain instances blockchain technology platforms are deemed to be facilitating the trading or clearance and settlement of securities, the next issue is whether such platforms must register as an exchange, an ATS, a broker-dealer, a clearing agency, or a transfer agent.

9.4.2 Securities Exchanges

Section 3(a)(1) of the Exchange Act defines an "exchange" as "any organization, association, or group of persons, whether incorporated or unincorporated, which constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange as that term is generally understood, and includes the market place and the market facilities maintained by such exchange." Exchange Act Rule 3b-16(a) interprets the definition to mean any organization, association, or group of persons that: (1) ***brings together the orders of multiple buyers and sellers*** and (2) uses established, nondiscretionary methods (***whether by providing a trading facility*** or by setting rules) ***under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of a trade***.

Rule 3b-16(b) of the Exchange Act expressly excludes the following systems from the meaning of "exchange": (1) systems that merely route orders to other facilities for execution; (2) systems operated by a single registered market maker to display its own bids and offers and the limit orders of its customers, and to execute trades against such orders; and (3) systems that allow persons to enter orders for execution against the bids and offers of a single dealer. Absent an exemption, an exchange must register as a national securities exchange pursuant to section 6 and section 19(a) of the Exchange Act. (Colby, R.)

If a blockchain technology platform brings together multiple buyers and sellers of digital assets that are deemed securities, the platform could be required to register as a securities exchange unless it falls within an exclusion from registration.

9.4.3 ATS

In 1998, the SEC adopted Regulation ATS, which allows an ATS to choose whether to register as a national securities exchange or to register as a broker-dealer and comply with additional requirements of Regulation ATS. (Regulation ATS) An "alternative trading system" means any organization, association, person, group of persons, or system: (1) that constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange within the meaning of Rule 3b-16 under the Exchange Act, and (2) that does not set rules governing the conduct of subscribers other than the conduct of such subscribers' trading on such organization, association, person, group of persons, or system; or discipline subscribers other than by exclusion from trading. (Regulation ATS, Rule 300(a))

Any system exercising self-regulatory powers, such as regulating its members' or subscribers' conduct when engaged in activities outside of that trading system, must register as an exchange or be operated by a national securities association. (Colby, R.) The SEC can effectively require a dominant ATS to register as a national securities exchange if it finds it is necessary or appropriate in the public interest or consistent with the protection of investors. (Rule 3a1-1(b))

A blockchain technology platform may be required by the SEC to register as an ATS if it maintains a market place or facilities for bringing together purchasers and sellers of digital assets that are deemed securities, and it does not set rules governing the conduct of subscribers other than the conduct of such subscribers' trading on such platform. If the platform is not required to register as an ATS, the operator of the platform may be required to register as a broker-dealer.

9.4.4 Broker-Dealers

Section 15 of the Exchange Act requires registration with the SEC of all broker-dealers using interstate commerce or the facilities of any national securities exchange to effect transactions in securities (other than exempted securities and certain short-term debt instruments). Section 3(a)(4)(A) of the Exchange Act defines a "broker" as "any person engaged in the business of effecting transactions in securities for the account of others." The Exchange Act and the rules thereunder do not define these terms. The courts and the SEC have taken an expansive view of the scope of these terms. (Colby, R.) The SEC and the courts apply a "facts and circumstances" analysis in evaluating whether a person has acted as a broker, with no single element being dispositive. (Id.)

www.elsevierdirect.com

Depending on the circumstances, the operator of a blockchain technology platform may be deemed a broker-dealer if the operator of the platform is deemed to be engaged in the business of effecting transactions in securities for the account of others.

9.4.4.1 Engaged in the Business

Courts have read "engaged in the business" as connoting a certain regularity of participation in purchasing and selling activities rather than a few isolated transactions. (Id.) Two factors are important in determining whether there is "regularity of business": the number of transactions and clients, and the dollar amount of securities sold, as well as the extent to which advertisement and investor solicitation were used. (Id.)

Besides "regularity of business," courts and the SEC have identified several other factors which indicate that a person is "engaged in the business." (Id.) These factors include: (i) receiving transaction-related compensation; (ii) holding oneself out as a broker, as executing trades, or as assisting others in settling securities transactions; and (iii) soliciting securities transactions.

The operator of a blockchain technology platform could be deemed to be engaged in the business of effecting transactions in securities because it will more than likely receive transaction-related compensation, execute trades for users of the platform, and solicit users to engage in such transactions.

9.4.4.2 "For the Account of Others"

In order to be considered a "broker," a person must be effecting transactions in securities for others, not itself. (Colby, R.) A firm effecting transactions solely on its own behalf is generally not considered to be acting as a "broker." (Id.)

Unless the operator the blockchain technology platform is executing all transactions as a principal to the transaction, the platform operator could be deemed to be effecting transactions in securities for others.

9.4.4.3 Role of Compensation in Analysis

In SEC guidance and enforcement actions, the agency has stated that receiving commissions or other transaction-related compensation is one of the determinative factors in deciding whether a person is a "broker" subject to the registration requirements under the Exchange Act. (SEC Study of Investment Advisers and Broker-Dealers) Transaction-related compensation refers to compensation based, directly or indirectly, on the size, value or completion of

www.elsevierdirect.com

any securities transactions. The SEC will look behind the terms of a compensation arrangement to determine its economic substance, that is, to determine whether it is transaction-related. (Definition of Terms) The receipt of transaction-based compensation often indicates that a person is engaged in the business of effecting transactions in securities. (Colby, R.)

If the operator of a blockchain technology platform receives transaction-related compensation, in the sale of a digital asset that is deemed a security, the platform could be deemed to be acting as a broker-dealer.

9.4.4.4 Effecting Transactions in Securities

Courts and the SEC have determined that a person "effects transactions in securities" if the person participates in such transactions "at key points in the chain of distribution." (Mass. Fin. Servs., Inc. v. Sec. Investor Prot. Corp.) According to the SEC, such participation may include, among other activities: (i) assisting an issuer to structure prospective securities transactions; (ii) helping an issuer to identify potential purchasers of securities; (iii) screening potential participants in a transaction for creditworthiness; **(iv)** ***soliciting securities transactions (including advertising)***; (v) negotiating between the issuer and the investor; (vi) making valuations as to the merits of an investment or giving advice; (vii) ***taking, routing or matching orders, or facilitating the execution of a securities transaction***; (viii) handling customer funds or securities; and (ix) preparing and sending transaction confirmations (other than on behalf of a broker-dealer that executes the trades). Handling customer funds may also include handling customer's digital currencies, such as Bitcoin, in connection with Bitcoin-denominated securities transactions. (BTC Trading Corp.)

A platform that facilitates transactions in digital assets could be deemed effecting securities transactions if it is helping an issuer to identify potential purchasers of securities. The platform could also be deemed to be effecting securities transactions because it is soliciting securities transactions and facilitating negotiations between the issuer and the investor. The operator of a digital currency trading platform could be deemed to be effecting transactions in securities because it is taking, routing or matching orders, or facilitating the execution of a securities transaction. Finally, the operator of a digital asset trading platform could be deemed to be effecting transactions because it is handling customer funds (even if the funds are a digital currency) or securities.

9.5 BTC Trading Corp

In *Securities Exchange Commission v. BTC Corp.*, the SEC sanctioned a computer programmer for operating two online platforms that traded securities purchased with the virtual

currencies Bitcoin or Litecoin without registering the venues as broker-dealers or stock exchanges. (BTC Trading Corp.) The programmer, Ethan Burnside, also was sanctioned for conducting unregistered offerings. (Id.)

Burnside and his company BTC Trading Corp. operated two online enterprises – BTC Virtual Stock Exchange and LTC-Global Virtual Stock Exchange. (Id.) These exchanges provided account holders the ability to use Bitcoin or Litecoin to buy, sell and trade securities of businesses (primarily virtual currency-related entities) listed on the exchanges' websites. (Id.) The platforms were not registered as broker-dealers despite soliciting the public to open accounts and trade securities. (Id.) The platforms were not registered as stock exchanges despite enlisting issuers to offer securities for the public to buy and sell. (Id.) Burnside conducted separate transactions in which he offered investors the opportunity to use virtual currencies to buy or sell shares in the LTC-Global exchange itself and a separate Litecoin mining venture he owned and operated. (Id.) These offerings were not registered with the SEC as required under the federal securities laws. (Id.)

Burnside operated two online enterprises that were not properly registered to engage in the securities business they were conducting. (Id.) (Calamari, A.) BTC Trading Corp. and Burnside actively solicited the public to open accounts by advertising the websites for both of his stock exchanges on the Bitcoin Forum and other websites dedicated to virtual currency. (BTC Trading Corp.) The solicitation efforts resulted in approximately 2,655 users opening online accounts with LTC-Global exchange and executing approximately 60,496 trades through the website, paying a total of 12,081 litecoins in transaction-based compensation. (Id.) Approximately 7,959 users opened online accounts with the BTC exchange and executed approximately 366,490 trades through the website, paying a total of 2,141 bitcoins in transaction-based compensation. (Id.) The SEC found that in this line of business, Burnside and BTC Trading Corp. were required to register their online enterprises with the SEC as brokers or dealers. (Id.)

The SEC also found that Burnside and BTC Trading Corp. failed to register the LTC-Global exchange or the BTC exchange as exchanges despite providing issuers a platform to create and list initial and secondary offerings of securities in exchange for a listing fee. (Id.) A total of 52 issuers paid BTC Trading Corp. 11,450 litecoins in listing fees to list their shares with the LTC-Global exchange, and 69 issuers paid 210 bitcoins in listing fees to list their shares with the BTC exchange. (Id.)

The SEC concluded that Burnside and BTC Trading Corp. willfully violated Sections 5 and 15(a) of the Exchange Act. (Id.) Without admitting or denying the SEC's findings, Burnside and BTC Trading Corp. consented to cease and desist from committing or causing any future violations of the registration provisions. (Id.) Burnside agreed to be barred from the securities

industry with the right to reapply after two years, and to pay $58,387.07 in disgorgement and prejudgment interest plus a penalty of $10,000. (Id.)

Any firm that is planning to operate a platform that uses blockchain technology to facilitate trading should proceed with caution. While the SEC has not taken not the position that digital currencies are securities, the SEC has taken the position that transactions that use digital currencies can constitute the consideration for a purchase or sale of securities and the trading of such securities may require registration with the SEC as a broker, a dealer, an ATS, an exchange.

While the BTC Trading Corp. case is instructive on the issue of whether certain blockchain technology platforms must register as a broker, a dealer, or an exchange, the SEC has not addressed in what instances a blockchain technology platform must register as a clearing agency.

9.5.1 Clearing Agencies

Congress directed the SEC in 1975 to facilitate the establishment of a national system for the prompt and accurate clearance and settlement of securities transactions when it added Section 17A to the Exchange Act as part of the Securities Acts Amendments. (Clearing Agency Standards) At the time of the adoption of the Securities Acts Amendments, the Senate Committee on Banking, Housing and Urban Affairs stated the "banking and security industries must move quickly toward the establishment of a fully integrated national system for the prompt and accurate processing and settlement of securities transactions". (Senate Report)

A key component of the SEC's supervision of the securities clearance and settlement system is its authority to regulate clearing agencies. Before performing clearing agency functions, including trade comparison, netting, matching, and settlement activities, intermediaries must either register with the SEC or apply for an exemption from registration. The SEC's ability to achieve these goals and its supervision of securities clearance and settlement systems is based on the regulation of registered clearing agencies. (Clearing Agency Standards)

Clearing agencies are self-regulatory organizations that are required to register with the SEC. There are two types of clearing agencies: clearing corporations and depositories.

9.5.1.1 Clearing Corporations

Clearing corporations compare member transactions (or report to members the results of exchange comparison operations), clear those trades and prepare instructions for automated settlement of those trades, and often act as intermediaries in making those settlements. (Clearing Agencies) Clearing corporations provide several essential services to the market, including

comparing and confirming trade data submitted by participants (or reporting to participants the results of trade comparisons submitted by the exchanges), acting as the common counterparty and guaranteeing the completion of the trade if either side defaults or goes out of business, and preparing instructions for their participants regarding their settlement obligations. Clearing corporations generally instruct depositories to make securities deliveries that result from settlement of securities transactions.

A blockchain technology platform could be required to register as a clearing corporation if it compares the trades of users of the platform, clears the trades, and prepares instructions for automated settlement of the trades. The platform could also be required to register as a clearing corporation if the platform acts as the common counterparty and guarantees the completion of trades.

9.5.1.2 Depositories

In 1975 Congress considered the idea of separately regulating securities depositories, but instead defined clearing agencies in §3(a)(23)(A) to include depositories. There are statutory exceptions in §3(a)(23)(B), including: (1) any national securities exchange or solely by reason of its providing facilities for comparison of data respecting the terms of settlement of securities transactions effected on such exchange or by means of any electronic system; and (2) any bank, broker, dealer, if such bank, broker, dealer would be deemed to be a clearing agency solely by reason of functions performed by such institution as part of customary brokerage.

Depositories provide multiple services to the market by retaining custody of equity and debt securities issues and maintaining ownership records. The organization also effects deliveries of securities between participants via a book entry system that transfers ownership of securities electronically, thus eliminating the need for the physical movement of securities. Depositories receive instructions from the clearing corporation to deliver and receive securities on behalf of its participants, or from participants themselves, to move securities from one participant's account to another. The institutions also communicate with settling banks to net settle any financial obligations. Depositories hold securities certificates in bulk form for their participants and maintain ownership records of the securities on their own books.

A blockchain technology platform that retains *custody* of digital assets that are deemed securities could be deemed to be acting as a depository. In the BTC Trading Corp. case the SEC concluded the defendants had *custody* and control of customer funds by virtue of controlling the digital wallet in which the assets were stored. (BTC Trading Corp.) Similarly, a blockchain technology platform could be deemed to be acting as a depository if it effects deliveries of securities between participants via the blockchain (a book entry system that transfers ownership of electronically), without the need for the physical movement of securities.

www.elsevierdirect.com

Even if a blockchain technology platform is not deemed to be acting as a depository, it could be deemed to be acting as a transfer agent.

9.5.2 Transfer Agents

A "transfer agent" is defined in section 3(a)(25) of the Exchange Act as "any person who engages on behalf of an issuer of securities or on behalf of itself as an issuer of securities in: (i) countersigning such securities upon issuance, (ii) monitoring the issuance of such securities with a view to preventing unauthorized issuance, a function commonly performed by a person called a registrar, ***(iii) registering the transfer of such securities, (iv) exchanging or converting such securities, or (v) transferring record ownership of securities by bookkeeping entry without physical issuance of securities certificates***". Transfer agents are required to register with the SEC.

Transfer agents record changes of ownership, maintain the issuer's security holder records, cancel and issue certificates, and distribute dividends. Because transfer agents stand between issuing companies and security holders, efficient transfer agent operations are critical to the successful completion of secondary trades. Section 17A(c) of the Exchange Act requires that transfer agents be registered with the SEC, or if the transfer agent is a bank, with a bank regulatory agency. (SEC – Transfer Agents) No registered self-regulatory organization governs transfer agents. (Id.) The SEC has promulgated rules and regulations for all registered transfer agents, intended to facilitate the prompt and accurate clearance and settlement of securities transactions and that assure the safeguarding of securities and funds. (Id.) The rules include minimum performance standards regarding the issuance of new certificates and related record-keeping and reporting rules, and the prompt and accurate creation of security holder records and the safeguarding of securities and funds. The SEC also conducts inspections of transfer agents. (Id.)

A blockchain technology platform could be required to register as a transfer agent if it monitors the issuance of securities or registers the transfers of securities. While it is unlikely a blockchain technology platform would countersign securities, platforms like the Distributed Autonomous Organization ("DAO") could be deemed to be monitoring the issuance of securities with a view of preventing unauthorized issuance (i.e., a registrar, registering the transferring of such securities). Other blockchain platforms could be deemed to be registering the transfer of securities, exchanging or converting securities, or transferring record ownership of securities by a bookkeeping or ledger entry without physical issuance of securities certifications.

Any firm that is planning to trade in or develop a platform that uses blockchain technology to clear or settle transactions in securities should proceed with caution. While the SEC has not

taken not the position that digital currencies are securities, the SEC has taken the position that transactions that use digital currencies may involve securities and the trading, clearance, or settlement of such securities transactions may require registration with the SEC as a broker, a dealer, an ATS, an exchange, a clearing agency, or a transfer agent.

While the SEC has addressed the issue of whether a blockchain technology platform must register as a broker, a dealer, or an exchange, and has solicited public comment on whether a blockchain technology platform must register as a transfer agent, the CFTC has not addressed in what instances a blockchain technology platform must register with the CFTC.

9.6 CFTC Regulation of Blockchain Technology

On June 2, 2016, the CFTC entered into a settlement agreement with Bitfinex for offering illegal off-exchange financed retail commodity transactions in Bitcoin and other digital currencies, and for failing to register as a Futures Commission Merchant ("FCM") as required by the Commodity Exchange Act ("CEA"). The Order requires Bitfinex to pay a $75,000 civil monetary penalty and to cease and desist from future such violations of the Act.

9.6.1 Introduction

The Bitfinex case is of interest to blockchain technology platforms because it marks the most recent action in which the CFTC has confirmed its belief that digital currency is a commodity and can therefore be regulated under the CEA. Unlike previous CFTC actions against Derivabit and TeraExchange, the CFTC spent relatively little time on the issue of whether digital currencies are commodities. The CFTC appears to have taken the position that all digital currencies are commodities. The CFTC bases its commodity argument on the belief that the definition of "commodity" in §1a(9) of the CEA is broad, and includes, among other things, "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in."

The Bitfinex case is of interest to blockchain technology platforms because it is the first time the CFTC has expressed an opinion with respect to the applicability of the exception for contracts of sale of a commodity that result in actual delivery within 28 days to transactions involving blockchain technology and digital wallets.

9.6.2 Facts

Bitfinex operated an online platform for exchanging and trading digital currencies, mainly Bitcoins. Bitfinex's "Exchange Trading" feature permitted users to exchange dollars for Bitcoins and to trade other digital currencies. Users accessed Bitfinex's platform and placed

orders through its website. Bitfinex also offered users a "Margin Trading" feature. Through this feature, Bitfinex permitted traders to borrow dollars and Bitcoins from other users on the platform in order to open leveraged positions on Bitfinex's exchange. Bitfinex referred to the participants on the platform who act as lenders as "Margin Funding Providers."

In order to initiate a loan, Margin Funding Providers entered offers in Bitfinex's online tool to lend funds with their own chosen terms, or they could lend at the "Flash Return Rate" set by the market. When an offer to borrow was accepted by a trader ("Financing Recipient"), the Financing Recipient could use the borrowed funds to buy or sell Bitcoins on Bitfinex's exchange. In addition to repaying the borrowed funds, Financing Recipient were responsible for paying fees and interest to the Margin Funding Providers. Bitfinex was not a principal, counterparty, or market-maker in any Bitcoin trade. Bitfinex administered and enforced the contracts established between Margin Funding Providers and Financing Recipients.

From April 2013 to August 2015, when a customer purchased Bitcoins on Bitfinex, the purchased Bitcoins were held for the benefit of the buyer in Bitfinex's omnibus settlement wallet. The individual customer interests in the omnibus settlement wallet were accounted for in real time on Bitfinex's database. However, the omnibus settlement wallet was owned and controlled by Bitfinex and Bitfinex held all "private keys" associated with its omnibus settlement wallet. Financing Recipients had no rights to access or use the bitcoins that they had purchased until Bitfinex released them, following satisfaction of the Financing Recipient's outstanding loan. Bitfinex considered Bitcoins held in the omnibus wallet to belong to the Financing Recipients, but subject to a lien in the amount of any outstanding loan plus fees owed to the Margin Funding Provider.

In August 2015, Bitfinex changed its model so that Bitcoins purchased using the Exchange Trading feature were held in multi-signature wallets established by a third-party firm that were individually enumerated for each trader. Bitcoins purchased using the Exchange Trading feature were settled to the Blockchain on an intra-day basis. However, Bitfinex retained control over the private keys to these wallets as well.

In January 2016, Bitfinex changed its model again so that Bitcoins purchased using both the Exchange Trading and Margin Trading features were held in individually enumerated, multi-signature wallets. However, Bitfinex continued to retain control over the private keys to those wallets.

Bitfinex's Margin Trading services were available to retail customers, and are not limited to eligible contract participants ("ECPs") or eligible commercial entities ("ECEs"). However, corporate users comprised a significant portion of Bitfinex's trading volume during the Relevant Period. In 2015, 88% of the dollars deposited to and withdrawn from Bitfinex were by corporate users.

Bitfinex's platform permitted users, including individuals and entities that did not meet the definition of an eligible contract participant or eligible commercial entity, to borrow funds from other users on the platform in order to trade Bitcoins on a leveraged, margined, or financed basis. Bitfinex was not registered with the CFTC.

According to the CFTC, Bitfinex "did not actually deliver" Bitcoins "purchased on a leveraged, margined, or financed basis to the traders who purchased them" Bitfinex held the purchased Bitcoins in electronic wallets that it owned and controlled. Bitfinex offered a "Margin Trading" feature permitted traders to borrow dollars and bitcoins from other users on the platform to purchase other currencies on the exchange.

As part of the Title VII of the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd–Frank Act"), the CFTC was given more extensive jurisdiction which broadly applies to transactions with non-eligible contract participants or non-eligible commercial entity and financing on a leveraged or margined basis. Further, those transactions are subject to §4(a), §4(b), and §4b of the CEA which subjects the transaction to be treated "as if the agreement, contract, or transaction was a contract of sale of a commodity for future delivery." These provisions require those entities that are dealing with a future delivery to be registered with the CFTC.

9.6.3 CFTC Jurisdiction

Title VII of the Dodd–Frank Act amended the CEA and gave the CFTC new authority over certain leveraged, margined, or financed retail commodity transactions. Section 742(a) of the Dodd–Frank Act added Section 2(c)(2)(D) to the Act. That jurisdictional provision broadly applies to any agreement, contract, or transaction in any commodity that is entered into with, or offered to (even if not entered into with), a non-eligible contract participant ("non-ECP") or non-eligible commercial entity ("non-ECE") on a leveraged or margined basis, or financed by the offeror, the counterparty, or a person acting in concert with the offeror or counterparty on a similar basis. Section 2(c)(2)(D) further provides that such an agreement, contract, or transaction shall be subject to Sections 4(a), 4(b), and 4b of the CEA "as if the agreement, contract, or transaction was a contract of sale of a commodity for future delivery."

9.6.4 The Actual Delivery Exception

Section 2(c)(2)(D)(ii) of the CEA excepts certain transactions from CFTC jurisdiction. Section 2(c)(2)(D)(ii)(III)(aa) excepts a contract of sale that results in "actual delivery" within 28 days...." The CFTC has stated the determination of whether "actual delivery" has occurred within the meaning of Section 2(c)(2)(D)(ii)(III)(aa) of the CEA:

requires consideration of evidence beyond the four corners of the contract documents. In determining whether actual delivery has occurred, the [CFTC] employs a functional approach to assess whether there has been a "real and immediate" transfer of "possession and control" to the "buyer or the buyer's agent" of the commodity.

The CFTC examines how the agreement, contract, or transaction is marketed, managed, and performed. Ownership, possession, title, and physical location, as well as the relationships between the buyer, seller, and possessor of the commodity, and the manner in which the sale is recorded and completed are all relevant considerations in determining whether there has been actual delivery. Thus, physical delivery of the entire quantity of the commodity, including the portion purchased using leverage, margin or financing, into the possession of the buyer, or a depository other than the seller, the seller's parent company, partners, agents and affiliates will satisfy the actual delivery exception, provided that the purported delivery is not a sham. By contrast, actual delivery will not have occurred if only a "book entry" is made by the seller purporting to show that delivery of the commodity has been made.

9.6.5 Section 4(a) of the CEA

Retail commodity transactions within the scope of Section 2(c)(2)(D) of the CEA are subject to enforcement under Section 4(a) of the Act, among other provisions, as if such transactions are commodity futures contracts. Section 4(a) of the CEA makes it unlawful for any person to offer to enter into, execute, confirm the execution of, or conduct an office or business in the United States for the purpose of soliciting, or accepting any order for, or otherwise dealing in any transaction in, or in connection with, a commodity futures contract, unless such transaction is made on or subject to the rules of a board of trade that has been designated or registered by the CFTC as a contract market or derivatives transaction execution facility for the specific commodity.

9.6.6 Section 4(d) of the CEA

Section 4d(a) of the CEA requires all persons acting as futures commission merchants ("FCMs") to register with the Commission. Section 1a(28) of the Act defines an FCM as an individual, partnership, corporation or trust, that is engaged in soliciting or accepting orders for retail commodity transactions, or that accepts money in connection with such transactions.

www.elsevierdirect.com

9.6.7 Analysis

The CFTC concluded that Bitfinex's platform did not fall within the scope of the actual delivery exception to the Act. While discussing the past guidance from the CFTC on the actual delivery exemption, the Bitfinex Order relies on an option from the Eleventh Circuit Court of Appeals which does not make reference to this guidance. In that case the court stated the term: "actual delivery" is unambiguous, and is therefore given its ordinary meaning. "Delivery" is "[t]he formal act of transferring something; it denotes a transfer of possession and control." The Bitfinex order the CFTC stated:

> *[a]ctual delivery" denotes "[t]he act of giving real and immediate possession to the buyer or the buyer's agent." Id. "Actual delivery" is distinct from "constructive delivery."... (holding that "the electronic transfer of documents indicating control or possession" without physical transfer of the commodity "is by any definition constructive, rather than actual."); "Actual" is that which "exist[s] in fact" and is "real," rather than constructive.*

(Bitfinex Order)

The CFTC concluded Bitfinex's transactions did not result in actual delivery to the Financing Recipients who traded on Bitfinex's platform. Bitfinex did not transfer possession and control of any bitcoin to the Financing Recipients, unless and until all liens on the bitcoin were satisfied. Prior to satisfaction of the liens, the Financing Recipients' Bitcoins were held in an omnibus settlement wallet owned and controlled by Bitfinex, and to which Bitfinex held the private keys needed to access the wallet.

The CFTC found Bitfinex's accounting for individual customer interests in the Bitcoin held in the omnibus settlement wallet in its own database was insufficient to constitute "actual delivery" noting that "book entry" purporting to show delivery is insufficient to fall within the scope of the exemption. The CFTC also noted the exemption did not apply because Bitfinex's change to its model in August 2015 and January 2016, where it retained control over the private keys to those wallets, and because the Financing Recipients had no contractual relationship with the third-party firm that established the wallets.

The Bitfinex order is of interest because the CFTC did not rely on its own guidance on the "functional approach" for evaluating the applicability of the actual delivery exemption set forth in the CFTC's past guidance. Instead the CFTC staff relied on a plain language application of the term that did not look "beyond the four corners of [the] contract[s]" traded on the Bitfinex platform to determine whether the actual delivery had occurred within 28 days. Similarly, the CFTC did not "examine how the ... contract, or transaction" on the Bitfinex platform

was "marketed, managed, and performed..." The CFTC also found the fact that Bitfinex had the authority to force liquidate customers' positions without the customers' prior consent if their equity fell beneath a preset level, which further evidenced Bitfinex's possession and control over the bitcoins. Finally, the CFTC concluded that the delivery of digital currencies from the digital wallet of a user of the Bitfinex platform, to another use of the Bitfinex platform, was because it was similar to a "book entry" by a seller that purported to show that delivery of the digital currency had been made.

Throughout the course of a year, Bitfinex used several different means of delivery. First, delivery was made to a wallet owned and controlled by Bitfinex (a single-signature wallet). Then, the model was voluntarily changed to a multi-signature wallet established by a third-party firm whereby Bitfinex still had control over the private keys, but was no longer a single-sig wallet. Finally, in January 2016 Bitfinex began using individually enumerated multi-signature wallets where the Bitfinex continued to retain control over the private key. None of these solutions were enough for the CFTC to find there to be "actual delivery" and therefore these models of delivery did not allow Bitfinex to qualify for the exemption from jurisdiction.

Following this analysis to its conclusion, all transfers of digital currencies between digital wallets could be deemed to fall outside the scope of the actual delivery exemption. The CFTC draws a distinction between *"actual"* versus *"constructive"* delivery. The CFTC views actual delivery as "the act of giving real and immediate possession to the buyer or the buyer's agent." Whereas, constructive delivery is defined as "an act that amounts to a transfer of title by operation of law when actual transfer is impractical or impossible." The CFTC argues that actual delivery must be met before the exception applies and actual delivery does not occur in any of Bitfinex's three delivery models.

If delivery to a digital wallet is not "actual delivery," then when could actual delivery ever take place? Further, if actual delivery is not met within the digital commodity space, how is it ever achieved with other commodities regulated by the CFTC? These are the hard questions not yet addressed by the CFTC. While this is the first time it has taken the question of delivery head on, it will likely not be the last as the CFTC strives to have a stronger grasp on regulating digital currency and as more platforms ask for answers to these hard questions.

Any firm that is planning to trade in or develop a platform to facilitate the trading of virtual currencies should proceed with caution, particularly if the platform proposes to offer users of the platform the ability to engage in margin or leverage trading. While the CFTC has taken the position that digital currencies are commodities, and that transfers between digital wallets do not fall within the scope of the actual deliver exception to the Act, these positions have not been confirmed by an act of Congress, the courts, or CFTC rules that have been subject to public comment under the Administrative Procedure Act.

Any firm that is looking to operate a platform to facilitate the trading of digital currencies should make sure the platform is properly structured to comply with the CEA. Due to the lack of clearly defined guidance with respect to the authority of the CFTC, and other regulators to supervise digital currencies, it is important that you engage experienced counsel to assist you in navigating the regulatory requirements that may apply to any business you are building.

9.7 Conclusions

Silicon Valley and Wall Street are betting blockchain technology can change everything. Blockchain technology has the potential to improve the trading of certain types of securities and derivatives and to address the limitations of the current post-trade process. These optimistic appraisals have been echoed by former Chair White and Commissioner Stein of the SEC.

While the technology is not fully mature, blockchains represent an attractive option for financial institutions to improve the efficiency of trading and post-trading functions. However, there are a number of technological and regulatory barriers to widespread adoption of the technology. Before blockchain technology can be deployed across various sectors of the financial services industry, it is imperative that regulators in the United States, Europe, and Asia provide meaningful guidance to the industry on whether the use of blockchain technology requires users of the technology to register as brokers, dealers, ATSs, exchanges, clearing houses, or transfer agents.

While there is significant potential for the use of blockchain technology in the financial services industry, there is considerable work that must be done to more clearly define the regulations that apply to such technology. The regulation of securities exchanges in the United States and Europe has not undergone meaningful changes since the early part of the last decade. Regulation of clearing houses in the United States has not been considered in a meaningful way since the early 1980s. Unfortunately, the review of the laws, rules, and regulations in both areas did not consider the use of blockchain technology.

References

Bergmann, L., 2004. Speech: International Securities Settlement Conference – "The U.S. view of the role of regulation in market efficiency" ("Bergmann"). Available at https://www.sec.gov/news/speech/spch021004leb.htm.

Colby, R., 2015. What is a broker-dealer? Available at https://www.davispolk.com/sites/default/files/files/.../WhatisaBroker-Dealer.pdf.

DTCC, 2016. Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-trade Landscape ("DTCC"). Available at http://www.dtcc.com/news/2016/january/25/blockchain-white-paper.

Goldman Sachs, 2015. Emerging Theme Radar: What if I Told You... ("Goldman"). Available at http://www.goldmansachs.com/our-thinking/pages/what-if-i-told-you-full/, 2015.
H.R. Rep. No. 94-229, 94th Cong., 1st Sess. 92 (1975) ("House Report").
In re BTC Trading, Corp., SEC Release No. 34-73783, 2014 ("BTC Trading Corp."). Available at https://www.sec.gov/litigation/admin/2014/33-9685.pdf.
Mass. Fin. Servs., Inc. v. Sec. Investor Prot. Corp., (1977) 411 F. Supp. 411, 415 (D. Mass.), aff'd, 545 F.2d 754 (1st Cir. 1976), cert. denied, 431 U.S. 904 (1977).
Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System ("Nakamoto"). Available at https://bitcoin.org/bitcoin.pdf.
Pinna, A., Ruttenberg, W., 2016. Distributed ledger technologies in securities post-trading. European Central Bank ("ECB Paper"). Available at https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.
PricewaterhouseCoopers, 2016. What is the blockchain? Available at http://www.pwc.com/us/en/financial-services/publications/qa-what-is-blockchain.html.
Securities Acts Amendments of 1975, Pub.L. 94-29, 89 Stat. 97 (1975). Available at http://legislink.org/us/pl-94-29.
Securities Act of 1933.
Securities Exchange Act of 1934.
Securities Exchange Act Release No. 13163 (Jan. 13, 1977), 42 Fed. Reg. 3916 (January 21, 1977) ("NSCC Order").
Securities Exchange Act Release No. 40760 (Dec. 8, 1998), 63 Fed. Reg. 70844 (Dec. 22, 1998) ("Regulation ATS"). Available at https://www.federalregister.gov/documents/1998/12/22/98-33299/regulation-of-exchanges-and-alternative-trading-systems.
Securities Exchange Act Release No. 68080 (Oct. 22, 2012), 77 Fed. Reg. 66219 (Nov. 2, 2012) ("Clearing Agency Standards"). Available at https://www.federalregister.gov/documents/2012/11/02/2012-26407/clearing-agency-standards, Oct. 22, 2012.
Securities Exchange Act Release No. 44291 (May 11, 2001), 66 Fed. Reg. 27759 (May 18, 2001) (Definition of Terms in and Specific Exemptions for Banks, Savings Associations, and Savings Banks Under Sections 3(a)(4) and 3(a)(5) of the Securities Exchange Act of 1934). Available at https://www.gpo.gov/fdsys/pkg/FR-2001-05-18/pdf/01-12388.pdf.
Securities Exchange Act Release No. 76743 (Dec. 22, 2015), 80 Fed. Reg. 81948 (Dec. 31, 2015) ("Transfer Agent Release"). Available at www.sec.gov/rules/concept/2015/34-76743.pdf.
Securities Exchange Act of 1934, §17(A)(2), 15 U.S.C. §78q-1(a)(2).
Securities Exchange Act of 1934, § 17(f)(1), 15 U.S.C. §78q-(f)(1).
Securities and Exchange Commission Study on Investment Advisers and Broker-Dealers (Jan. 2011). Available at https://www.sec.gov/news/studies/2011/913studyfinal.pdf.
Securities Exchange Act. 15 U.S.C. § 78q-1(a)(1)(A)-(D) (2016).
See S. Rep. 94-75, 94th Cong., 1st Sess. 7 (1975) ("Senate Report").
Stein, K., 2015. Speech – Surfing the Wave: Technology, Innovation, and Competition – Remarks at Harvard Law School's Fidelity Guest Lecture Series. Available at https://www.sec.gov/news/speech/stein-2015-remarks-harvard-law-school.html.
White, M.J., 2016. Keynote Address at the SEC – Rock Center on Corporate Governance Silicon Valley Initiative. Available at www.sec.gov/news/speech/chair-white-silicon-valley-initiative-3-31-16.html.

Note

1. Bitcoins were purportedly developed in 2008 by an anonymous computer programmer known as "Satoshi Nakamoto."

CHAPTER 10

Global Financial Institutions 2.0[1]

Alyse Killeen, Rosanna Chan

Contents

10.1 Blockchain 214

10.2 Global Financial Institutions 217

10.3 Frameworks and Antecedents of Change 219

10.3.1 International Organizations: Core Components 220

10.3.2 Framework for Dynamic, Iterative Change of Global Financial Institutions 221

10.4 Blockchain and Global Financial Institutions 2.0 223

10.5 Needs That Change Post-Global Financial Institutions Blockchain Adoption 228

10.6 The Innovation Ahead 230

References 239

Notes 240

> *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.*
>
> ***Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Oct. 2008***

As Bitcoin and the concept of cryptocurrency become increasingly prominent in public discourse and the signs of disruption to traditional banking and financial institutions rapidly emerge, it is pragmatic to ask: How will Global Financial Institutions 2.0 persist? While old institutions may become obsolete, new mechanisms and institutions will likely arise. The advent of blockchain technology not only challenges the very definition and traditional operations of Global Financial Institutions, but also inevitably demands a reshaping of tomorrow's institutions.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00010-3
Copyright © 2018 Elsevier Inc. All rights reserved.

10.1 Blockchain

The Bitcoin blockchain and other public blockchains like it function as trust-not-needed infrastructure upon which people, entities, and devices may transact to exchange value and data. Because of the nature of the network infrastructure, one may transact on the blockchain with either familiar or unknown parties – again, people, entities, or devices – without concern for transaction validity or record. Just as the Internet catalyzed and now functions as the foundation for digital innovation, the blockchain has catalyzed and will function as the foundation for a fundamental rethinking and retooling of ledger and record management, and their dependent applications. The blockchain is the foundation for communication and transactional innovation, impacting the practice of verifying asset ownership and how people and entities sell and pay for things. New marketplaces will develop, completely new assets will be exchangeable and common assets will be transacted in novel ways, and new parties will emerge to transact, as access to the transactional economy will be very broadly democratized. Access to the economy is fundamentally and radically transformed.

By the fourth quarter of 2016, total global population Internet penetration had reached around 47%[2,3] with Internet growth projected to be approximately 9% annually, driven by emerging markets.[4] As the world continues to becomes increasingly more connected, blockchain technology will lay the foundation for people to transact and produce in new ways. "Although the world has been wired to connect and communicate, the infrastructure to broadly transact and transmit value has been limited. Bitcoin wires this connected global village to transact, and to share value."[5]

TEXT BOX 12.1:

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party." – Satoshi Nakamoto, Nov. 1, 2008, Saturday[6]

END BOX

Blockchain *def.* – A public and permissionless, immutable ledger managed by a peer-to-peer network. The blockchain allows the proof and transfer of ownership of digital currency without the verification of a trusted third party. It is an append-only database to which changes may be committed only by adding data according to the established rule set, and cryptographically verified by anyone. By means of the transaction of a blockchain's digital currency, the blockchain may be used to transfer data, records, and thus assets other than digital currency, and function as a settlement layer for other protocols. In proof-of-work blockchains such as the Bitcoin blockchain, the network's miners choose which transactions to include in time-stamped blocks and the order in which transactions are to be included. The network's

established rule set defines what record of ordered transactions (or data changes) is to be accepted as historically accurate.

Bitcoin *def.* – The unit of digital currency that is specific to, and may be transmitted by, the Bitcoin blockchain peer-to-peer network. In addition to its function as a currency, bitcoin enables blockchain technology by allowing the incentives of the parties to a transaction to align with the incentives of miners managing the network to record and order the transaction. Cryptographer Adam Back, the inventor of proof-of-work system, hashcash, and cofounder of Blockstream, explained the interdependent relationship of bitcoin and the blockchain, "Bitcoin is the tokenized representation of security in the blockchain, and the blockchain is a distributed data structure that provides security. If you take the currency out of [the blockchain], you collapse the incentive structure of [the blockchain] and you have nothing left."[7]

Note, within this chapter the term blockchain is used to reference both the Bitcoin blockchain peer-to-peer network infrastructure specifically, and to blockchains that are fundamentally similar to the Bitcoin blockchain in that they are public and permissionless, immutable ledgers, managed by a decentralized or distributed network of nodes.

Bitcoin blockchain establishes the ability to securely transact without the permission of intermediaries, and is valuable in contexts in which the distribution of influence is preferred or valuable against centralized influence.[8] Though digital currency is not a new phenomenon, the blockchain's ability to prevent the double-spend of digital currency without dependence upon a centralized ledger is new, and empowers a shift away from reliance on trusted financial institutions to intermediate transactions (e.g. JP Morgan Chase & Co., Bank of America, Wells Fargo, Citigroup), and to the distributed blockchain network as a transaction platform.

The transactional ledger of the Bitcoin blockchain is kept by a distributed network and is publicly available, rather than balanced and held privately by an institution. The distributed nature of the network, and the existence of long-tail mining node network participants, is important for the maintenance of the non-discriminatory inclusion of transactions and transactional participants.

During the Cold War, Paul Baran designed the first distributed relay node architecture to be a survivable communications system as a solution to the American military's reliance on the hub to spoke high frequency radio connections model that is so vulnerable to destruction by a physical attack, such as the nuclear attack threatened in the Cold War. Baran's new system allowed a network of end points to continue to communicate even if one end point within the network was damaged in a physical attack. The distributed network pictured in Fig. 10.1 in the rightmost of the three images found in Fig. 10.1 routes communication around damaged end points, where the hub and spoke system could have been rendered ineffective. Even after a portion of nodes is incapacitated, a distributed network is resilient and can continue to

www.elsevierdirect.com

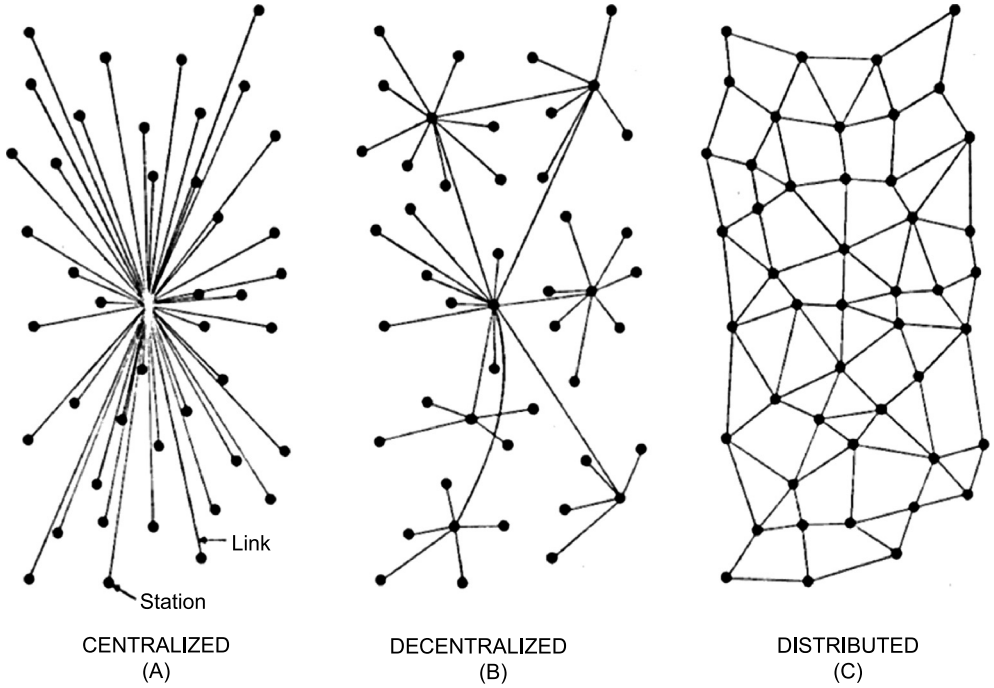


Figure 10.1: Centralized and distributed systems of data transmission[9] (from *On Distributed Communications Networks* (1964) by Paul Baran).

perform as designed and intended. This differs from centralized systems, which may be completely destroyed if a central node or hub is attacked.

The decentralized network pictured in Fig. 10.1 is a blend of the centralized network and Paul Baran's distributed network. This network, like the centralized network, may be destroyed by an attack that affects only a small number of nodes. The number of nodes that must be attacked in order to obliterate or materially alter the functionality of a decentralized network changes as the relative size of central hub nodes changes (as defined by the number of links to/from the hub). A decentralized network may be destroyed or rendered vulnerable by the attack of a single node if that single node links to a large enough share of the decentralized network's nodes.

The type of attack that can destroy a decentralized or centralized network goes far beyond physical attack to include network corruption, third party influence, taxation, co-option, and data siphoning. Exposure to a broad range of threat types emphasizes the importance of the Distributed Network. The Satoshi white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" does not use the term decentralization, and only uses the term distributed to describe the

www.elsevierdirect.com

Bitcoin blockchain network. The blockchain mining network is designed and referenced by Satoshi as a Distributed Network.

Today, financial institutions and other trusted third parties manage our critical ledgers, including sales and payment records, debt and credit records, land title records, mortgage records, medical records, records of identity, and more. When individuals and entities trust these institutions, implicit in that trust is the trust in the institution's ability to keep digital records. Ensuring that an institution's records may be trusted to be historically accurate, honest, and complete is a problem that blockchain technology can solve. Trust is a prerequisite for a functioning society, and in financial exchanges in particular, large institutions have been the purveyors of trust. The new use of cryptography and ledger transparency for transaction verification on the blockchain may come to redefine the concept of trust, and introduce new paradigms of trust that could put large, centralized organizations at a disadvantage.

Blockchain technology may be considered a type of "next-generation business process improvement software," says multinational professional services network, PricewaterhouseCoopers. When applied to institutional process improvement, blockchain ledger technology may be considered in two buckets: 1) open ledgers, such as the Bitcoin blockchain ledger, capable and designed to verify anonymous actors in the network, and 2) private ledgers, closed to unknown actors and designed to require actors in the network to be classifiable and identified. Blockchain technology removes inefficiencies from the financial institutions' administrative processes. In a period of rising complexities and costs, intense public and regulatory scrutiny, and an increasing quantity and diversity of demands, the opportunity for internal operational efficiencies couldn't have come at a better time.[10] Further, the blockchain may also be considered a collaborative technology, providing the ability to improve the business processes that occur between companies, and lowering the cost of trust.[11]

Global financial institutions have recognized and acknowledged both the power and institutional opportunity of Satoshi's innovation of blockchain ledger technology. "The blockchain is as much a mindset as it is a technology. Once it was possible to see a workable decentralized list-keeping platform in action – a tool and a methodology for building digital trust engines that could be used for a wide range of purposes – the cat was out of the bag."[12]

10.2 Global Financial Institutions

TEXT BOX 12.2:

"By shaping the ways in which individuals organize themselves and their economic transactions, institutions form the backbone of societies." – World Economic Form Report, 2015[13]

END BOX

Institution *def.* – An established organization or corporation (as a bank or university) especially of a public character, or, a custom, practice, or law that is accepted and used by many people.[14] A country's public institutional environment as characterized by the first definition is a critical factor in its level of productivity, prosperity, and the prosperity of its citizens, and is influential in shaping a country's technology and human capital profile.[15]

Global Institution *def.* – An established organization or corporation whose operations, client or service base, targeted goals, or outcomes are of multi-country interest.

Global Financial Institution *def.* – A global institution that deals with money (as a bank, savings and loan, credit union, etc.)[16] or monetary policy. Such an entity may establish formal and legally binding constraints along with enforcement processes for the transfer or value or data, or for the access of financial tools and processes. These institutions also have established informal constraints, such as behavioral norms, reputation or demographic-based gated access, self-defined codes of conduct, implied incentives of stakeholders, and language. Though this is true of institutions generally, the impact of formal and informal constraints becomes increasingly pronounced at scale.

Note, within this chapter our conceptual definition of the "global financial institutions" term is of financial institutions whose activity has broad multi-country consequence. This includes large commercial banks and investment banks, significant development banks, international financial institutions established by more than one country for cooperation in managing global finance networks (e.g. Bretton Woods Institutions), and large-scale investment firms such as Blackstone Group (BX) or KKR & Co. L.P. (NYSE: KKR).

Geopolitical, technological, economical, and social trends are driving the increasingly complex and growing number of national and international challenges that stretch beyond the current capabilities of traditional institutional governance, and are ill fit to the formal and informal constraints of our global institutions, and global financial institutions. Amidst these changing conditions, individuals are redefining their identities in measure against advancing technology and globalization and the resultant changing nature of their work and employment, socio-economic status, personal effects of long-term shifts in growth levels in the developed world, and other forces.[17] "The paradox is that at the very moment when we need to construct the building blocks of global governance, institutions like the European Union and the United Nations are under attack from the rising tide of populism and xenophobia."[18]

It is very clear to both the individual and institutions that serious challenges such as these demand a new kind and function of global institution. Though we cannot know for certain what the new contemporary and future-looking institutions will look like, we can extrapolate based upon our knowledge of the environment that they will operate in and the technology

available to meet these institutions' emerging and now existing, yet unmet, needs. To be sustainable (both relevant and competitive), institutions will need to be adaptable and agile, and able to respond quickly and securely to challenges and trends. Individuals will expect access and communication ability to other individuals and institutions, and where existing global financial institutions fail to offer this, nimble startups will rise to take their place. Finally, institutional brand is important; as the founder and executive chairman of the World Economic Forum, Klaus Schwab, said, "We know that institutions, to be effective, need to be trusted and impartial."[19] Blockchain technology will play a role in the reformation in kind and function of global financial institutions.

TEXT BOX 12.3:

"At Santander we work hard to ensure our banking is simple, personal and fair and believe new Blockchain technology will play a transformational role in the way we achieve our goals and better serve our customers, adding value by creating more choice and convenience." – Sigga Sigurdardottir, Chief Customer and Innovation Officer at Banco Santander (a global banking group with operations across Europe, Latin America, North America, and Asia, focused on retail banking), 2015

END BOX

Global institutions notably include International Organizations, which are inter-government organizations set up by member countries from around the world and characterized by inter-government cooperation and joint management of international goals. Some of the most prominent global institutions are those created after World War II: the United Nation (UN), and under Bretton Woods, the International Monetary Fund (IMF), and the International Bank for Reconstruction and Development (IBRD) that, along with International Development Association (IDA), became the World Bank. These were initially established with 53 countries of the Allied Forces, and now have membership countries from a majority of the world (the UN currently has 193 member countries). The overarching common goal for these institutions is to ensure international peace and stability and to prevent another world war.

10.3 Frameworks and Antecedents of Change

Today's International Organizations are fundamentally a reflection of necessary institutional responses to the global issues and conditions of the 20th century – a time that looks increasingly different from the 21st century and what the 21st century will continue to become. Whether 20th century International Organizations can adapt to meet 21st century issues is

www.elsevierdirect.com

still unknown. This same difficult question and uncertainty faces governments, banks, corporations, and universities. Global financial institutions broadly will need to address pressure to adapt to changes between the centuries and those that have developed during the 21st century.

Examination of the core components of global institutions through the lens of the 21st century empowers the re-imagination of Global Institutions 2.0, identifying what remains relevant, what is obsolete, and what is new. Though this section focuses on International Organizations, the proposed framework may also be relevant in part or whole to other types of global financial institutions.

10.3.1 International Organizations: Core Components

- Global Goals
- Participation
- Products and Services
- Operational Processes
- Measurement and Outcomes

(International Organizations, inter-government organizations set up by member countries from around the world, are also referred to here within as Global Institutions.)

Global Goals – The vision of Intergovernmental Organizations is to tackle challenges that require coordinated global efforts and broad adoption of goals and aims by stakeholders. Such challenges may include those of the environment, refugees, financial stability, connectivity, human rights, international trade, and disaster relief.

Participation – Membership of these Global Institutions must be multinational in order to best achieve interconnected global goals. As such, Global Institutions require the means to represent multiple viewpoints of their diverse and numerous member countries that themselves are composed of international citizens. Currently and through democratic processes, Global Institutions depend on governments to represent citizens; governments are now the main agent of implementation. The criticisms of this aggregation of diverse voices include concerns over the reliance on trickledown effect, and the difficulty that governments must not only understand their constituents but also act in their interests.

It is worthwhile to note, that while many private nonprofit organizations (e.g. Gates Foundation) and government institutions (e.g. USAID) may share similar global social goals, decisions in these organizations are made very differently, led by either private individuals or actors managing their national government interests. Differently from either approach, Intergovernmental Organizations are coalitions of many countries and require decision-making

from multiple countries made through each country's representatives, who aim to apply global interests to their decision making.

Products and Services – These could, for example, be global facilitation, neutral bi-partisan arbitration, crisis efforts, development loans, and other methods intended to meet the end objectives. The challenge is to connect impact on the ground on the micro scale, to global macro goals.

Internal Process and Governance – Global Institutions are governed by principles of neutrality, transparency, and governance. Like any public institution, there exists accountability and due process in institutional decision making and operations. Global Institutions have complex internal processes, as client country coverage and engagements span the globe, oversight and membership is multi country, and multiple donors exist. Much of the complexity comes from the need to cooperative involve many different stakeholders, functions, and levels of governance. Internal processes have complex webs of checks and balances, complicated hierarchies, and formal practices that date back to the time of the Second World War.

Measurement and Outcomes – Global Institutions must measure and track impact, and the achievement of goals. The challenge of international efforts is tracking impact on the ground around the world and aggregating it to assess global levels of performance. The difficulty is not simply in data collection and the harmonization of measurements across the globe, but also in identifying the attribution of engagement by global institutions to the resulting impact. Though goals are at a global level, interactions that contribute to outcomes can come from multiple sources at local, national, and global levels. Major advances in data collection, along with global adoption of mobile phones and smart devices, should allow Global Institutions to advance in solving the challenge of tracking impact and progress of global goals.

10.3.2 Framework for Dynamic, Iterative Change of Global Financial Institutions

The previous section lays out some of the core components of Global Institutions to help guide a re-articulation of Global Institutions 2.0. Though discussed through the lens of Intergovernmental Organizations, lessons may be applied in part or whole to other types of global financial institutions. For today's global financial institutions, it is critical to be adaptive and flexible in order to keep up with rapid change, though, at the same time, this flexibility must be balanced with the qualities of stability and consistency rightfully expected of a global institution.

Institutions are born out of the opportunity or necessity to solve a given set of needs. If the needs that justified the institution's solutions disappear, the institution may become obsolete. Similarly, there will arise opportunities and necessities for new solutions to cater to new

www.elsevierdirect.com

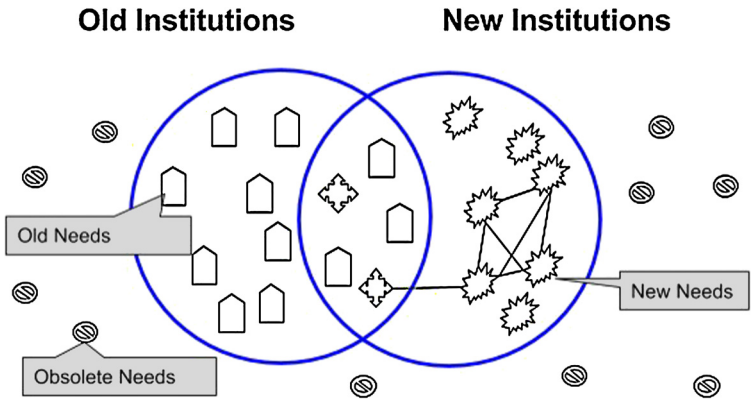


Figure 10.2: The dynamics of an evolving ecosystem and the transition from old institutions to new as once critical needs be obsolete or of less significance and as new needs rise to prominence (by author Dr. Rosanna Chan).

needs, and this will give rise to new institutions or new opportunities for existing institutions. Within this dynamic, Global Institutions 2.0 will be required to be continually examining the global needs of their clients or of the populations the serve (and/or of their future clients, and future populations they could serve), and continually examining the solutions used to address them.

The Venn diagram in Fig. 10.2 depicts the evolving ecosystem of old and new institutions. The circles represent the set of needs relevant and irrelevant to "Old Institutions" and "New Institutions." Here, old and new refer not only to the age of institutions, but represent the differences in approach, technology, and organizational structure of these institutions. The elements within the Venn circles represent "Remaining Needs," "New Needs," and "Obsolete Needs." At any particular time, institutions can fall under four different categories: 1) Old Institutions that cater exclusively to outdated needs, 2) Old Institutions that cater to old as well as new or current needs through the utilization of old (traditional) methods; these are traditional institutions that have adapted, 3) New Institutions that are able to address old needs, or both old needs and new needs, using new methods, and 4) New Institutions that address only new needs. Global Financial Institutions 2.0 are the Old Institutions that have adapted or New Institutions that address old or new global needs, using new or old, but still relevant, approaches, including new technology and methods. There also exists a subset of institutions that combine both old and new institutional processes to address both old and new needs.

As new tools and technologies become available, some needs may become obsolete while other needs may newly emerge. Institutional design that iteratively adapts to the changes in needs and the availability of new tools is essential for institutional sustainability. Global Financial Institutions 2.0 must embed this cycle of institutional adaptation into their internal

processes and governance; dynamic iteration aimed at incorporating cultural shifts and technology innovation must be part of the institution's vision and goals. Institutions must always continue to change.

TEXT BOX 12.4 Dynamic, Iterative Global Institutional Change: Best Practices in Internal Institutional Review

- A continuous iterative process that is crucial during times of rapid change: re-examination of institutions to ensure relevance, and evolution to defend against obsolescence.
- Adaptability and openness to changes in the environment and as a result to technology innovation, while also examining what remains.
- A simple framework used as a starting point to structure discussion:
  - Identify what needs are irrelevant, remain, and are created.
  - Consider how Global Institutions 2.0 may need to evolve.
  - Examine the relevant factors that contribute to redefining institutions 2.0 and potential constraints.

END BOX

10.4 Blockchain and Global Financial Institutions 2.0

TEXT BOX 12.5:

"We see three trends [in institutional blockchain adoption] we believe will be important: incumbents focus on protecting their intellectual property as they explore new collaborative opportunities with customers, suppliers, and competitors; large financial institutions will need strategic plans to set parameters for technology risk taking; and market participants will start to develop the processes that surround the transactional layer." – PwC, What's next for blockchain in 2016?, 2016[20]

END BOX

The Bitcoin blockchain provides global financial institutions and all others with a universal and trustworthy ledger that may be used as 1) a transactional ledger and payments network, 2) a technical infrastructure to develop new applications upon, or 3) a template to copy for the development of private blockchains. With the use of blockchain technology in these manners, in addition to new broader payment capabilities, secure identity authentication is introduced, inter-institutional cooperative ledgers become possible, non-counterfeitable digital cash may be utilized, and the opportunity for programmable securities is unveiled. The incredible power of Satoshi's innovation is that each of these blockchain-reliant capabilities independently has

www.elsevierdirect.com

the power to transform global financial institutions and world economies. Understanding the external opportunities now available, the internal possibilities for efficiency and change, and the competitive inter-institutional dynamic that could be triggered, institutions quickly began to learn about the Bitcoin blockchain. As PricewaterhouseCoopers stated above, in investigating the integration and use of blockchain technology, institutions are concerned with the associated technical risk, the development of new processes, and the protection of what is developed. Concern is weighed against the technology's potential to positively change the operating and process conditions of global financial institutions.

"We are also fully aware of the blockchain's potential to disrupt many of our existing business models. On the other hand, it is no secret that the banking industry is facing a number of very difficult challenges. It would be irresponsible of us to ignore a technology that, on the face of it, offers the chance for such significant cost reductions and efficiency gains. That this technology is likely to enable significantly improved and potentially radically changed business models makes it all the more interesting for us." – UBS Group Technology White Paper, 2016[21]

Blockchain technology of both a public and private nature provides value to global financial institutions. Public blockchains include the Bitcoin blockchain and Ethereum blockchain, and are accessible to anyone with a computer and Internet access; public blockchains provide a permissionless ledger and transaction network, and are therefore highly censorship-resistant (and censorship-proof in their perfect form). Private blockchains are defined by permissioned or credentialed user accesses for read and/or write functions; access to private blockchains is restricted. In 2015 and 2016 financial institutions began to roll out their own, proprietary and private blockchains. On the public blockchain, there is one list of transactions that everyone shares. As the ledger runs on an open network and is managed by verifiable consensus mechanisms, everyone can be sure of its validity; it may be monitored and checked for accuracy in real time. There are also multiple other benefits of a public, permissionless blockchain for global financial institutions. For instance, it is much simpler to deal with one ledger than to reconcile many, and with this simplicity come cost and operational efficiencies. When cooperative parties share one ledger and transactional network, they must agree beforehand – and remain in agreement – on how data should be structured, transferred, and stored. Best practices are collaboratively defined and employed: A shared blockchain has the advantage of intrinsic standardization and interoperability,[22] and a public blockchain is the ultimate shared blockchain.

Yet the benefit of a permissionless and transparent ledger may be premature for today's global institutions. Blockchain company CEO, Micah Winkelspecht of Gem said, "Quite frankly, financial institutions don't have the need for a censorship-resistant blockchain. They do have a need for speed, and custom assets that they can represent."[23] Beyond anti-censorship though,

the blockchain offers much more including that which is immediately relevant and appealing to financial institutions.

Settlement is one such problem – a very costly one – which financial institutions are eager to address. The blockchain enables the near real-time settlement of most types of financial transactions, which has the effect of eliminating a transaction's counterparty risk, freeing up capital, and reducing transaction cost. Because blockchain technology can make transactions irrevocable, trade data is more accurate and settlement risk is comprehensively reduced.[24] Without the blockchain, capital allocated for a transaction is not available for use until that transaction settles, so capital is tied up. The risk that exists in the interim period between creation of a transaction and settlement may require collateral to be secured at a central bank to insure against it; again, capital is tied up. Distributed ledger technology provides an efficient alternative.

Other institutional benefits of blockchain technology are reaped as a result of the decentralized computing model of the blockchain network, and are strengthened as the network is increasingly more distributed on the spectrum of centralized to distributed (see Fig. 10.1). A distributed network of transaction is more robust and secure against most threats than are the centralized models traditionally used; it is a safer, more reliable, and much less expensive transaction and ledger system. In a catastrophic event, unless every single computer on the network is destroyed, there will remain at least one node with the latest copy of the ledger that can carry forward with the ledger's processing. Additionally, because the blockchain uses cryptography to establish the viability of the ledger and because there is a nominal cost to send a transaction, the network is more resilient to cyber-attack including direct Distributed Denial of Service (DDoS) attacks than are other payment and ledger systems. That cost of cybersecurity and business continuity management is reduced. (Note that as the network is reliant on the Internet, attacks on Internet infrastructure may impact blockchain networks.)

Decentralized computing does not just reduce operational costs for institutions and prevent security failings, but also has the potential to reduce the requirements and costs for the resolution planning necessary in case of an institutional failure. For example, after global financial services firm Lehman Brothers collapsed in 2008, it took years to disentangle open trades and understand where assets were located. Had trades been transacted upon a blockchain network no open trades would have existed, and a history of transactions and asset locations would exist.

An entirely new blockchain-based market fabric will connect institutions, individuals, assets, and other entities or tools that exist in the now complex labyrinth of intra-entity systems, vendor systems, market wide systems, and so on, that global financial institutions depend upon. In addition to the changing fundamental conditions of transactional ledger immutability and transparency, settlement speed and efficiency, and network security of this new market fabric,

www.elsevierdirect.com

global financial institutions will also be transformed by the evolving needs of the population they address and serve. Just as the blockchain network fundamentally changes institutions, so too will it change the needs of the populations served. For instance – and of risk to financial institutions – individuals are empowered by the disintermediation of trusted third parties for transactional security and access to financial tools available on the blockchain, and with that may come new paradigms which put global, centralized organizations at a disadvantage.

There are similarities between global institutions and public blockchains. Just as many important global institutions were created in response to the global crisis after the Second World War, in much the same way, the creation of bitcoin was a response to the global financial crisis and developing catastrophic erosion of public trust for financial intermediaries. Additionally, the development of blockchain protocol has been instilled with similar ideals on acting at a global level to the betterment of human good.

Blockchain technology was heralded as a "Trust Machine" by The Economist (Oct 31, 2015). It is indeed apt that in these times of growing distrust, people would rather trust code than other people or institutions. To give context to the enormity of this function of a public, immutable ledger such as that of the Bitcoin blockchain, consider the role that record keeping has played in human evolution since the beginning of when written word was introduced. From Gregorian chants, to recording of scientific discoveries, to the establishment of laws and institutions, to providing accounts and evidence, and to draft agreements and contracts, record has played a role. Records are fundamentally important to society (see also Ajinkya, B., et al. 2006).

The digital age introduced major challenges to core economic principles. First, with the digital age, information-based goods have become exchangeable assets. Information goods are goods that are built on intellectual property, or information such as music, software, academic journals, and movies. Today, value is embedded in digital information. While technology has enabled information goods to be easily and nearly costlessly recorded, produced, reproduced, and disseminated, this fundamentally disrupts basic economic tenets. The efficiency of the market system relies on three fundamental axioms governing goods: excludability, rivalry, and transparency. Digital technology challenges the very tenets upon which markets are constructed and function. (See Kahin & Varian 2000.)

Excludability breaks down because with digital information goods it is difficult to exclude others from using the same information. It is difficult to stop those who have not paid for the good from using the digital asset belonging to the producer. Rivalry is a characteristic of goods where consumption by one consumer prevents simultaneous consumption by other consumers. Information goods are non-rivalrous as they are often characterized by very low to negligible marginal costs of production such that two consumers can enjoy it almost as

cheaply as one. Digital goods are considered relatively complex, often consisting of unobservable components. The economic axiom transparency declines as this creates difficulties in identifying the good and in formulating consumer valuation of a digital good. When these axioms break down, the pricing and market clearing functions of the invisible hand fails.

Blockchain is revolutionary as it restores economic value to digital goods or assets through restoring excludability, rivalry and transparency, and, as such, fulfills the missing piece that is needed for the digital economy to fully function. By restoring excludability, rivalry, and transparency to informational goods, blockchain allows economic value to be attributed to digital goods and thereby creating assets that can be valued by market functions.

It is difficult to appreciate how seminal and historical an innovation blockchain technology is, in part because it is now hard to recognize the fundamental weaknesses of today's digital economy. The early 21st century saw the emergence of rapid growth in participation and use of the Internet without question of the value of information that is shared or transmitted to third parties. Many people today rely on Uber, Facebook, Google, and Gmail on a daily basis, and as Tapscott & Tapscott (2016) rightly point out, current interactions with digital platforms require enormous leaps of faith in third parties, "Because the infrastructure lacks the much-needed security, we often have little choice but to treat the middlemen as if they were deities." Perhaps, it is hard to recognize a revolutionary solution when the inherent fundamental problem is not so evident.

Blockchain has the capability to instill trust in the digital age and to create viable digital assets. With the growing distrust of institutions and people in positions of power, the emergence of blockchain could enable people to trust instead in code. The ability to finally create immutable digital goods is a major inflection point in human history and a significant advancement. While on one hand, the technology has been described as "trusted transactions directly between two or more parties, authenticated by mass collaboration and powered by collective self-interests, rather than by large corporations motivated by profit" (Tapscott & Tapscott, 2016), self-interests are also motivated by profit; the irony is that code is written by people.

The challenge, which Satoshi was able to resolve in his innovative design, was the incentive structure or payoff matrix that incentivized self-interests toward a collective good. This is no small feat and required astute mechanism design. Even on the blockchain, the recent massive attack on Ethereum DAO in 2016 is an example that the code people trust is written by people, and people are fallible. The technology allows us better tools, and yet ultimately it's people that create and use these tools. Human fallacy, and immoral intent exists, whether in coders or hackers, whether at investment banks, government, or elsewhere. Programmers are not necessarily more benevolent than anyone else.

www.elsevierdirect.com

10.5 Needs That Change Post-Global Financial Institutions Blockchain Adoption

"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. . . . What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." – Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Oct 2008

Global financial institutions such as large banks and brokerages have long held the position of the trusted third party, validating the authenticity of transactions and managing the transactional ledger. The introduction and eventual broad penetration of blockchain technology significantly alters the population's need for these institutions to continue to be trusted third-party middleman. The value proposition of global financial institutions to the population and enterprises changes with the adoption of the blockchain. Individuals and enterprises do not need to rely on institutions to gain access commerce, the markets, or financial tools. With permissionless access to the blockchain, the institution's role changes.

But how will individuals and enterprises access the blockchain? It is likely that what is today known as a wallet and is used by early bitcoin and cryptocurrency adopters to store digital currency, will develop to become a user's connection to the blockchain and financial systems. Having a smart wallet will be much like having a bank in your pocket (perfect for U.S. millennials, 71% who would rather go to the dentist than listen to their bank[25]). Your smart wallet will be used to manage your accounts, to configure and carry out your transactions, to manage your preferences and identity, to communicate with the institutions and individuals you choose to work with, and to purchase new tools, information, or other capabilities that might become available and desirable.

Not only will individuals use wallets in this way, but so too may enterprises. This may seem like the current digital banking system, but in reality it has the potential to be much more. In this new paradigm, not only do the needs traditionally served by financial institutions change, but the needs addressed and expressed by global financial institutions change as well. As blockchain infrastructure and the global financial system, including financial tools, can be accessed without the facilitation of an institutional intermediary, the entire ecosystem changes. Some traditional needs will be mad obsolete, other traditional needs will be addressed in new ways, and a smaller group may remain completely unchanged. At the same time, new needs will emerge. Potential and limitations of individuals and institutions will be redistributed.

In this new future, capital markets will be more direct, financial products may act as their own accountants, points-of-sale may automatically send sales tax to the state, individuals will have greater control of their personal data and personal data sharing, and so on; entire sets of institutional processes that now create friction while providing trustworthy data or connectivity will be superseded. Yet within these new modes institutions could still serve a role. Credentials and reputation will still be important and necessary, depending on the conditions of a transaction or other situation, and institutions may step in as providers of credentials or reputation. Further, there may also still be in a role of identity verification. In the blockchain and smart wallet world, your private key becomes extremely valuable as it confirms your identity and permits access to your resources and data. If a private key is stolen, a malicious actor could do significant harm. Financial institutions could provide credentialing and verification, reputation, and safe guardianship of private keys, and thereby of identities. Start-ups and open-source-focused developers will be working to assure this doesn't happen, and it may be for the best that identity, credentials, and reputation are managed by trusted technology rather than trusted institutions.

Tim May's seminal 1992 document *The Crypto-Anarchist Manifesto* states: "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity of the other. . . . Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation. The technology for this revolution – and it surely will be both a social and economic revolution – has existed in theory for the past decade." The Bitcoin blockchain is the innovation of Satoshi Nakamoto, a pseudonymous actor or group of actors, and emergent from the activity and previous innovations of the Cypherpunks (a small group of engineers connected by a mailing list for the discussion of cryptography and its effect on society).

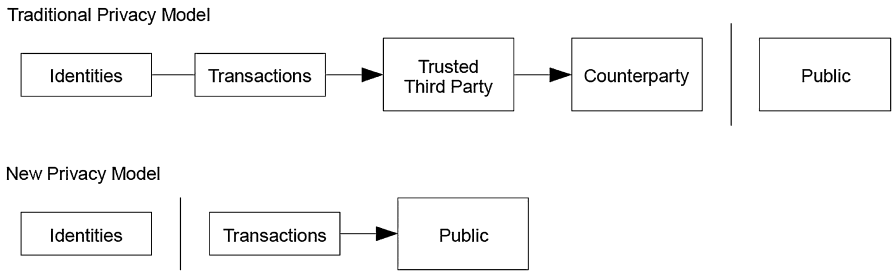


Figure 10.3: The Bitcoin blockchain's privacy and identity dynamic[26] (from *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) by Satoshi Nakamoto).

www.elsevierdirect.com

It is clear that Cypherpunks had been building on one another's work for decades.[27] Reusable proof of work (RPOW) was introduce by Hal Finney in 2004, and was built upon Adam Back's Hashcash. Hashcash was developed in 1997, and used to protect against DDOS attacks and later as the mining function in bitcoin.[28] Nick Szabo built upon Finney's RPOW and introduced bit gold, a digital unit of value. Then when Satoshi introduced bitcoin and the Bitcoin blockchain, Satoshi cited both Adam Back's hashcash and Wei Dais' b-money, the later that was announced on the cypherpunks mailing list in 1998.[29] It is important that global financial institutions note and remain prepared for the innovation that will be built upon Satoshi's innovation (see Fig. 10.4). We've seen the beginning of this new, powerful, entrepreneurial work, but are still early down the path of what will now be developed because the Bitcoin blockchain exists. This future innovation will continue the revolution that Satoshi introduced, further changing the needs and values that drive global financial institutions.

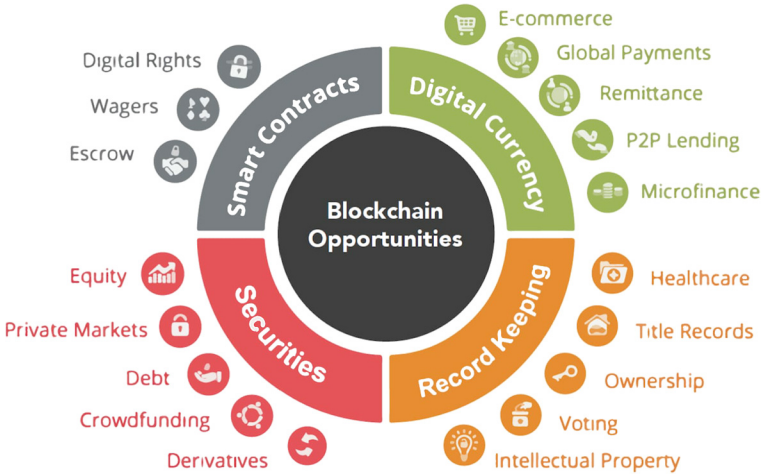


Figure 10.4: The areas of opportunity for blockchain-led innovation (from *Factom Investor Deck 2016* by Peter Kirby).

10.6 The Innovation Ahead

TEXT BOX 12.6:

"We have begun to see a clear outline of what a blockchain-enabled financial system might look like. We and our peers are not so much interested in cryptocurrencies as we are in these other possibilities." UBS Group Technology White Paper, 2016[30]

END BOX

The UBS Group Technology authors go on to acknowledge, as the blockchain community has long purported, "The blockchain can be used to provide the basic services that are essential to any financial system, and can do so in ways that are often better and more efficient than the tools we use now." Satoshi's innovation in its entirety is of transformational value to global financial institutions; the secure identity authentication, the blockchain technology infrastructure, the bitcoin currency, and the opportunity for programmable securities, all have the power to revolutionize the world's most important financial institutions.

At a high level, while identity authentication has long been purview of the institutions, the blockchain provides non-replicable, cryptographically secured identity and pseudonymous identity that can be managed by the individual (see Fig. 10.3). Further, while the ledger of transactions and ownership has been the purview of institutions, each managing their own proprietary ledger(s) in their own databases, blockchain technology provides a single decentralized record of transactions managed by a network of miners. This technology allows for the distribution and transaction of a non-fiat digital currency in a cash-like manner, while most other forms of currency are the purview of governments and institutions. Lastly, while simple and complex securities have been the art and demise of global financial institutions, the programming capability of blockchains allows for the development of "smart contracts" and programmable money; agreements may be self-enforcing. From these shifts in manners of influence, institutions are able to become better, more efficient record keepers by leveraging blockchain technology, and cost is reduced across the financial ecosystem. Efficiencies and cost reductions that occur within an institution may accelerate broad adoption by driving competition, or by presenting the threat of it. The simplification of the outdated practices of identification verification, ledger management, transaction, and contract, benefits institutions and those they service.

> *The path forward for sustained blockchain adoption and application is still uncertain, but the opportunities are endless. Prospective areas of adoption and application development:*

Identity and Credentials – The Bitcoin blockchain was designed to empower a user's management of their own identity. It also allows users to safely transact with others whose true identities are unknown. However, elements of a user's broader identity may be necessary in certain transactions. For instance, a seller may want to assure that a buyer is of legal age, or a buyer may want to assure that a seller is of a certain authority, like a licensed medical practitioner. With credentialed pseudonyms based on public-key cryptography, and the ability to transmit information on the blockchain along with an exchange of currency, identity could be private even while credentials or identity features are shared. People and institutions could

www.elsevierdirect.com

share parts of their identities in different contexts. For institutions, this could have the effect of creating efficiencies in services or the provision of resources and tools to a broader population. It also may allow global financial institutions to address and track groups of people that do not have government issued identity.

Asset Credentials – Because blockchain technology is excellent at publishing and maintaining a permanent record of data, it also may be used to manage asset identity and credentials. The challenge of this, along with any other form of data management on or off the blockchain is the "garbage in, garbage out" problem. The solution to all garbage in, garbage out problems is a well-documented process. For instance, a newly unearthed artifact from the Incan Empire discovered in Cusco, Peru by a credentialed archeologist (where credentialed may be defined as the achievement of a doctorate degree from a separately credentialed university, credentialed for relative excellence amongst all other universities in the field) would be registered to the blockchain according to a repeatable process, and leveraging the time stamping mechanism of the blockchain. (Note that each block of transactions processed on the network contains a time stamp.) At time of discovery, the team could photograph the object and commit the image and details of discovery to the blockchain, later a secondary archeologist could confirm object details on the blockchain, and as the object moved geographically or across guardians, each transition would be recorded and time stamped on the blockchain.

The identification and trading of assets of all sorts can be managed similarly, though this process could be of particular importance for high value assets where authentication and the record of ownership are critical. This is a more secure and reliable means of identifying assets, and allows trust in the provenance and authenticity of the items. With this, direct markets of high-value assets open. "As with the currency, transfer of assets is easy, immediate and final, with a traceable, auditable record of ownership going back to when the asset was first added to the chain."[31] For global financial institutions, this could have the impact of de-risking trade and supplying chain processes, amongst many other areas where asset identity and provenance are key.

Autonomous Financial Instruments – Smart contract technology will enable the creation of new, autonomous financial instruments. Financial instruments are assets that can be traded to provide an efficient flow and transfer of capital based on a set of established and understood conditions. The assets transferred may be cash, a contractual right to deliver or receive cash, a contractual right to the exchange of another type of financial instrument, or evidence of one's ownership of an asset.[32] Within the new and emerging field of autonomous financial instruments, smart securities are a subcategory. Securities are financial instruments that represent an ownership position in a stock, bond, or option. Smart securities would issue and administer themselves, and in the process, significantly reduce the costs of and create efficiencies of accessing capital markets. The cost of securities' custody, servicing, and reporting would

also be reduced.[33] In this new paradigm of stocks and bonds administering themselves, the security pays its own dividends and coupons, completes its own transfer of ownership, and reports changes in its market value and expected future value in real time. A derivative is a type of security that derives its value from underlying assets; a derivative contract is an agreement between parties that is based upon the performance of the underlying asset. Smart derivative financial instruments will automatically pay out when certain events happen in a market or specified conditions are met. With traditional "dumb" derivatives, banks hold the record of derivative contracts and execute upon their stipulations when conditions trigger payment or other contracted actions. This responsibility will be managed by the blockchain by adding programming capabilities to the blockchain ledger. Smart Securities are discussed further below.

Smart Securities – Securities empower corporations to raise capital through the issuance of stocks, bonds, and other related instruments. Similarly, government entities issue bond securities. These securities play a now indispensable role in the health of public and private institutions, and innovation in this area, though the application of blockchain technology will be powerful to the economy comprehensively. Today, the operation of issuing and servicing securities is complicated and inefficient. The accounting and legal fees of issuing and servicing a security, along with the registration costs and underwriting fees of a security, are an inefficiency that burdens the institutional or governmental Issuer, and the Owner. Once developed and adopted, smart securities will offer cost efficiency as well as efficiency of timeliness, trust, and communication. This exists in the code. Stocks, bonds, and other instruments that exist on the blockchain are self-administering. They require no custodian. The straightforward impact of the blockchain on securities is the reduction of costs of capital market access and of security custody, servicing, and reporting. It would also offer new possibilities. Smart securities may be customized to the profile of individual investors and institutional investors. Notably, smart securities and their associated efficiencies make it easier for smaller entities to issue equity and debt.

Escrow – Another form of autonomous financial instrument is the smart escrow contract, where funds are transferred only upon the condition that goods are delivered or services are confirmed rendered as stated in the contract, and then the funds are transferred immediately. Confirmation may be human or machine, and will likely often leverage the increasingly ubiquitous Internet of Things (IoT). Smart contracts and escrow will greatly simplify delivery versus payment. IoT is discussed further below.

Volatility Evasion – Global financial institutions can leverage programmable currency to solve for the inefficiencies and risks now inherent in the contemporary financial system, such as volatility risk. Foreign exchange risk, for instance, is a consequence of currency volatility and has the effect of increasing interest rate risk, transactional risk, leverage risk, and more.

www.elsevierdirect.com

With bitcoin and other programmable currencies, banks and other financial institutions may develop specialized currencies that mitigate the volatility risk in a transaction. This would be particularly valuable in the transaction of high value assets, where the time between the contract negotiation of a sale and the transfer of title leaves both parties exposed to currency movements (though smart contracts may also impact the time between sale and title transfer). Private and/or proprietary smart currencies may provide financial institutions and their clients greater stability and predictability in exchange.

Regulatory Compliance – Smart, programmable currencies, contracts, and private blockchains may allow for compliance rules to be incorporated directly into the currency, contract, or blockchain itself. This could permit regulators a real-time view of system activity, and move regulators into a role of active prevention. While this potentially makes for a safer financial system, the risk of abuse, including the loss of privacy and individual autonomy, is also clear. In the pursuit of safe financial systems (or otherwise), regulatory rules can be programmed into financial products, making the system and products automatically compliant. Traditionally, it is the banks' and financial institutions' responsibility to comply with regulatory rules, which is an expensive and time intensive obligation; institutional savings from automated compliance could be highly significant.

Notably, similar regulation-intelligent systems could be used to check transactions against lists of any sort, including sanctions lists, and block transactions and communications. This may result in a loss of critical fungibility of a digital currency, and create an ask-your-banks-for-permission-to-pay culture, a term noted by Brett Scott in The War on Cash. Ask-your-banks-for-permission-to-pay is antithetical to the Satoshi vision and innovation of blockchain technology, and replicates or amplifies inefficiencies that exist in the traditional system.

Internet of Things – The Internet of Things is the network of connected autonomous devices, and is the connection of the Internet to the physical world through ubiquitous sensors. The number of objects able to record and transmit data is steadily rising, and 50 billion things are projected to be linked to the Internet by 2020. This network of connected objects creates continuous streams of data that are applicable to a broad array of business practices. Blockchain technology and cryptocurrency allow this data to be monetized, and empower these connected devices to transact or share data relevant to smart contract-based transactions.

The IoT could have many valuable applications including asset financing, for instance. Asset financing may be based on parameters such as distance driven, or the weight of a load carried, rather than being based on the period of time for which the asset is leased, which has been easier to measure. Once sensors can transmit trustable data to communicate these new variables (distance and weight), asset financing can be made more precise and thus efficient.

Risk management and pricing may be made similarly efficient. Collateral management is a used for risk management, and better data on the quality, condition, location, and movement

(or lack thereof) of collateral provides more accurate assessment and pricing of risk. Other uses of blockchain-linked IoT include understanding customer needs. Through transparency into a business' operations, the business' bank could understand its customer's needs and proactively identify additional growth financing requirements, for example, by exposing when machinery is working at full capacity or when inventory turnover exceeds historical rates. Opportunities at the intersection of IoT and the blockchain are endless.

Global Goal Setting in International Organizations – Global goal setting could be disrupted by blockchain in that the agenda need not be set by global institutions (and the representation by member governments) but by wider participation. There can be benefits in bringing additional multidimensionality to global goal setting by greater inclusion from a wider set of participants, such as from intended beneficiaries, or organizations who need to implement the programs. While currently international organizations do solicit inputs across multiple stakeholders from all areas to draft global goals (Tallberg et al., 2016), blockchain has the potential to not only open the process to a greater global participation on a massive scale, but also effectively aggregate inputs in an efficient manner. Even though the technology may not necessarily take away the need for discussion and debate, utilization of blockchain could essentially mean that global agenda need no longer remain behind closed doors with select number of participants. Rather, it can allow greater participation at global micro levels as well as allow more efficient means to come to global agreements.

Participation in International Organizations – The participation in organizations will be disrupted by blockchain in that the technology fundamentally challenges the boundaries of organizations. Participation need not be exclusive to traditional roles of bankers, government bureaucrats, investment bankers, but given the scalability of mass participation, blockchain can democratize participation in global organizations like never before. Hypothetically, participation in Global Financial Institutions 2.0 could be someone who is living in a slum South Asia, or a doctor fighting Ebola in West Africa, or a Ph.D. student in Eastern Europe who happens to be specializing in migration, or a mother in East Asia sending her kid to school for the first time. Imagine a Global Institution 2.0 where dynamic global teams that draw from the complete spectrum of perspectives and knowledge that the entire world can offer, to formulate global goals, to make global good decisions and to tackle global challenges. Blockchain challenges the boundaries of Global Institutions as it can allow formal and official input by anybody in the world. Depending on topic, issue, challenge or decision, or the level of perspective needed, the set of participants in Global Institutions 2.0 could essentially be any global citizen. Blockchain won't merely function as an agglomerate of voices, but would allow inputs by different participants to also be paid, be held accountable, and verified by other global citizens. Furthermore, Blockchain can increase transparency and thus actors are kept in check by permanent record of actions and decision, thus held accountable by the global community. Experts could be evaluated or vouched by peers with expertise in the same area or

www.elsevierdirect.com

field to ensure that participants have the adequate knowledge. Teams and groups balanced by differing views, from micro- to macro viewpoints.

With greater diffusion of participants, Global Institutions 2.0 may look less like an organization with clear boundaries between those within and those outside the institution, but more like a global network made up of different global citizens who can participate.

Products and International Organizations – The means to achieving global objectives could be fundamentally disrupted by blockchain and will produce new products and services. Blockchain has wide applicability to development projects and efforts around the world, including relevance to many of the United Nation's Sustainable Development Goals: blockchain developments in E-commerce (such as Open Bazaar) and global payments have direct applicability to the global goals for economic growth; blockchain applications to equity, debt, crowdfunding will facilitate global goals for industry and innovation; healthcare blockchain applications have direct link to the global goals for universal health; blockchain and identification can have huge impact on goal of universal identification; blockchain disruptions to microfinance and P2P lending can facilitate greater access to finance and banking the underserved; and lastly, tile records, ownership, contract management, and land titling on the blockchain can facilitate justice, jobs, and economic growth overall (https://sustainabledevelopment.un.org/sdgs).

These are only a small number of examples of the broad spectrum of opportunities for blockchain applications in the developing world being massive (see also Schiller, B., 2016 March). The technology would have the greatest delta and impact among developing countries, as many face issues of conflict, corruption, weak institutions, political distortions or simply very outdated practices. To provide context, many systems in the developing world have not been digitalized – even not basic public services. Therefore, the opportunity to leapfrog from 20th century digital to 21st century blockchain networks with the means to strengthen transparency, inclusion and greater access to key goods and services could be the tool that the global community can leverage to fulfill global goals and, in particular, the Sustainable Development Goals.

Fundamentally blockchain can affect products of global institutions in three ways: 1) replacing old products with new blockchain based products, i.e. voter registration, government records, identification, etc., 2) creating new products that circumvent old processes – such as digital wallets, smart contracts in procurement and implementation, or a universal id, and 3) directly transferring assets, either goods or payments, to beneficiaries rather than through an intermediary, such as aid, social benefits, educational credits, health, etc. That is, there is a possibility to overcome the challenge of the arm's-length intervention through many layers of intermediaries, and creating a more direct linkage between macro goals with interventions at the micro level.

i) *Replacing old product with blockchain-based product* – The most direct application of blockchain to replace existing old products would be ledger/record based type goods. Registrations, licenses, permits, and certification – basically potentially anything that entailed people to produce a piece of paper verified by some third party. While records still need to be maintained by institutions or organizations – the ability to safely record information and for it to be accessible anywhere would make a huge difference to many billions in poverty and most vulnerable. The reliance on paper records, or records kept by government agencies is prone to be destroyed, or lost – particularly for those in conflict and fragile states, migrant populations or refugees (Poast and Urpelainen, 2013). Currently, Bitfury and Government of Georgia are piloting land titling on blockchain – the success of which could provide an empirical data point to support the hypothesized potential for blockchain uses for records.

Likewise, financial securities that rely on digital ledgers, existing markets can also be replaced by blockchain such as stock exchanges, carbon credit trading, equities markets, and insurance.

ii) *Creation of new products that circumvent old processes* – Blockchain has the potential to give birth to new products because it allows a trusted network of interactions between multiple stakeholders. That is, rather than the need for each country to build their own systems, develop their own security firewalls, and then ponder and negotiate integration and interoperability between countries, blockchain protocol can ensure trust and security across countries. This paves the way for countries to harmonize many areas, such as trade and logistics, identification, payments and remittances, visas and passports, and markets, even global stock exchange.

The inter-operability across countries that blockchain technology facilitates implies that individuals can theoretically access global markets like never before – and not just access, but also create markets like never before. Rather than markets being segmented along countries, blockchain can allow for global markets to operate much more cohesively. For example, companies can issue their own stocks without needing to go through an exchange (i.e. Overstock), or individuals can create information goods to sell directly to consumers such as music, art, books or sports card without needing to go through a publisher, or recording company. Greater scale economies would be possible as producers can sell to anybody in the world. The possibilities are only limited by what digital goods and assets can be created, and traded with a level of trust and security – from anywhere in the world. This could be enormous in terms of opportunities to earn livelihoods for billions of people in developing countries.

New products would also include products such as smart contracts that automate simple actions or transfers.

iii) *Direct transfers* – Global institutions operate through intermediaries and implementing agencies as the means to achieve global objectives. Blockchain can facilitate the means to

www.elsevierdirect.com

distribute aid or disburse benefits to the people who need it directly. This does not necessarily imply that interventions will bypass national institutions; it actually means that the channel can operate with smart contracts and escrows that allows all layers of approvals to be done effectively, transparently and with full accountability. In other words, the linkage from global to national level, to citizen level can be much closer tied, with the transparency of being able to track impact on the ground much more effectively.

The challenges that remain in terms of product development in international organizations are that while the technology has enormous potential to improve trust and security in the digital age, major constraints in developing countries remain that will hamper adoption. For example, access to electricity, water, Internet connectivity are just some of the very basic necessary inputs missing to the majority of the world's very poor. More than 4 billion people in the world are not connected to the Internet – so how would blockchain be applicable to them? This underscores the importance for developers of blockchain applications to take into account of the many different contexts that the technology would need to operate in what could have major impact on adoption. The tech needs to be amenable and adaptable to different ecosystems, i.e. Khan Academy lite is a great example of context, whereas internet.org ran into controversies. It also needs to be complemented with the 'real' side, i.e. human capacity, existing institutions, cultural norms and perception, tech utilization and adoption. What this entails is a close working relationship with developers as to the challenges in developing countries to work towards blockchain's potential to change the lives of the bottom billion (Schiller, 2016).

Operational Internal Processes in International Organizations – Blockchain has the potential to improve accountability in a much more effective and efficient manner, facilitate faster decision-making, help speed up processes, improve governance and incorporation of large scale inputs simply, and, thereby, also the potential to facilitate a more open decision-making process (see also previous section on Participation and Blockchain). Furthermore, adoption of blockchain within internal bank processes could circumvent traditional convoluted loan application processes, with automation, greater leveraging of data and risk assessments. For example, multibillion development loans take months if not years of labor-intensive preparation. Each one meticulously handcrafted, each one requiring a team, costing millions in research, identification, and design at every single time. On one hand, there is a need for each loan to adapt to particular circumstances, however on the other, there are many similarities and commonalities among loans that could be programed via smart contracts, following defined set of common variables, and fulfilled by automation. With adequate data, loans could be processed based on adaptive matrices and historical models, and implemented all through blockchain. This has the potential to reduce massive cost, processing time, enhance transparency, increase scale and consistency of loans across different countries.

Measurement within International Organizations – Blockchain has the potential to improve data quality for measurement and tracking impact through greater precision in measuring, verifying and recording impact: from micro data level to aggregation. For example, production data can be tracked via value chains on the blockchain to have precise measurements from domestic production to export and international trade data. Global Institutions have traditionally taken a leading role in the compilation of global indicators, developing methods of harmonized measurements, and procedure for numbers to be verified across all countries. However, much of the current global data is extrapolated through sometimes precise, sometimes fuzzy surveying methods to arrive at estimates. However, given the reduction in cost and the ease for data collection, blockchain can be deployed or automated from real time census data that can measure continuously across time over the current method of time specific sampling. The evolution of data collection can provide much needed innovation in global institutions across all key components of the institution: global goals, participation and stakeholders, products and services, and internal processing. The advent of new data analytics and precision measurement could contribute to better monitoring and assessments of risks, ex ante assessments and predictive models, and better historical models to base forecasts. The biggest potential delta of blockchain is the verification of data points and the possible ability to tracking goods and services around the world.

References

https://sustainabledevelopment.un.org/sdgs.

Adam Back & Greg Maxwell: Sidechains Unchained. Interview by Brian Fabian Crain and Sebastien Couture. YouTube. Epicenter Bitcoin, 3 Feb. 2015. Web. 10 Feb. 2015.

Ajinkya, B. Barton, J. Benston, G. Butler, M. Core, J. Demski, J., … Waymire, G.B., 2006. Recordkeeping and human evolution 20, 201–229.

Baran, P., 1962. On Distributed Communications Networks.

Batlin, Alex, Jaffrey, Hyder, Murphy, Christopher, Przewloka, Andreas, Williams, Shane, 2016. Building the Trust Engine: How the Blockchain Could Transform Finance (and the World). UBS Group Technology. UBS. Print.

Belinky, M. Rennick, E. Veitch, A., 2015. The Fintech 2.0 Paper: rebooting financial services. Santander InnoVentures, Oliver Wyman, and Anthemis Group.

Census Information, 2016. U.S. and World Population Clock. http://www.census.gov/popclock/.

Dai/Nakamoto Emails. Gwern., 17 Mar. 2014. Web. Oct. 2016.

Financial institution. Merriam-Webster.com. Merriam-Webster, 2016. Web. October 2016.

Garfinkel, Haskell, Drane, Jeremy, Marsh, Cathryn, 2016. What's Next for Blockchain in 2016? Rep. Financial Services Institute, PricewaterhouseCoopers. PwC. Print.

Hashcash. Hashcash. Adam Back, Web. Oct. 2016.

institution. Merriam-Webster.com. Merriam-Webster, 2016. Web. October 2016.

Internet Live Stats, 2016. http://www.internetlivestats.com/internet-users/ (last accessed October 2016).

Kahin, B., Varian, H., 2000. Internet publishing and beyond: the economics of digital information and intellectual property.

Kaldor, Mary. Our global institutions are not fit for purpose. It's time for reform. In: World Economic Forum. 24 Jan. 2015. Web. Oct. 2016.

Killeen, Alyse M., 2015. The confluence of bitcoin and the global sharing economy. In: Lee, David (Ed.), Handbook of Digital Currency, Bitcoin, Innovation, Financial Instruments, and Big Data, vol. 1, 1st ed.. Elsevier, pp. 485–502. Print.
Lopp, Jameson, Apr. 2016. Bitcoin and the rise of the cypherpunks. CoinDesk 9. Web. Oct. 2016.
Meeker, M., 2016. Internet Trends 2016. http://www.kpcb.com/blog/2016-internet-trends-report (last accessed October 2016).
Nakamoto, S., 2008a. Bitcoin: A Peer-to-Peer Electronic Cash System.
Nakamoto, S., 2008b. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.
Poast, P., Urpelainen, J., 2013. Fit and feasible: why democratizing states form, not join, international organizations. International Studies Quarterly 57 (4), 831–841.
The Millennial Disruption Index. Publication. Scratch, Viacom Media Networks. Viacom Media Networks, 2013. Web. Oct. 2016..
Rizzo, Pete. Gem Shifts Focus with New Emphasis on Blockchain, CoinDesk, 8 Jan. 2016. Web. June 2016.
Sala-i-Martin, Xabier, Crotti, Roberto, Di Battista, Attilio, Drzeniek Hanouz, Margareta, Galvan, Caroline, Geiger, Thierry, Marti, Gaelle, 2015. The Global Competitiveness Report 2015–2016. Rep. World Economic Forum. World Economic Forum. Print.
Schiller, B., 2016, March. How the technology behind bitcoin is going to change the lives of the bottom billion. Co.exist.
Schwab, Klaus. Why we need institutions to solve the world's problems. In: World Economic Forum. 8 July 2016. Web. Oct. 2016.
Tallberg, J., Sommerer, T., Squatrito, T., 2016. Democratic memberships in international organizations: sources of institutional design. Review of International Organizations 11 (1), 59–87. http://doi.org/10.1007/s11558-015-9227-7.
Tapscott, D., Tapscott, A., 2016. Blockchain Revolution. Penguin Random House.
The Trust Machine, 2015. The technology behind bitcoin could transform how the economy works. The Economist 417 (8962).
Transfers and servicing of financial assets (rep.), 2016. PwC.

Notes

1. All views are those of the authors and do not reflect the views of the World Bank or its member countries.
2. Census Information, 2016. U.S. and World Population Clock. http://www.census.gov/popclock/ (last accessed October 2016).
3. Internet Live Stats, 2016. http://www.internetlivestats.com/internet-users/ (last accessed October 2016).
4. Meeker, M., 2016. Internet Trends 2016. http://www.kpcb.com/blog/2016-internet-trends-report (last accessed October 2016).
5. Killeen, Alyse M. "The Confluence of Bitcoin and the Global Sharing Economy." *Handbook of Digital Currency, Bitcoin, Innovation, Financial Instruments, and Big Data*. Ed. David Lee. 1st ed. Vol. 1. Elsevier, 2015. 485–502. Print.
6. Nakamoto, S., 2008b. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf (last accessed August 2016).
7. "Adam Back & Greg Maxwell: Sidechains Unchained." Interview by Brian Fabian Crain and Sebastien Couture. *YouTube*. Epicenter Bitcoin, 3 Feb. 2015. Web. 10 Feb. 2015.

8. Killeen, Alyse M. "The Confluence of Bitcoin and the Global Sharing Economy." *Handbook of Digital Currency, Bitcoin, Innovation, Financial Instruments, and Big Data*. Ed. David Lee. 1st ed. Vol. 1. Elsevier, 2015. 485–502. Print.

9. Baran, P., 1962. On Distributed Communications Networks.

10. Garfinkel, Haskell, Jeremy Drane, and Cathryn Marsh. *What Is Blockchain?* Rep. Financial Services Institute, PricewaterhouseCoopers. PwC, 2016. Print.

11. Garfinkel, Haskell, Jeremy Drane, and Cathryn Marsh. *What Is Blockchain?* Rep. Financial Services Institute, PricewaterhouseCoopers. PwC, 2016. Print.

12. Batlin, Alex, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka, and Shane Williams. *Building the Trust Engine: How the Blockchain Could Transform Finance* (*and the World*). UBS Group Technology, UBS, 2016. Print.

13. Sala-i-Martin, Xabier, Roberto Crotti, Attilio Di Battista, Margareta Drzeniek Hanouz, Caroline Galvan, Thierry Geiger, and Gaelle Marti. *The Global Competitiveness Report 2015–2016*. Rep. World Economic Forum. World Economic Forum, 2015. Print.

14. "institution." *Merriam-Webster.com*. Merriam-Webster, 2016. Web. October 2016.

15. Sala-i-Martin, Xabier, Roberto Crotti, Attilio Di Battista, Margareta Drzeniek Hanouz, Caroline Galvan, Thierry Geiger, and Gaelle Marti. *The Global Competitiveness Report 2015–2016*. Rep. World Economic Forum. World Economic Forum, 2015. Print.

16. "financial institution." *Merriam-Webster.com*. Merriam-Webster, 2016. Web. October 2016.

17. Schwab, Klaus. "Why We Need Institutions to Solve the World's Problems." *World Economic Forum*. World Economic Forum, 24 Jan. 2015. Web. Oct. 2016.

18. Kaldor, Mary. "Our global institutions are not fit for purpose. It's time for reform." *World Economic Forum*. World Economic Forum, 24 Jan. 2015. Web. Oct. 2016.

19. Schwab, Klaus. "Why We Need Institutions to Solve the World's Problems." *World Economic Forum*. World Economic Forum, 8 July 2016. Web. Oct. 2016.

20. Garfinkel, Haskell, Jeremy Drane, and Cathryn Marsh. *What's next for blockchain in 2016?* Rep. Financial Services Institute, PricewaterhouseCoopers. PwC, 2016. Print.

21. Batlin, Alex, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka, and Shane Williams. *Building the Trust Engine: How the Blockchain Could Transform Finance* (*and the World*). UBS Group Technology, UBS, 2016. Print.

22. Batlin, Alex, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka, and Shane Williams. *Building the Trust Engine: How the Blockchain Could Transform Finance* (*and the World*). UBS Group Technology, UBS, 2016. Print.

23. Rizzo, Pete. "Gem Shifts Focus With New Emphasis on Blockchain." *CoinDesk*. CoinDesk, 8 Jan. 2016. Web. June 2016.

24. Belinky, M., Rennick, E., Veitch, A., 2015. The Fintech 2.0 Paper: rebooting financial services. Santander InnoVentures, Oliver Wyman, and Anthemis Group.

25. *The Millennial Disruption Index*. Publication. Scratch, Viacom Media Networks. Viacom Media Networks, 2013. Web. Oct. 2016.

26. Baran, P., 1962. On Distributed Communications Networks.

27. Lopp, Jameson. "Bitcoin and the Rise of the Cypherpunks." *CoinDesk*. CoinDesk, 9 Apr. 2016. Web. Oct. 2016.

28. "Hashcash." *Hashcash*. Adam Back, Web. Oct. 2016.

29. "Dai/Nakamoto Emails." *Gwern*., 17 Mar. 2014. Web. Oct. 2016.

30. Batlin, Alex, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka, and Shane Williams. *Building the Trust Engine: How the Blockchain Could Transform Finance* (*and the World*). UBS Group Technology, UBS, 2016. Print.

31. Batlin, Alex, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka, and Shane Williams. *Building the Trust Engine: How the Blockchain Could Transform Finance* (*and the World*). UBS Group Technology, UBS, 2016. Print.

32. Transfers and servicing of financial assets (rep.), 2016. PwC.

33. Batlin, Alex, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka, and Shane Williams. *Building the Trust Engine: How the Blockchain Could Transform Finance* (*and the World*). UBS Group Technology, UBS, 2016. Print.

CHAPTER 11

Open-Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?

Angela Walch

Contents

11.1 Financial Sector Hype 245

11.1.1 Who Is Interested in Blockchain Technology? 246

11.1.2 What Do They Like About It? 246

11.2 FMIs and Operational Risk 249

11.3 Open-Source Operational Risks of Public Blockchains 251

11.3.1 Hampered Decision-Making and Grassroots Open-Source Software Development Practices 253

11.3.1.1 Decentralized Software Governance 253

11.3.2 Inadequate Software Maintenance and Problematic Open-Source Funding Model 256

11.3.3 Fractured Networks Caused by Open-Source Software Forking Practices 259

11.3.3.1 March 2013 Bitcoin Hard Fork 260

11.3.3.2 Bitcoin Block Size Debate 261

11.3.3.3 July 2016 Ethereum Hard Fork 262

11.3.3.4 51% Attack Risk 263

11.3.3.5 Lessons Learned 263

11.4 Reflections 266

References 267

Notes 269

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00011-5
Copyright © 2018 Elsevier Inc. All rights reserved.

Every reader of this *Handbook* will be well aware that blockchain technology, also called 'distributed ledger technology' or 'DLT,' is all the rage in financial circles at the moment. One cannot escape white papers by various banks and consulting firms, speeches by central bankers, and a deluge of articles, books, conferences, summits, and workshops proclaiming the imminent transformation of the financial system by this revolutionary technology. The Gardner Hype Cycle put blockchain technology at virtually the top of its hype cycle curve in the summer of 2016, indicating that the zeitgeist around blockchain technology is soon to fall into the "trough of disillusionment" as sky-high expectations collide with harsh realities (Burton and Willis, 2016).

This chapter delves into some of those harsh realities, as it focuses on the risks created by the use of what I call 'grassroots' open-source software[1] methods in the operation of public blockchains, and the resulting fragility of any systems that rely on public blockchains as underlying technological infrastructure. Public blockchains, otherwise referred to as 'open' or 'permissionless' blockchains, allow anyone to become part of the computer network that maintains the blockchain; to join, one simply downloads and begins to run the applicable software. Private blockchains, otherwise referred to as 'closed' or 'permissioned' blockchains, allow only those who have received 'permission' to join the computer network that maintains the blockchain, thus limiting the network to those who are known and trusted. Public and private blockchains are diametrically opposed to one another, and the seemingly simple decision about access to the network of transaction processors fundamentally changes the risk profile (as well as the capabilities and emergent properties) of a blockchain.

This chapter limits its analysis to public blockchains, and explores how the use of three common practices from the grassroots open-source software world gives rise to operational risks for these blockchains. These practices are: (1) the use of the informal, semi-decentralized grassroots open-source software development process to maintain the blockchain software; (2) the use of the funding model (or lack thereof) for grassroots open-source software development; and (3) the practice of forking software code that is an inherent feature of open-source software.

As each of these practices generates operational risks for public blockchains, systems built on these structures (such as financial market infrastructures, or "FMIs") would be similarly subject to these systemic vulnerabilities. Threats to financial market infrastructures are threats to broader financial stability, which makes the financial sector's fascination with all things 'blockchain' extremely significant. While existing FMIs are of course subject to systemic risks, it is important not to gloss over serious operational risks in certain forms of blockchain technology in the rush to fix our much-maligned existing FMIs. Important trade-offs exist in repairing or replacing our current financial market infrastructures, and it is vital to assess those trade-offs through crystal-clear, rather than rose-tinted, lenses.

In Section 11.1 of this chapter, I describe the excitement about blockchain technology in the financial sector, as well as the features of the technology that are seen as attractive and transformational. Blockchain technology appears to offer the silver bullet of solutions to financial practices in providing reliability and certainty.

In Section 11.2, I provide background information on how financial market infrastructures are treated by global financial regulators. Given FMIs' acknowledged significance to maintaining global financial stability, their reliability and resilience are crucial, and I note particularly how regulators have identified governance and operational risks as critical ones for FMIs to manage.

In Section 11.3, I provide the core contribution of this chapter, in analyzing three practices common to grassroots open-source software development that create systemic instability for public blockchains: (1) informal governance of the software code; (2) funding software development and maintenance in an uncertain or experimental way (if at all); and (3) the practice of forking the software code to make changes to it. I explicate how each of these practices produces significant operational risks for public blockchains, as already demonstrated by real-world events with both Bitcoin and Ethereum, the best-known public blockchains.

In Section 11.4, I reflect on the implications of these operational risks in how we choose to use public blockchains, as well as their implications for the use of grassroots open-source software practices in critical systems, generally. As some think that blockchain technology will revolutionize virtually every system of record-keeping or exchange that we have, it is important to reexamine the basic attributes of the technology to understand the trade-offs we would make in choosing to integrate public blockchains widely.

11.1 Financial Sector Hype

The financial world has become obsessed with blockchain technology. There are infinite conferences and workshops devoted to it, blockchain and fintech thought leaders ply their wisdom through Twitter and other forms of media, and every significant financial player, from J.P. Morgan to DTCC all the way up to the world's central banks, is experimenting with the technology, and proclaiming that it will transform the financial sector. Mark Carney, Governor of the Bank of England, discussed the technology in his important Mansion House speech in June 2016 (Carney, 2016), and blockchain technology proponents presented to representatives from 90 central banks at the Federal Reserve in June 2016 (Rapier, 2016). Blockchain technology is the ultimate trend at the moment, and no one wants to be left behind.

In this section, I describe the financial sector's great interest in blockchain technology, the features of the technology that are celebrated by the sector as transformative, and the benefits that the sector hopes to achieve through the use of the technology.

www.elsevierdirect.com

Once this foundation is laid, I can demonstrate more clearly with my analysis in Section 11.3 how common practices from grassroots open-source software development make public blockchains, as currently structured, inappropriate for the financial sector's plans.

11.1.1 Who Is Interested in Blockchain Technology?

Since the summer of 2015, the financial world has been intoxicated by blockchain technology. Around 70 banks have joined together in a consortium called R3Cev to develop distributed ledger technology together (Eha, 2016). Hyperledger, an open-source consortium for the development of common blockchain tools, was formed in conjunction with the Linux Foundation, and has received code contributions from Digital Asset Holdings and IBM, among others (Rizzo, 2016). The Bank of England has formed a partnership with Big-Four accounting firm PWC to investigate the use of distributed ledgers in the financial sector (PWC, 2016). Numerous central banks, financial regulators, and international economic organizations have spoken out about the promise of blockchain technology to revolutionize financial systems. A belief in the benefits of blockchain technology to the financial sector is clearly widely shared, and a plethora of blockchain-related books have been released in the past year, proclaiming the technology's virtues. It is fair to say that the consensus view is that blockchain technology is a massive innovation that will transform and improve financial structures and practices. Dissenting voices are few and far between.[2]

11.1.2 What Do They Like About It?

Blockchain technology is attractive to the financial sector due to its most celebrated purported attributes. In report after report from central banks, prestigious consulting and financial institutions, and international economic groups, the following descriptors are repeatedly cited as potentially transformative for finance:

- *Immutability*
- *Trustlessness*
- *Visibility/Transparency*
- *Resilience*

What all of these features have in common is that they suggest that the technology is something reliable – that it can be counted on, whether that reliability has to do with the truth of what the blockchain displays or its continued operation in a crisis. In this section, I discuss in more detail what the financial world likes about these claimed features, and industry visions of how these features would improve it. In describing these features, I do not mean to suggest that it has been definitively established that blockchain technology actually has these features,

as all of them can be questioned or critiqued to some extent. However, these features are repeatedly claimed to exist in blockchain technology, and are attractive to the financial sector for the reasons below.

Immutability: The ledgers that operate through blockchain technology are said to be immutable – i.e., unchangeable. This means that, in theory, once an entry is added to the blockchain, it cannot be altered or removed. This is attractive to participants in the financial sector because it means they can rely on the truth of the ledger – immediately, and without having to expect corrections to it. An important implication of this is that amounts set back in reserve to address settlement risk could be foregone, and finance could proceed more efficiently. (As DTCC, 2016 White Paper on blockchain technology noted, however, immutability is not particularly attractive to financial transactions, as there are inevitably errors and fraud in the real world that require corrections to be made (DTCC, 2016, p. 8). The prominent consulting firm Accenture recently announced that it is patenting an "editable blockchain," triggering widespread derision from public blockchain advocates (Arnold, 2016).)

Trustlessness: The decentralized nature of blockchain technology is attractive because it is said to eliminate the need to count on a central trusted party to operate it – i.e., to make updates to the ledger and to keep the technology running. Thus, you no longer need the intermediaries who serve as aggregators of risk – known as central counterparties. You trust that the network—through the magic of cryptography, algorithms, and a defined process for achieving consensus—is maintaining a truthful ledger.

This is a very attractive idea. In the finance world, trust is everything, because the outcomes are largely determined by how trustworthy a counterparty is. Will it pay you back as promised? Will the company do as well as it predicted? All of finance is essentially a gamble on the trustworthiness of the other side, and being able to eliminate even one uncertainty (the trustworthiness of a central counterparty) is extremely valuable. (For now, we will gloss over the fact that, even with a blockchain, one must trust the integrity of the code, the developers, and the transaction processors. The rosy view is that eliminating trust in a central operator of the ledger is an unsullied innovation.)

Visibility/Transparency: In traditional public blockchains like Bitcoin or Ethereum, the common ledger that is the blockchain is visible to all nodes (parties) in the network. So, everyone sees the same thing. This means that it is possible to evaluate risk and therefore price it more accurately. If risk decisions are based on current and reliable information, the theory goes, they will be better decisions. Blockchain or distributed ledger technology allows for this visibility and transparency because the ledger is distributed to multiple parties simultaneously. This means that every participant in the blockchain or distributed ledger network has a live, up-to-date copy of the ledger, and sees any changes in real time as they are made. Everyone sees the same thing, and knows that the ledger represents truth. This is a boon to the financial

www.elsevierdirect.com

sector because time delays in confirming trades add uncertainty to the process, and force participants to reserve resources against this settlement risk. With instantaneous settlement, it is said, there is no need to reserve against settlement risk, saving lots of money.

Some have gone so far as to say that blockchain technology could have prevented the Financial Crisis, particularly the fall of Lehman Brothers, as the Department of the Treasury and the Federal Reserve would have had real-time information to help them determine whether Lehman was solvent and could be saved (Giancarlo, 2016). In a world that is looking for ways to avoid crises while maintaining a growing economy, blockchain technology appears to offer potent tools well-suited for this purpose.

Resilience: The critical importance of financial market infrastructures has long been recognized, but has received renewed attention following the 2008 Financial Crisis. These pathways of communication can rapidly transmit financial crises, and their failure can trigger or worsen a crisis. Global financial regulators therefore set standards for financial market infrastructures, such as payment, clearing, and settlement systems. In the past few years, cyber-resilience of financial market infrastructures has been particularly emphasized (Bank for International Settlements, 2015), as hack after hack has hit major companies, government agencies, and even the SWIFT consortium operated by the world's financial institutions (Perlroth and Corkery, 2016). A systemic outage in a financial market infrastructure is a worst-case scenario for the financial system, so blockchain technology's reputation for resilience is highly attractive to global financial regulators.

Blockchain technology's purported resilience derives from its decentralized structure. As the network operates on a peer-to-peer basis rather than through a central server, there is no single point of failure in the network. Theoretically, there are as many up-to-date and operational copies of the distributed ledger as there are nodes in the network. This is highly desirable for a digital infrastructure, as it would be extraordinarily difficult to knock out all nodes simultaneously. Central banks and other international economic organizations have commented on this as an extremely attractive feature of blockchain technology (see, e.g., Carney, 2016).

All of these claimed features – immutability, trustlessness, visibility/transparency, and resilience – add up to increased reliability. Given that a major function of the financial sector is simply keeping track of who has what, a reliable record-keeping system is vital. If blockchain technology offers a more reliable record-keeping system, then risk is reduced because something (truth, timeliness, long-term existence and ongoing operation) can be counted on. This means that more risk can potentially be taken in other areas, particularly if the whole concept of settlement risk evaporates because settlements are instantaneous. If the financial sector can know things in real time and those things can't be changed, then people within the sector can make decisions more quickly, with the confidence that they are standing on something certain, rather than upon shifting sands. And, these factors all should lead to big savings for the

financial sector, by eliminating steps (and people) from (as well as speeding up) all sorts of processes. Increased savings and greater efficiencies should yield bigger profits, making the promise offered by this technology heady indeed.

Thus, the finance industry contemplates using blockchain technology in virtually every trading, settlement, clearing, and recording function that it engages in, from stocks, to bonds, to foreign exchange, to derivatives. If it is traded or recorded in the financial sector, blockchain technology, proponents say, is going to revolutionize it.

11.2 FMIs and Operational Risk

Before delving into the operational risks stemming from the use of grassroots open-source software practices in public blockchains, this Section 11.2 provides a brief overview of what financial market infrastructure is, its extreme importance to global financial stability, and how global regulators treat operational risk in existing financial market infrastructures.

Financial market infrastructures are "multilateral systems among participating financial institutions. . . used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions," which "include payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories" (Federal Reserve, 2016, p. 3). These systems allow our vast economies to keep track of who owns (and owes) what.

Unsurprisingly, the uninterrupted operation of financial market infrastructures is extraordinarily important to global financial stability. Failure in a system that functions as financial market infrastructure could disrupt financial markets and affect the public's faith in the financial system (Federal Reserve, 2016).

Given the massive problems that could be caused by failures of financial market infrastructures, regulators around the world have worked together to adopt principles to help FMIs mitigate their risks. The goal behind these principles is generally "to foster the safety and efficiency of payment, clearing, settlement, and recording systems and to promote financial stability, more broadly" (Federal Reserve, 2016, p. 3). Many countries have based their guidance to FMIs on the April 2012 *Principles for Financial Market Infrastructures* (PFMI) report by the Bank for International Settlement's Committee on Payment and Settlement Systems (CPSS)[3] and Technical Committee of the International Organization of Securities Commissions (IOSCO).

The risks that the international guidelines for FMIs are intended to address include credit risk, operational risk, liquidity risk, legal risk, systemic risk, general business risk, and custody and investment risk (Federal Reserve, 2016; PFMI, 2012). In this Chapter, I focus on operational

www.elsevierdirect.com

risk, as it is important to understand whether public blockchains can live up to their reputation for reliability, so prized by the financial sector. The Federal Reserve's definition of operational risk is fairly standard:

> *The risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the [financial market infrastructure]... includ[ing] physical threats, such as natural disasters and terrorist attacks, and information security threats, such as cyberattacks. Further, deficiencies in information systems or internal processes include errors or delays in processing, system outages, insufficient capacity, fraud, data loss, and leakage.*
>
> **(Federal Reserve, 2016, p. 5)**

Essentially, operational risk is a catch-all sort of risk that deals with unexpected external events, and problems caused by human imperfections. These are precisely the types of risks that, in Section 11.3, I argue are generated by the use of common grassroots open-source software practices in public blockchains.

To help mitigate operational risks, the *Principles for Financial Market Infrastructures* include these standards:

> *Principle 2: Governance: An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.*[4]
> *Principle 3: Framework for the comprehensive management of risks: An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.*
> *Principle 17: Operational risk: An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to have a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfillment of the FMI's obligations, including in the event of a wide-scale or major disruption.*
>
> **(PFMI, 2012, pp. 1–3)**

As I will discuss in Section 11.3, these widely-recognized principles for mitigating operational risk in FMIs are fundamentally at odds with common practices of public blockchains,

and it is very difficult to see how they could be met in public blockchains without altering certain grassroots open-source software practices that help contribute to their openness. Thus, if we were to build financial market infrastructures atop public blockchains as they exist currently, we would be accepting a new flavor of operational risk. The question becomes, then, whether the benefits of public blockchains serving as the underlying technology of FMIs (e.g., reduction of settlement risk) can justify the acceptance of this type (and potentially higher level) of operational risk.

11.3 Open-Source Operational Risks of Public Blockchains

Reliable, certain, resilient (yet speedy) systems are the Holy Grail for the financial world, and many believe that blockchain technology represents the finding of the Grail for the record-keeping systems that comprise much of finance (Kaminska, 2016). It remains to be seen, however, whether this quest has been completed.

An important decision remains to be made as blockchain development proceeds apace: whether public or private blockchains will be used to transform the world of finance. Most experimentation and development work on blockchain technology in the financial sector has involved private, or closed, blockchains. However, the debate over the appropriate form of blockchain technology (public or private) has not yet been resolved. A number of prominent, respected players in the blockchain and finance worlds have noted that public blockchains like Bitcoin and Ethereum remain in the hunt. For instance, MUFG, the world's third largest bank, announced in October 2016 that it was working with Coinbase, a Bitcoin exchange, to conduct cross-border payments through Bitcoin (Eha, 2016). And SEC Chair Mary Jo White stated in November 2016 that the SEC is looking at whether blockchain technology used in the financial sector will be permissioned (White, 2016), suggesting that the debate between public and private blockchains has not yet ended.

This paper contributes to the public-versus-private blockchain debate, explicating how the use of traditional grassroots open-source software practices in public blockchains would expose any financial market infrastructures they undergird to new and potentially increased operational risks in exchange for the benefits they seductively promise. There are trade-offs to all improvements we make, and in this case, the new operational risks seem quite hefty.

In this Section 11.3, I explore a set of operational risks generated by the use of customary grassroots open-source software practices in the creation and maintenance of public blockchains. The risks and practices that I examine include:

1) the risk of impeded decision-making about changes to the software code, resulting from using the typical informal grassroots open-source software development process;

www.elsevierdirect.com

2) the risk that the software is inadequately maintained due to insufficient or problematic funding for software development and maintenance, as is common with open-source projects; and
3) the risk that the software (and the blockchain and other structures built on it) forks, resulting in fractured blockchain networks, due to the customary practice of forking open-source software to make desired changes to it.

There are no doubt other critically important operational risks to public blockchains, as I and others have explored (Kiran and Stannett, 2014; Peters et al., 2014; Walch, 2015). However, in this Chapter, I am focused on the operational risks most related to the use of customary grassroots open-source software practices in the running of public blockchains. This analysis marks an expansion of my examination of the operational risks generated by Bitcoin's status as open-source software in an earlier paper (Walch, 2015), as the topic merits deeper engagement.

Before jumping into the analysis, a very brief primer on open-source software is in order.

Open-source software is software for which the source code (i.e., the part of the code that is readable by humans) is made freely available to all. It is distinguished from proprietary software, for which the owner of the code does not make the source code available, and for which the owner places limits on use. Open-source software comes with a set of core freedoms: "the rights to access the source code, modify the program, and redistribute it, either in its original or modified form." (Nyman, 2015, p. 14.)

Various practices from the open source software area will be explained as I analyze them in the subsections below. However, one important distinction underlies the entire analysis: whether an open-source project is (a) initiated and run by an independent set of software developers (sometimes called an "autonomous" open-source project (West and O'Mahoney, 2008), though I prefer "grassroots"); or it is (b) created and run by a legal entity (like a corporation) (sometimes called a "sponsored" or "corporate" open-source project) (Nyman, 2015, p. 24). Grassroots and corporate open-source projects vary significantly in how decisions are made about the code. With a grassroots project, decisions are made through an informal process to reach "rough consensus" (described further below), while in a corporate project, "ultimately the sponsor company. . . decides what is included in the end product." (Nyman, 2015, p. 24.) Though there is a spectrum on which different open-source projects lie, fully grassroots open source lies at one end of the spectrum (where control and power are eschewed), while corporate open source lies at the other end (where control and power are explicit).

Control over decision-making relates to all of the practices I discuss in this Section 11.3, including how the software code changes, how software development is funded, and whether

and how the software code is forked. As my analysis will reveal, a lack of defined or accountable control over these processes generates operational risks for public blockchains, impacting their suitability to serve as financial market infrastructures (or other critical societal systems).

11.3.1 Hampered Decision-Making and Grassroots Open-Source Software Development Practices

As noted in Section 11.2, clear governance structures are viewed as essential for FMIs. This makes perfect sense for something that is seen as critical to global financial stability. If something goes wrong with an FMI, a clear chain of command is desirable in order to make decisions quickly, and with accountability. This is a basic tenet of the human experience – that governance structures emerge, and that with high-stakes matters, clarity on responsibility is crucial. This is why there is a long, clear line of succession for the office of President of the United States, and why we insist upon a clear chain of command and well-defined protocols in the military, police and fire departments, hospitals, nuclear reactors and power plants. With high-stakes matters, humans have decided that clear hierarchy and structure are helpful in safe and effective management.

Public blockchains use a very different governance model: the software development process commonly used to develop and maintain grassroots open-source software. In this subsection, I describe how this software development (i.e., governance) model hampers the decision-making around changes to a public blockchain's software code.

First, a brief overview of the software development process of grassroots open-source software and public blockchains is appropriate.

11.3.1.1 Decentralized Software Governance

The hallmark of blockchain technology is that it is decentralized – i.e., that there is no central party that maintains this data structure. Public blockchains are decentralized in two ways. First, the network of transaction processors that maintains the ledger is decentralized, and anyone in the world may freely join this network of computers without needing permission. Second, and more important for our purposes, the governance of the software code that comprises public blockchains is also decentralized and informal. Governance of the software code is extremely important because the code itself is ever-evolving, as new releases of software are issued to fix problems, make improvements, and add new features. With public blockchains, these code changes come about through the efforts of a team of software developers loosely organized under a model typically used for grassroots open-source software.

Public blockchains are generally built with open-source software. This means that anyone can see, make use of, and make changes to the software code, so long as they make the code they

www.elsevierdirect.com

build from it open-source. The governance process of open-source software is famously informal, with the coders who actually make decisions about changes to the code (known as core developers) gradually rising to the top of the leadership pyramid based on their reputation and performance. The coders of grassroots open-source projects do not work for a single organization, and the group of coders working on an open-source project may be quite fluid. And, decisions about the code are made based on "rough consensus" rather than a formalized voting or other decision-making process. Further, with grassroots open-source projects, coders generally work on the code without compensation, largely because there is no business or entity there to pay them. Contributing to the code is viewed as an altruistic, community-building action within the coding community, so coders usually participate in open-source projects as a hobby rather than a full-time job. (I address the risks raised by this funding model in Section 11.3.2 below.)

This has been the general software development model used with public blockchains, particularly with Bitcoin. It is worth thinking through the implications of this governance model, particularly in the context of a public blockchain supporting financial market infrastructure (or any other critical public system, really). In considering the governance implications I describe in the following paragraphs, I ask the reader to imagine using this type of governance model with our military defenses (e.g., nuclear weapons) or in an intensive care hospital unit, to concretize how ill-suited this model is for high-stakes matters.

There are a number of ways that the grassroots open-source governance model could hamper decisions about the code. First, in this model, no one has the official responsibility for keeping the software operational (Walch, 2015). By this, I mean that no one is necessarily accountable for a failure to do so. People choose (or not) to participate in the software development process, and have complete freedom (without consequence, other than possible reputational harm) to help or not help in a moment of crisis. Developers who have previously maintained the software are under no obligation to act in a crisis, and may find it riskier to act than to abandon the system. While core developers have acted in the past to resolve crises with the Bitcoin and Ethereum blockchains (the March 2013 fork, for Bitcoin, and the DAO theft, for Ethereum), there is no guarantee that they would do so in the future (Walch, 2015).

Second, under the grassroots open-source governance model, no one is in charge of making decisions for the network. I have argued previously:

> *"As there is no defined power or accountability structure, no one has to listen to anyone else's ideas about how to resolve a crisis. There are no definitively appointed decision-makers. This is different from having no one responsible for keeping the software operational; this risk is that even if people decide to take on responsibility for resolving a problem with the . . . software. . . , their authority to*

> *do so, and their resulting ability to implement their solution, is in question. This means that anyone with a suggested resolution to a crisis may merely propose a solution, but it may take too long to achieve buy-in from other members of the . . . community to successfully implement the solution in an emergency situation. We see this type of argument commonly made in debates over the limits of the executive power of the President of the United States, who may need to act quickly in a crisis without waiting for specific authority from Congress."*
>
> **(Walch, 2015, p. 871)**

Third, this amorphous governance model can lead to unacknowledged centralization of power, resulting in unaccountable or unchecked power. The core developers of public blockchains are more powerful than the rank-and-file developers on these projects. In Bitcoin, for instance, a small number of core developers are the only people who have the passwords to actually enter changes into the underlying code. They also act as the voice of the blockchain through their interactions with the media, regulators, and others in the blockchain ecosystem, as their recommendations and insights are seen as relevant and consequential to the future of the applicable blockchain. As an example, many core developers are frequent panelists or keynote speakers at blockchain or fintech conferences around the world.

What is problematic about unacknowledged centralization of power is not the *centralization* part, but the *unacknowledged* part. Unacknowledged, or hidden, power, can lead to the exercise of unaccountable, unchecked power. With precisely delegated power, it is clear what actions one can and cannot take, but with amorphous powers, the limits of power are fuzzy, and can easily be expanded. Unaccountable power is a bad fit for financial market infrastructures, or for other critical public systems. (The unaccountable power that can arise in these structures is, ironically, exactly what these open systems were designed to fight against, as they are reactions to the closed (unaccountable) software development process for proprietary software.)

All of these scenarios described in this Section 11.3.1 could either paralyze or delay critical decisions about the software code, endangering all structures built on top of it. Indeed, a debate is ongoing in the public blockchain world over which software changes should be considered purely technical versus those considered more ideological, and these debates create the potential for software forks, as I describe in Section 11.3.3 below. Moreover, if someone does act as if her or she has authority (similar to Vitalik Buterin of Ethereum), there is a chance that the decision will not receive buy-in from the blockchain community, again potentially leading to forks in the code and blockchain.

As with law, change is necessary to all software in order for it to continue to be useful. If a software governance process generates paralysis, the software cannot improve or adjust to

www.elsevierdirect.com

changing conditions. The balance between concentrated and distributed power is difficult to strike, but the standard grassroots open-source software development process appears too far along the spectrum of (nominally) distributed power to govern critical systems like financial market infrastructures.

Perhaps in recognition of this problem, newer public blockchains appear to be tweaking the typical informal open-source governance process, adding more structure. Zcash, a cryptocurrency launched to wide interest in October 2016, is based on the Bitcoin code, but with enhanced privacy through 'zero-knowledge proofs.' It has established a slightly more formal governance structure than that used on Bitcoin, but analysis of that structure and its implications will have to wait for a future paper. Ethereum, another public blockchain, has also adjusted governance, relying heavily on founder Vitalik Buterin to guide the trajectory of the project. Zcash also has a founder, Zooko Wilcox, who is strongly identified with the project. Crucial to note here is that the governance structures of Zcash, Ethereum, and others are experiments, or works-in-progress, and it is unclear whether they will function better than the purer grassroots open-source software development process used in Bitcoin. It is one thing to experiment with a new type of technology for financial market infrastructures, but another level of risk is added when the governance of the technology is also experimental.

Given that the global standards for financial market infrastructures state that

> *"FMI[s] should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders."*
>
> **(PFMI, 2012, p. 1)**

it is unlikely that using informal, experimental, grassroots open-source governance practices in public blockchains could satisfy this standard.

11.3.2 Inadequate Software Maintenance and Problematic Open-Source Funding Model

The second common open-source software practice I examine is how open-source software development is funded. It is widely acknowledged that funding grassroots open-source software development is very difficult, as it relies on coders to contribute to the code without pay, or to find alternative sources of funding that may raise conflict of interest questions. In this section, I explore how relying on the traditional open-source software development model to

fund public blockchains exposes them to the operational risk of inadequate attention to software maintenance and development, or to particular interests shaping the trajectory of these public structures. This risk is problematic for any public blockchain that serves as the backbone of financial market infrastructure (or any other critically important public system).

As mentioned earlier, one of the celebrated attributes of open-source software is that those who develop the software code generally do so without compensation. Developing free open-source software is seen as an altruistic or reputation-enhancing activity among the coding community, and is often done by software developers outside of their regular paid employment. This is part of the ideology of the open-source software movement, and it has been successful with many types of software.

There has been a slowly dawning realization, however, that this funding model may be a bad fit for critically important software. Following the 2014 discovery of the catastrophic Heartbleed bug in Open SSL (an open-source software that runs a key security layer of the Internet), a group of technology companies formed the Core Infrastructure Initiative to better support the development of critical open-source software projects. Many open-source software projects have only a few active developers, when a much more substantial dedicated team of coders is needed to adequately maintain the software (Wheeler and Khakimov, 2015). Inadequate attention to the code over time increases the likelihood that bugs aren't seen and fixes aren't made. The Core Infrastructure Initiative is raising funds from its members to pay developers on various open-source projects that are deemed to have a critical need. Mozilla, a prominent company that maintains certain open-source software like the Firefox web browser, recently formed the Secure Open Source ('SOS') project to provide funds to increase the security of selected open-source projects. This initiative grew out of a 2015 Mozilla research project that involved surveying cybersecurity experts about key threats to cybersecurity. The report for the project noted that

> *"Participants saw the funding of security audits of critical open source projects as a key unresolved and priority issue in cybersecurity policy. Indeed, funding for free and critical open source projects emerged as an interesting outlier in becoming the one issue perceived by all as both highly desirable and feasible in a government cybersecurity policy agenda."*
>
> ***(Francois et al., 2015, p. 15)***

Bugs continue to be found in critical open-source projects, including the critical vulnerability termed "Dirty Cow" discovered in the Linux kernel in October 2016.

The open-source software funding dilemma plagues the software development process for public blockchains as well. When Bitcoin was created as free open-source software

by the mysterious "Satoshi Nakamoto" back in 2008/2009, it was of little if any significance to the public. Beginning with a community of one (the creator), it gradually spread through a group of early adopter coders, spending years wandering in the wilderness before it gained widespread attention around 2013. And the cryptocurrency exchanged on the Bitcoin blockchain had little value for a very long time, only gradually moving from a few cents per bitcoin to a few dollars, to its explosion in value in 2013. Thus, for the first several years of its life, Bitcoin was a low-stakes project, a game for the early participants in the system. It was fine for the early coders to work on the software as a hobby because there was little money at stake for them or anyone else. No one would lose much if the system failed altogether. It was just a really interesting experiment.

The stakes changed dramatically once more of the public became aware of Bitcoin and began to see its usefulness. And, as speculators entered the market and the mining sector professionalized from one guy with a computer in his bedroom to vast server farms strategically placed around the world, the stakes continued to increase. Suddenly, it mattered a great deal if there was a bug in the code, or if the software had not been optimized to run most efficiently. The software had to run smoothly 24/7, and coders had to respond to crises on an emergency basis in this now mission-critical system. Unsurprisingly, it became impossible for key developers to run an always-on mission-critical system as an unpaid hobby. Seeing the need for dedicated attention to the code, companies within the Bitcoin ecosystem (e.g., BitPay, Blockstream) began paying some core developers. Several non-profits (Bitcoin Foundation, MIT) also stepped up to fund the developers.

Public blockchains that have been introduced since Bitcoin gained mainstream recognition do not have the same chance to make unnoticed mistakes in their youth. They are potentially high-stakes from the day they are launched, as they purport to facilitate the exchange of value for members of the public. This means that expecting developers to run these systems for free in their spare time is a significant risk. Recognition of this problem has spawned creative ways to fund the software developers for Bitcoin and other public blockchains. With Ethereum, the software developers have been compensated by a "pre-sale" of ether, the currency of the Ethereum blockchain, and finances appear to be managed by the Ethereum Foundation, a Swiss non-profit set up specifically to offer financial and advisory support to the development team. With the recently released Zcash blockchain, the developers will fund themselves through the issuance of "tokens" that will trade on the blockchain (in effect, acting as an issuer of money that will be used in this particular blockchain community). A flurry of so-called "app coins" have sprung up in 2016 and 2017, funded, like Zcash and Ethereum, through the sale of tokens by developers. Called an "Initial Coin Offering" or ICO, this funding model has drawn scrutiny from securities attorneys, who warn that the issuance of these tokens without registration may violate the securities laws (Byrne, 2016).

The different approaches to the problem of funding open-source software development are creative, but more research into the implications of the funding methods, as well as their stability over the long term, is needed. As I have discussed elsewhere, these private funding structures create potential conflicts of interest in these public structures (Walch, 2015). If developers are tied to a particular funding source, there is the chance that the developers will be influenced by the people who are paying them, rather than by the interests of the people using or relying on the blockchain. Further, there is the question of whether developer funds will be around in the long term, or whether they could be cut off if the funder loses interest or it becomes politically controversial to fund a particular blockchain. This is problematic in a public structure like a public blockchain, particularly if it comes to underlie financial market infrastructures or other critical systems.

As discussed in this subsection, the use of grassroots open-source software funding methods creates operational risks for public blockchains, which negatively impact their suitability to support financial market infrastructures.

11.3.3 Fractured Networks Caused by Open-Source Software Forking Practices

The final open source practice that I consider in the context of public blockchains is that of forking software code. Anyone who has followed the blockchain world over the past several years has been made vividly aware of the possibility that a public blockchain could fork into two (or more) separate networks (and accompanying ledgers), as the Ethereum blockchain did in dramatic fashion during the summer of 2016 (and as I discuss later in this Section 11.3.3).

In this subsection, I will explain the practice of forking in open-source software, provide examples of how this phenomenon has manifested in public blockchains, and explicate the operational risks this practice raises for public blockchains.

First, what is "forking" in open source software? As Nyman noted in his recent work on the topic, "a very general interpretation of what forking means is copying an existing [software] program and distributing a modified version of it." (Nyman, 2015, p. 1.) If source code is publicly available, and can legally be changed by anyone, then open-source software code is inherently forkable. This is in sharp contrast to proprietary software, which cannot be forked by anyone other than its owner, both because the source code is not made publicly available, and because legal restrictions forbid it. But, "with open source software, one cannot *forbid* anyone from forking the code." (Nyman, 2015, p. 1, original emphasis.)

Fascinatingly, there is little academic research on code forking, with Linus Nyman's 2015 dissertation, *Understanding Code Forking in Open Source Software*, the first wide-ranging academic work to focus on this important practice. Nyman's work reveals that there are pros

www.elsevierdirect.com

and cons to the forking phenomenon, with sustainability of the software one potential plus and complexity and confusion a potential negative, "with forks spawning forks of their own that, in turn, may be forked, and forked again." (Nyman, 2015, p. 6.) Forking of significant open-source software projects, such as GNU/Linux or MySQL, has been relatively rare, but the potential outcomes that Nyman notes are significant in evaluating the operational risk profile of public blockchains. These outcomes are: (a) peaceful co-existence of both old and new software; (b) the old version of the software dies; (c) the new version of the software dies; or (d) there is a contentious co-existence of the old and new software. With public blockchains, it is not just software that forks, but entire networks, making the forking option even more consequential.

In Bitcoin, for instance, there are different types of forks that can occur through new releases of software, with varying effects on the network (bitcoin.org 2016). Hard forks are the most extreme, in that they can create competing versions of the blockchain when nodes within the network run different versions of the software. This makes it highly desirable that all (or a great majority of) nodes upgrade simultaneously to a new release (Bitcoin.org, 2016).

Although forks are part and parcel of open-source software, with public blockchains, forking appears to have much graver consequences than it does in other forms of open-source software. This is due to several unique attributes of public blockchains: the fact that they purport to actually embed and transfer value, and the fact that they purport to serve as an authoritative record of events (whatever those events may be). If these structures fragment, there is no longer a *single* authoritative data structure, but *many*, greatly undermining the technology's service as a single, reliable source of truth.

Below, I provide three real-world examples from the public blockchain world that demonstrate some potential consequences of the forking possibility: 1) the March 2013 hard fork in the Bitcoin blockchain; 2) the "block size debate" within the Bitcoin community, ongoing since summer 2015 and still unresolved; and 3) the hard fork in the Ethereum blockchain in July 2016.

11.3.3.1 March 2013 Bitcoin Hard Fork

In March 2013, a hard fork unexpectedly occurred in the Bitcoin network. This meant that two different versions of a distributed ledger were being recognized as accurate by different portions of the network. In essence, the network had fractured in two, meaning that there were also two distinct ledgers being maintained.

The cause of the fork was the use of different versions of software by the computers that operated the network. Some computers had upgraded to a new version of the software, while

others had not. This is not an unlikely occurrence in a system of disaggregated computers, whose owners cannot be compelled to adopt new versions of the code.

What to do when the Bitcoin network is split in two? Which tokens on the ledgers are bitcoins and which are something new? The existential chaos spawned by the fork was quickly recognized, and the community of software developers and transaction processors went to work to pull everyone back onto the same chain. This required getting a certain portion of the computing power to agree to use the previous version of the software so enough of the network was running the same code. Clearly, the most efficient way to achieve this would be for a few holders of big chunks of computing power to downgrade, rather than asking individuals who held a miniscule portion of the network's power. So, the core developers went after the big-enough fish, asking them to forego amounts they had been paid for performing transaction processing services on one chain, and switch to the other chain. The switchers had to *sacrifice their own earnings for the benefit of the Bitcoin network as a whole* – i.e., act altruistically for the greater good.

Through these frantic efforts, the severed networks were reunited. But, how was the surviving chain selected? Ironically, it was by the core developers, in this system that purports to have no humans in charge and to operate purely through the power of code and mathematics.

11.3.3.2 Bitcoin Block Size Debate

The Bitcoin community learned a lot from the March 2013 fork, and has been extremely skittish of a hard fork ever since. Hence, we have seen the long-running drama known in the industry as "The Block Size Debate."

The Block Size Debate is a dispute over how large a block within the Bitcoin blockchain should be. This is part of a larger discussion of how the Bitcoin software and network must change to accommodate a higher number of transactions per second, as it must if it were to become more widely used. Different factions of software developers have introduced various proposals for how to scale up the network, but the issue has remained unresolved since the summer of 2015 – around two years as of this writing. The general consensus is that a hard fork would be necessary to implement certain proposals to scale the network, making the decision fraught with risk.

Though the size of a block would seem to be a purely technical question, with the answer determined by weighing the technical characteristics of the network, the debate has revealed that it is very much a political question, with implications for the purposes and values of the Bitcoin technology generally. This is because the resolution of the question may affect how expensive it is to participate in processing the transactions on the network, meaning the network could become more and more centralized as costs to participate increased. As the

Bitcoin network was created as an expression of a particular political philosophy (libertarianism leaning toward anarchism), there is a contingent of developers who feel strongly that the network needs to remain as decentralized as possible to be true to its founding principles. Others feel that the principles of the network need to move with the times (echoing the debates over whether the U.S. Constitution should be hewn to as it was intended by its drafters, or should live and flex over time with societal changes).

The debate has been impassioned, with shifts in the cast of characters, prominent developers publicly renouncing Bitcoin, and international summits to try to reach agreement, but the network has not been able to move forward with a resolution. Diplomacy and public relations skills have become vital as developers try to persuade the large mining pools (many in China) that their solution to the problem is the best. This is because the software change cannot be implemented without a certain percentage of the computing power (provided by the miners) adopting it.

And, probably in large part because the consequences are so extreme, the debate has paralyzed the Bitcoin community. Neither side can be guaranteed to win enough votes, so the election remains unheld. Estimates of the percentage of the computing power that must adopt a new release for a Bitcoin hard fork to be deemed a success vary, but the July 2016 Ethereum hard fork (discussed below) has revealed that even a small number of holdouts can result in a competing blockchain.

In some ways, the situation is similar to the inertia that grips major social programs such as Medicare or Social Security. There is general agreement that significant change is needed to these programs, but the change is difficult to push through, in part because the transition will be so difficult. Here, the consequence is that any real change to the software can completely shatter the system into split chains, making it as fragile as a brittle set of bones.

11.3.3.3 July 2016 Ethereum Hard Fork

A third example of the forking risk played out during the summer of 2016 with a controversial hard fork of the Ethereum public blockchain.

The saga began with the creation of the DAO, a "decentralized autonomous organization" built on top of the Ethereum blockchain. Designed as an automated venture capital fund for blockchain investments, the DAO drew around $150 million in investments, but was hacked shortly after its launch, resulting in the transfer of $60 million of ether (the currency of the Ethereum blockchain) to its attacker. As the DAO's premise was that it was "unstoppable code" with which no humans could interfere, the Ethereum core developers were faced with two undesirable options: (a) do nothing about the hack because it was merely an exploit of

the software code every investor in the DAO had agreed to, creating a black eye for the technology, and potentially opening Ethereum and DAO coders up to lawsuits; or (b) issue a new release of Ethereum software that would remedy the theft by taking back the hacked ether, undermining the Ethereum blockchain's claims to be immutable and demonstrating the centralized power possessed by the core developers.

Ultimately, the core developers decided to recommend the hard fork, which required them to persuade the miners of the Ethereum network to adopt the newly-released software. They persuaded most, but not all, to upgrade to the new software. The end result was that Ethereum split into two separate blockchain networks: (a) the Ethereum network that adopted the new software release, and (b) the Ethereum network that did not (now known as Ethereum Classic). Each now has its own set of core developers and miners, and seems to operate independently from the other. These blockchains are identical up to a certain point, and then diverge in content, which means that any system built atop the Ethereum blockchain prior to the fork had to make a decision about which blockchain to remain on.

And, as one might expect after the Ethereum developers' intervention, the question of whether a public blockchain is or should be immutable has become a hot topic in blockchain circles.

11.3.3.4 51% Attack Risk

Finally, the forking risk is complicated further in public blockchains through the 51% Attack risk. Public blockchains, as currently structured, are vulnerable to the risk that participants in the transaction processing (mining) network could monopolize decisions about the path of the network, including potentially adopting new forms of software, revising previous entries on the blockchain, or preventing new entries from selected (or any) parties from being entered on the blockchain. This is because whatever 51% of the transaction processing network decides to do, is done, as the networks run through majority rule.

The vulnerability of a network to a 51% attack can increase immediately following a fork, as the computing power previously devoted to the single 'parent' network becomes split between the two 'child' networks. This means that less computing power is needed to attack each of the surviving networks. This played out in the immediate aftermath of the July 2016 Ethereum hark fork, with a threat by a miner to attack the Ethereum Classic network (Quentson, 2016).

11.3.3.5 Lessons Learned

The forking-related events described above reveal a number of important truths about public blockchains, and in this subsection, I reflect on what these episodes can teach us.

www.elsevierdirect.com

First, the 2013 fork in the Bitcoin blockchain demonstrates that new software releases for public blockchains can lead to fractured networks. A fork into separate blockchains can happen when a new release is incompatible with earlier releases, and, because there are no forced software updates in a public network, there is no way to guarantee that all members of the network will move to the new version of the software in a timely manner. In part, fear of a forked network is driving the paralysis of Bitcoin in the never-ending block size debate.

Second, the 2013 Bitcoin fork also reveals that rejoining forked blockchains may require human coordination (amongst the developers and the miners), as well as a willingness on the part of certain miners to sacrifice their earnings on one blockchain as part of rejoining the other blockchain.

Third, both the 2013 Bitcoin fork and the July 2016 Ethereum Hard Fork show that the core developers of public blockchains wield significant power in identifying and remedying a fork, in that they can coordinate communications within the mining network, and influence which chain survives (although the existence of Ethereum Classic shows they cannot necessarily eliminate a competing chain).

Fourth, the Bitcoin block size debate demonstrates how the risk of a forked network can paralyze a public blockchain, potentially leaving significant problems with the code unsolved because the appropriate solutions are disputed. Certain miners in the Bitcoin network have emerged as holdouts on various proposals, indicating how difficult it is to force consensus on a controversial software change.

Fifth, the July 2016 Ethereum Hard Fork shows that events related to processes built on top of public blockchains can influence decisions about changes made to the underlying blockchain software itself. The DAO's problems were not a problem with the Ethereum blockchain, but with the DAO's code, yet led to a hard fork in the Ethereum blockchain through a new Ethereum software release that essentially erased the DAO theft. This means that disparate applications and processes built upon a public blockchain may be impacted by decisions made by other applications built on that blockchain, in addition to decisions made about the underlying blockchain itself. In the DAO episode, other applications built on the Ethereum blockchain were affected by Ethereum's hard fork, even though the fork was driven by events associated solely with the DAO.

Sixth, the DAO hack and the resulting Ethereum hard fork are reminders that our human imperfections manifest in the software code that we write. Many have suggested that software code can automate governance, yet humans cannot write flawless code, meaning that human interventions will remain necessary even with automated technologies. Because we cannot predict the future perfectly, there will always be risks we cannot anticipate, so our governance

systems must maintain at least a hint of flexibility, much as legal contracts and laws themselves are amendable to fix errors or adjust to new circumstances.

Seventh, the Ethereum hard fork and the ongoing existence of Ethereum Classic demonstrate that competing blockchains can result from a hard fork. This phenomenon raises many questions, including practical ones such as which of the splintered chains to recognize and treat as legitimate, and how legal rights and liabilities tied to processes built on top of the parent chain play out when the parent chain splits in two. For instance, which series of trading records is legitimate, when there are suddenly two networks? Given that forks can spawn forks can spawn forks (*ad infinitum*), this could become rather complicated to manage, with each fork raising potentially contentious legal and economic issues. The forking of a blockchain network is analogous to a spin-off of a company, which is an enormously complicated process requiring careful attention to details to ensure that rights and obligations are appropriately defined and separated. Thus, any systems built atop public blockchains, including financial market infrastructures, may have these complexities sprung on them at any time through hard forks, greatly reducing any control these systems have over their risk exposures.

Eighth, all of the learnings I have described here cumulatively point to how public blockchains magnify normal software risk for processes built on them, and would do the same for any financial market infrastructures that relied on them. This is because public blockchains attempt to yoke their participants together in ways that other software does not – the *chain* of blockchain technology binds its users as well as the data stored in the ledger.

At a fundamental level, blockchain technology's benefit is that it keeps everyone in the network on the same (metaphorical) page. Each person has a real-time, correct version of the shared ledger. For the system to continue to have value, everyone must remain on the same page. Running the software and participating in the network means that one is committing to staying on the same page as other network participants. (Thomas (2016) similarly explores the problems raised by maintaining a shared state in blockchains.) A 'single-member blockchain' is an oxymoron, as a blockchain is inherently a group activity, intended to memorialize the relevant actions of its participants.

With the possibility of software forks inherent to open-source software, a public blockchain's network cohesion (and entire value proposition) is threatened every time a non-backwards-compatible software release is proposed and unevenly adopted by the network. Each proposal for a hard fork is analogous to calling for a binding referendum on secession from the blockchain, with votes cast through the choice of upgrading to the new software release (or not). Continuing with the real-world referendum analogy, if one is in the minority of computing power that chooses not to adopt (vote for) the new release, one has essentially seceded from the blockchain. Suddenly, those on the left-behind chain have to find their own resources (developers, miners, etc.) to continue to function, just as Ethereum Classic has had to. So,

www.elsevierdirect.com

each proposed hard fork is incredibly high-stakes, as evidenced by the agonizing Bitcoin block size debate.

Although the open-source software model has been highly successful in many instances, the forking possibility may make it unsuitable for public blockchains, at least if these blockchains undergird financial market infrastructures or other important societal systems. When we purport to embed actual value or records of group events in blockchain technology, it becomes qualitatively different from other software. Although my theory about this phenomenon is still taking shape, as I have explained here, I believe it has to do with tying the participants in the network together for every step that is taken. Those who break free of the chain must be willing to build a new system for themselves, exposing systems built atop the parent chain to these shifting foundations.

11.4 Reflections

This chapter seeks to contribute to the discussion of the risks that certain practices common to open-source software raise for public blockchains. In this chapter, I have focused on their potential role as the technology undergirding financial market infrastructures, whose uninterrupted operation is critical for global financial stability.

The reliability and certainty that the financial sector sees in blockchain technology is undermined in public blockchains by the use of traditional grassroots open-source software development processes, including informal governance, problematic funding, and the potential for software forks. These practices create operational risks for public blockchains, making them less solid than they are often said to be.

Of course, each public blockchain has its own particular characteristics, and thus a different overall risk profile. All share the exposure to forks, as that is an inherent characteristic of open-source software. Some may have more or less structured software development methods, and some have formalized the funding of software development through a non-profit foundation or through the issuance of a percentage of the applicable cryptocurrency to the founding development team. Each of these choices affects where the blockchain falls on the risk spectrum.

However, even with various tweaks to each of the practices outlined in this paper, public blockchains operate very differently from how we expect critical infrastructures to. As demonstrated with the regulations for financial market infrastructures, clear governance, comprehensive risk management, and identifying and mitigating operational risks are essential to managing these important structures. And, as outlined in Section 11.3 of this chapter, the grassroots open-source software practices associated with public blockchains are diametrically opposed to the more controlled practices we expect in high-stakes areas.

www.elsevierdirect.com

In a broader sense, the analysis in this chapter suggests that it may be time for a rethink about the role of grassroots open-source software in critical infrastructures outside the blockchain technology setting. Open-source software performs many infrastructural functions in our society, including processes crucial to the operation of the Internet. As with Bitcoin, practices that worked fine when the project was small-scale and low-stakes may be inappropriate for large-scale, high-stakes projects. We are discovering now that many critical open-source software projects, undergirding vital pieces of the Internet, are understaffed, underfunded, and insecure. We may be in the process of discovering why these revolutionary processes (loosely structured governance, unpredictable funding, forking as an option) have not been widely adopted for critical public practices. It may be that we just can't be comfortable enough with them to count on them in a crisis. Analogously, volunteer fire departments are relatively common in small towns, but cities pay fire departments to fulfill this important public function – the scale of the systems seems to dictate a more formal structure being needed in the more populous cities.

To open-source software devotees, these observations may be viewed as fighting words. Open-source is as much an ideology as it is a technical practice, and any critique of it inspires passionate defense by its adherents. The superiority of open-source software to proprietary software—pretty much regardless of the task or setting—is treated as dogma by open-source advocates, and, as critics of religion have long seen, questioning dogma can be dangerous.

Yet we cannot fully evaluate our practices unless we are able to question our most basic assumptions. The courage to question existing practices gave rise to Bitcoin itself, and continued questioning and critique will help us to responsibly use the underlying blockchain technology. Indeed, our infrastructures depend on it.

References

Arnold, M., 2016. Accenture to unveil blockchain editing technique. Financial Times.

Bank for International Settlements Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions, 2015. Consultative Report: Guidance on cyber resilience for financial market infrastructures. Available from: http://www.bis.org/cpmi/publ/d138.pdf. [Accessed 29 November 2016].

Bank for International Settlements Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, 2012. Principles for Financial Market Infrastructures. Available from: http://www.bis.org/cpmi/publ/d101a.pdf. [Accessed 30 November 2016].

Bitcoin.org, 2016. Bitcoin Developer Guide. Available from: https://bitcoin.org/en/developer-guide. [Accessed 4 December 2016].

Burton, B., Willis, D., 2016. Gartner's 2016 Hype Cycles Highlight Digital Business Ecosystems. Available from: www.gartner.com. [Accessed 30 November 2016].

Byrne, P.J., 2016. Against Tokens (and Token Crowdsales). The Back of the Envelope (a blog). Available from: https://prestonbyrne.com/2016/08/12/against-crowdsales/. [Accessed 1 December 2016].

Carney, M., 2016. Enabling the FinTech Transformation: Revolution, Restoration, or Reformation? (Speech that was to have been given by Mark Carney, Governor of the Bank of England at the Lord Mayor's Banquet for Bankers and Merchants of the City of London at the Mansion House, London). Available from: http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf. [Accessed 29 November 2016].

DTCC, 2016. Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape. Available from: http://www.dtcc.com/news/2016/january/25/blockchain-white-paper. [Accessed 29 November 2016].

Eha, B.P., 2016. MUFG Aims to use bitcoin to improve cross-border payments. American Banker.

Federal Reserve, 2016. Policy on Payment System Risk. Available from: https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf. [Accessed 30 November 2016].

Francois, C., et al., 2015. The Mozilla Cybersecurity Delphi 1.0: Towards a User-Centric Policy Framework. Available from: https://blog.mozilla.org/netpolicy/files/2015/07/Mozilla-Cybersecurity-Delphi-1.0.pdf. [Accessed 1 December 2015].

Giancarlo, J.C., 2016. Regulators and the Blockchain: First, Do No Harm (Special Address of CFTC Commissioner J. Christopher Giancarlo Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium). Available from: http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-13. [Accessed 29 November 2016].

Kaminska, I., 2016. Blockchain and the holy real-time settlement grail. Financial Times [online]. Available from: https://ftalphaville.ft.com/2016/02/26/2154510/blockchain-and-the-holy-real-time-settlement-grail/. [Accessed 1 December 2016].

Kiran, M., Stannett, M., 2014. Bitcoin risk analysis. NEMODE. Available from: http://www.nemode.ac.uk/wp-content/uploads/2015/02/2015-Bit-Coin-risk-analysis.pdf. [Accessed 1 December 2016].

Nyman, L., 2015. Understanding Code Forking in Open Source Software: An Examination of Code Forking, Its Effect on Open Source Software, and How It is Viewed and Practiced by Developers. Ph.D. Thesis, Hanken School of Economics.

Perlroth, N., Corkery, M., 2016. Details emerge on global bank heists by hackers. The New York Times. Available from: http://www.nytimes.com/2016/05/14/business/dealbook/details-emerge-on-global-bank-heists-by-hackers.html?_r=0. [Accessed 29 November 2016].

Peters, G.W., et al., 2014. Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: an operational risk perspective. arXiv.org. Available from: https://arxiv.org/ftp/arxiv/papers/1409/1409.1451.pdf. [Accessed 1 December 2016].

PWC, 2016. Bank of England FinTech Accelerator partners with PWC on distributed ledger Proof of Concept. Available from: http://pwc.blogs.com/press_room/2016/06/bank-of-england-fintech-accelerator-partners-with-pwc-on-distributed-ledger-proof-of-concept-.html. [Accessed 29 November 2016].

Quentson, A., 2016. Miners to attack ethereum classic after poloniex's listing. Cryptocoins News. Available from: https://www.cryptocoinsnews.com/miners-attack-ethereum-classic-polonixs-listing/. [Accessed 1 December 2016].

Rapier, G., 2016. Yellen reportedly urges central banks to study blockchain, bitcoin. American Banker.

Rizzo, P., 2016. Linux, IBM share bold vision for hyperledger project, a blockchain fabric for business. CoinDesk. Available from: http://www.coindesk.com/linux-ibm-hyperledger-blockchain-business/. [Accessed 29 November 2016].

Thomas, S., 2016. The Subtle Tyranny of Blockchain. Available from: https://medium.com/@justmoon/the-subtle-tyranny-of-blockchain-91d98b8a3a65#.l4jt4z2ze. [Accessed 1 December 2016].

Walch, A., 2015. The bitcoin blockchain as financial market infrastructure: a consideration of operational risk. NYU Journal of Legislation & Public Policy 18 (4), 837–893.

West, J., O'Mahony, S., 2008. The role of participation architecture in growing open sponsored open source communities. Industry and Innovation 15 (2), 145–168.

Wheeler, D.A., Khakimov, S., 2015. Open Source Software Projects Needing Security Investments. (White Paper of the Institute for Defense Analysis and the Linux Foundation). Available from: https://www.coreinfrastructure.org/sites/cii/files/pages/files/pub_ida_lf_cii_070915.pdf. [Accessed 1 December 2016].

White, M.J., 2016. Opening Remarks at the Fintech Forum. (Public Remarks delivered by SEC Chair at SEC Fintech Forum). Available from: https://www.sec.gov/news/statement/white-opening-remarks-fintech-forum.html. [Accessed 1 December 2016].

Notes

1. In this chapter, I distinguish between "grassroots" open-source software ("community-developed," Nyman, 2015, p. 24) and "corporate" open-source software. The distinction between the two is generally that "grassroots" open-source software emerges organically from and is maintained by a community of software developers (sometimes with the assistance of a purpose-built non-profit foundation), while a "corporate" open-source software project is created, owned, and controlled by a formal business entity, with some sort of participation from the larger developer community (Nyman, 2015).
2. Dave Birch of Consult Hyperion, Izabella Kaminska of the *Financial Times*, Matt Levine of *Bloomberg View*, and Steve Wilson of Constellation Research have been among the few prominent critics of the hype surrounding blockchain technology.
3. Since September 2014, the CPSS has been known as the Committee on Payments and Market Infrastructures.
4. I include Principle 2 regarding governance because poor governance can generate the human problems that are part of the wider concept of operational risk.

www.elsevierdirect.com

CHAPTER 12

Blockchain Architectures for Electronic Exchange Reporting Requirements: EMIR, Dodd Frank, MiFID I/II, MiFIR, REMIT, Reg NMS and T2S

Gareth W. Peters[#] , **Guy R. Vishnia**[##]

Contents

Executive Summary 273

Structure of Paper 274

12.1 Introduction to Modern Electronic Exchanges and Networks 274

12.1.1 Limit Order Books 275

12.1.1.1 Lit (Visible) Limit Order Book *275*

12.1.1.2 Dark (Hidden) Limit Order Book *276*

12.1.2 Regulated Markets and Primary Exchanges 277

12.1.3 Multilateral Trading Facilities (Alternative Trading System) 278

12.1.4 Organized Trading Facilities and Swap Execution Facilities 279

12.1.5 Broker Crossing Networks and Systematic Internalizers 281

12.1.6 Dark Pools 282

12.1.7 Hybrid Trading Systems 283

12.2 Evolution of Equity, Commodity, Currency and Derivatives Exchange Reporting and Transparency Regulations 284

12.2.1 Global Regulatory Authorities and Recent Electronic Market Regulations 284

12.2.2 MiFID I 287

[#] QRSLab details are available at http://garethpeters78.wixsite.com/garethwpeters.
[##] http://www.itg.com.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00012-7
Copyright © 2018 Elsevier Inc. All rights reserved.

12.2.2.1 Key Components of MiFID I 288
12.2.3 EMIR 291
12.2.3.1 Scope of EMIR 292
12.2.3.2 EMIR Reporting Information: LEI, UTI, and Required Data Fields 293
12.2.4 CFTC and Dodd–Frank 295
12.2.4.1 Reporting Specifications of the CFTC Dodd–Frank Regulations 297
12.2.5 MiFID II and MiFIR 298
12.2.5.1 Brief Summary of MiFID II and MiFIR Trading Venues 299
12.2.5.2 Transparency & Transaction Reporting Under MiFIR 300
12.2.5.3 Dark Caps and Large in Scale Waiver (LIS) 301
12.2.5.4 Record Keeping 302
12.2.5.5 Standardization of Reporting Under MiFID II and MiFIR 302
12.2.6 REMIT 303
12.2.7 Reg NMS 303
12.2.8 Settlement Under Target2 Securities (T2S) and Central Securities Depositories Regulation (CSDR) 304
12.3 The Role of Blockchain Technology in Electronic Exchanges 306
12.3.1 Brief Overview of Some Basics of Blockchain and Related Technologies 308
12.3.1.1 Permissioned and Permissionless Blockchains 310
12.3.1.2 Smart Contracts on Blockchains May Provide Automated Oversight on Transparency and Reporting 311
12.3.2 Overview of Blockchain Emerging in Electronic Exchanges 313
12.4 Blockchain Architecture for Order Record Keeping and Transaction Reporting 315
12.4.1 Entity Identification Requirements 316
12.4.1.1 Legal Entity Identifier (LEI) and User Identifiers 317
12.4.1.2 Entity Identification Blockchain 318
12.4.2 Order Record Keeping and Auditing With Blockchain 320
12.4.2.1 Architecture and System Design 320
12.4.2.2 Centralized Governed Auditing Blockchain 321
12.4.2.3 Decentralized Trading Entity Audit Chain 323
12.5 Conclusions 324

References 324

Notes 327

Executive Summary

Several international electronic primary financial exchanges have begun to announce they will explore the adoption of blockchain technology in their trade processing and reporting for execution and clearing. Therefore, in this work we will begin by providing a detailed discussion and overview of the new exchange regulations appearing in different jurisdictions around the world, including EMIR, Dodd–Frank, MiFID I/II, MiFIR, REMIT, Reg NMS and T2S. We will discuss their key features, specifically in regard to transparency reporting and trade/transaction reporting requirements. To achieve this we first discuss the emergence of a multitude of different trading venues that have arisen under the fragmentation directives for each asset class: equities, commodities, derivatives and currency. We highlight how each fits into this universe of different market and processing venues both primary, secondary, dark and lit and OTC.

Having overviewed the current status of regulatory requirements for reporting and the massive data sets such regulation will generate, discussing along the way the significant challenges faced by firms and market participants in meeting such requirements in an automated manner, we then develop and explain a solution based on blockchain architectures. This solution will be developed to specifically handle three key aspects of transparency and reporting requirements that will be universal in applicability in both UK, Europe and U.S. regulations.

To achieve this we will comment on the different emerging architectures and features that are being developed in a range of different blockchain technologies. This will include details on different forms of blockchain technology including: Permissionless blockchains, where anyone can participate in the verification process, i.e. no prior authorization is required and a user can contribute his/her computational power, usually in return for a monetary reward; Permissioned blockchains, where verification nodes are preselected by a central authority or consortium; Public blockchains, where anyone can read and submit transactions to the blockchain; and Private blockchains, where this permission is restricted to users within an organization or group of organizations. We explore these different architectures and features offered in the context of transaction reporting as well as market and trading event auditing.

We suggest a governed solution for the maintenance of secure sensitive personal identity data from market participants via a permissioned blockchain controlled by the regulator or

www.elsevierdirect.com

a consortium of market participants. Then by utilizing the latest blockchain frameworks such as Enigma we can facilitate the required transparency and reporting aspects that require access to these identities when performing pre- and post-trade reporting as well as for auditing. In this regard we also present a use case for immutable event auditing required by latest EMIR regulation in both centralized and decentralized ways. Finally we show how both architectures can work together in order to give the regulator a reliable, fast and easy solution for retrieving specific auditing data and combining it with relevant identification details.

Structure of Paper

The paper is structured as follows. In Section 12.1, an overview of modern electronic trading venues is discussed. In Section 12.2 a detailed discussion on regulations affecting electronic exchanges on the buy and sell side in major jurisdictions in the world is discussed, including: MiFID I, EMIR, Dodd–Frank, MiFID II and MiFIR, REMIT, Reg NMS as well as T2S and CSDR. Then in Section 12.3, an explanation of the role that blockchain technology will play in electronic exchanges is discussed, including an overview of key features of blockchain technologies and a discussion on what is emerging in electronic markets adoption of blockchains. In Section 12.4 we propose novel developments of blockchain architectures for transaction reporting which includes both the use of blockchain for identity auditing and trade reporting audits over the trail of transactions. Section 12.5 is a conclusion.

12.1 Introduction to Modern Electronic Exchanges and Networks

In discussing how blockchain architectures can be used to facilitate exchange and transaction transparency as part of new exchange regulations it will be important to first understand the current landscape of electronic exchanges. There are a number of trading venues possible to modern traders. A trader can choose to execute their orders in more than one venue, and in more than one venue type. A trader can choose to target all available venues, or only a subset of these venues based on his preferences, trading cost or other motivation. In addition there are new regulations that are emerging in different jurisdictions that are changing these venue options for traders. In this section we will first describe current venue types and then we will overview the changing nature of the securities exchange regulations in different parts of the world. Following this discussion, we then explore how blockchain can aid in meeting

www.elsevierdirect.com

these costly and challenging new regulation requirements, especially when it comes to pre- and post-trade reporting requirements.

There are numerous ways that one can go about classifying markets in which traders can operate and this can also depend on the asset class. One broad classification often adopted in practice and under regulations (Moloney et al., 2002) is to consider the distinctions between: Regulated Markets (RMs); Multilateral Trading Facility (MTFs); Organized Trading Facilities (OTFs); Swap Execution Facilities (SEFs); Designated Contract Markets (DCMs); Broker Crossing Networks (BCNs); Dark Pools (DPs) and Customized Liquidity Pools (CLPs), and the emerging area of Multilateral systems (MS).

Within these numerous categories of exchange venues it is useful to introduce some common terminology used. We refer to a multilateral as a venue that acts as a platform which brings together multiple third-party orders as opposed to bilateral markets in which trading is between the venue and the client.

We refer to non-discretionary markets as those in which trades are executed according to the venue's preset rules or parameters and the venue does not intervene as opposed to discretionary markets in which trading, and access to the platform, is at the venue's discretion.

Before continuing to detail different types of venues, it will be useful to explain briefly a key quantity in modern electronic exchanges, the Limit Order Book (LOB).

12.1.1 Limit Order Books

The Limit Order Book (LOB) can be viewed as a list of the willingness of people to buy or sell a certain quantity of a certain asset at a certain price. When a buy and a sell prices match, we have an execution (trade). Sizes do not have to match on a trade, and one part of the bargain can remain with residuals, see discussions in Gould et al. (2013), Richards et al. (2015), Panayi et al. (2015) and Panayi and Peters (2015). In modern market places one common distinction that has arisen for different types of LOB is between lit and dark books or sometimes referred to as lit and dark liquidity.

12.1.1.1 Lit (Visible) Limit Order Book

Understanding the order book dynamics and properties can give the trader, investor, and regulator in-depth knowledge of the current market status and can help in either earning significant gains or preventing markets from being gamed. Different markets use different trading systems and the regulation differs between the market and exchanges, but the basic mechanism or the Limit Order book is the same for all.

www.elsevierdirect.com

We can look at the order book as a two-price queue system, one for buy orders and one for sell orders: each position at the queue is called a level, i.e. the first in the queue on each side will be level 1, second will be level 2, etc. On each level there are also queues noting when the order was inserted to the level. This is called the depth of the level.

This data in the Lit Order books is visible to market participants usually by subscribing to a venue feed, whether directly or via a data provider such as Thompson Reuters or Bloomberg.

The formal definitions of the best bid, ask and the midpoint are:

BestBid = the maximum price a participant is willing to buy X amount of shares at a certain point in time.

$$BestBid = Max(P_b 1 \ldots P_b k) \tag{12.1}$$

BestAsk the minimum price a participant is willing to sell X amount of shares at a certain point in time.

$$BestAsk = Min(P_a 1 \ldots P_a k) \tag{12.2}$$

Mid price – the midpoint between the best bid and the best ask. It does not have to fall under the tick size rules.

$$Mid = (BestAsk + BestBid)/2 \tag{12.3}$$

12.1.1.2 Dark (Hidden) Limit Order Book

A Dark Limit Order Book (DLOB) is, as its name states, not publicly visible, i.e. the orders that reside within it are not public and no one knows at any point which entries and what sizes / prices are currently in the dark pool order book. In a DLOB there is no best Bid/Ask and volume being published, that is trading orders/interest are not disclosed to the market publicly. Only once a trade occurs in the dark pool will it be published and then visible to the public (via Boat platform for example[1]).

The Orders that reside in the DLOB are adhering to client limit prices and to queue/size priority as per venue rule book, but no one besides the sender of the order to the dark pool knows about this order until it is executed. In addition, it is also the case that removing or canceling an order from the DLOB is also not visible to the outside world. See discussions on such venues in Degryse et al. (2008) and Gresse (2015).

www.elsevierdirect.com

12.1.2 Regulated Markets and Primary Exchanges

Under such a classification an RM can be thought of as market place that is typically managed by the market operator who does not run this market primarily as an investment activity. In such markets they typically involve non-discretionary execution systems. In this setting non-discretionary refers to the fact that they are typically execution-only services that allow clients to make their own investment decisions and provide purely a platform for them to carry out trades to fulfill their investment decisions. Examples of such RMs include the Primary Exchanges (PEs) of each country. Typically such RMs are associated with formal, organized markets, including traditional stock exchange PEs but also newer multilateral platforms.

The PEs are the first and main trading platform in a country. The first equity exchange in Europe dates from around 1650 and most others have a long history of trading. In 1986 the London Stock Exchange (LSE) moved to an electronic platform and started the European move of replacing the traditional on-the-floor trader and opening new ways to settle and reconcile executions. In the beginning of the electronic trading period each exchange used its own platform but today it is reconciled into three or four major exchange providers.

Primary exchanges typically offer lit Limit Order Books (LOBs), which means that the best bid and ask prices and volumes (first level of the book) are published for any subscriber, and also deeper levels of the book are available for subscriptions. Levels of the book proceed in tick size, i.e. specific predefined sizes which may be different per stock based on its traded value.

In such RMs the market is typically informed of levels of trading interest pre- and post-trade. It is well documented that such forms of electronic trading are involved in price-setting since the active and timely disclosure of trading interest supports the development of a wider price formation. As a consequence, these RMs are offering an important market function for investors and consequently many transparency rules which require the disclosure of pre-trade bid/offer prices and post-trade trade price, volume and time information are required to be satisfied.

In contrast to RMs and PEs there are numerous other types of electronic market venues that have emerged in recent years. In general prior to recent regulations for instance in Europe, known as the Markets in Financial Instruments Directive 2004/39/EC (MiFID), to be discussed below, there was only a second type of venue which was associated with investment firms and brokers who provided discretionary execution services which were previously classified as Over the Counter (OTC) services. In such settings, they typically ran as client execution services that were bilateral between clients and a broker's proprietary order book or bilaterally between clients and a "crossed" book constructed from other clients orders. As these services became automated in nature, it removed the traditional client facing role of a

broker, consequently it was perceived to also remove the fiduciary duties typically imposed on client facing investment firms with respect to best execution obligations. To address this potential issue new regulation was developed to rectify this challenge and it will be discussed further below. We mention briefly that this was the background to the emergence of MiFID which was primarily aimed at the promotion of competition in such trading venues in order to improve innovation, price competition and investor choice, and to further support the transparency and efficiency of the competitive trading marketplace.

12.1.3 Multilateral Trading Facilities (Alternative Trading System)

MTFs were introduced in 2007 when MiFID regulation came into force, opening the traditional primary exchange-only execution market to competition which increased the transparency of the markets as well as making them fragmented.

An MTF is a trading system that facilitates the exchange of financial instruments between multiple parties. Multilateral trading facilities allow eligible contract participants to gather and transfer a variety of securities, especially instruments that may not have an official market. Typically an MTF is managed by either a market operator or investment fund which runs the operation as an investment service. MTFs are also typically non-discretionary execution environments.

These facilities are often electronic systems controlled by approved market operators or larger investment banks. Traders will usually submit orders electronically, where a matching software engine is used to pair buyers with sellers. However, until recently there have been few requirements made regarding conduct of business regulations.

These venues can be considered as a primary exchange in many ways, they offer pre- and post-trade transparency (publish bid–ask) and users can choose to target directly these venues. They often offer better rates and higher speed than the primary exchanges.

Security needs to be listed on the MTF and its trading universe will be a subset of the primary, where each MTF has its own universe as it can choose whether to list or not list a certain stock.

As a result of MiFID I in 2007, many new MTFs were opened in Europe, but over time they consolidated into three big ones: Chi-X (established 2007) – The first MTF to launch in Europe, Bats (established 2008) operated by the US-based BATS Global markets, and Turquoise (created by nine major investment banks in 2008). Chi-X and Bats were eventually combined in 2011, see discussions in Riordan et al. (2011) and BATS (2011).

July 29, 2016 | Download this day as CSV | Download from date | Options: Switch to % values Show More By Index Auctions: Included Excluded

Notional Value Summary | Volume Summary

Today | 5 Day Avg | MTD

Bats

	London	Paris	Frankfurt	Madrid	Zurich	Amsterdam	Market*	% of Mkt	Today % of Mkt
Lit Order Books									
Bats Europe	€2,686,510,899	€1,244,702,622	€1,502,126,036	€486,881,104	€903,446,803	€586,143,839	€8,925,142,463	20.54%	21.95%
CXE Book	€1,867,335,862	€981,737,684	€1,153,944,316	€389,543,282	€422,400,164	€489,472,545	€6,328,289,650	14.56%	15.98%
BXE Book	€819,175,037	€262,964,938	€348,181,720	€97,337,822	€481,046,639	€96,671,294	€2,596,852,813	5.98%	5.97%
LSE Group	€6,130,003,306						€8,781,118,117	20.21%	18.99%
London	€6,130,003,306						€6,130,126,521	14.11%	10.97%
Milan							€2,650,991,597	6.10%	8.01%
Euronext		€3,524,075,589				€1,624,125,123	€5,625,307,175	12.95%	14.41%
Turquoise	€1,549,188,137	€752,469,858	€855,099,998	€234,021,349	€310,789,882	€339,002,841	€4,977,189,232	11.45%	10.72%
Xetra			€3,906,260,323				€3,906,260,323	8.99%	8.46%
SIX Swiss Exchange					€2,803,869,352		€2,803,869,352	6.45%	6.20%
Nasdaq OMX							€2,158,756,067	4.97%	4.05%
Bolsa de Madrid				€1,457,209,642			€1,457,209,642	3.35%	3.34%
Aquis	€96,524,397	€33,593,468	€58,321,038	€7,497,717	€68,099,331	€22,809,868	€381,964,255	0.88%	1.27%
Oslo							€331,890,744	0.76%	0.69%
Equiduct	€20,677,083	€95,994,368	€21,849,292	€56,116	€2,113,090	€41,383,012	€215,657,544	0.50%	0.86%
Wiener Börse							€98,157,419	0.23%	0.10%
Irish Stock Exchange							€78,850,465	0.18%	0.09%
Lit Total	€10,482,903,822	€5,650,835,905	€6,343,656,688	€2,185,665,929	€4,088,318,459	€2,613,464,683	€39,741,372,800	91.45%	91.13%

This image is a snapshot from BATs markets at URL: https://www.bats.com/.

12.1.4 Organized Trading Facilities and Swap Execution Facilities

An OTF is any facility or system designed to bring together buying and selling interests or orders related to financial instruments; however, they apply typically only to non-equities. They form a new classification of trading venue which is designed to act as a regulatory "catch all" for all organized trading that occurs away from RMs and MTFs and that is not genuinely OTC, see discussions in MaretWiki (2016) and Linklaters (2016). These venues or electronic exchanges arose primarily after MiFID II regulations, whereas under MiFID there was only a requirement of MTFs (this will be discussed in detail below).

A very general definition of an OTF is currently in place so that this type of venue can capture any facility or system that is not an MTF or RM. They will allow multiple third party buying and selling interests in financial instruments to interact in a manner that results in a contract and may be both bilateral or multilateral in nature as well as discretionary and non-discretionary, with the exception that pure OTC trading and order routing systems are excluded from the category of OTF.

An OTF can typically be managed by either the market operator or investment fund which runs the operation as an investment service. Typically OTFs are run by broker-dealers, who under new emerging regulatory proposals of MiFID II will be prevented from trading against their own capital, see Commission (2016).[2] In particular they cannot undertake dealing on

their own accounts except for illiquid sovereign debt and they can only conduct matched principal trades with client permissions. There is then naturally a discussion that is playing out regarding the liquidity that would be offered to traders in such electronic exchanges should such regulations be enacted. OTFs are discretionary execution environments. Unlike in MTFs for OTFs they have historically experienced greater regulations for investor protection, with requirements on conduct of business and best execution.

To operate an OTF there will also now be an authorization required, in that it will become a licensable activity under MiFID II and any such request for authorization as an OTF must include a detailed explanation as to why the system does not correspond to and cannot operate as a regulated market, MTF or systematic internalizer. The new OTF license will also require that they apply pre-trade and post-trade transparency requirements in the same fashion as for RMs/MTFs. (To be discussed further in context of regulations below.) In addition they will need to comply with requirements to keep data relating to orders received for five years.

Fundamentally, the OTF is the MiFID II equivalent of the US Dodd–Frank Act SEF structure, see discussion in Commission (2016a).[3] In particular OTFs are intended to be similar in scope to a SEF, where the goal of such venues is largely to bring transparency and structure to Over the Counter (OTC) derivatives trading.

In the U.S. the SEF is a venue specifically developed to clear OTC swaps under a regulated platform. According to Dodd–Frank, any swap that is "made available to trade" must do so on a DCM or a SEF Commission (2016d). The SEF can be defined as "a trading system or platform in which multiple participants have the ability to execute or trade swaps by accepting bids and offers made by multiple participants in the facility or system, through any means of interstate commerce" that is not a designated contract market, see Commission (2016c).

The structuring and main principles of how SEFs operate were left to the Commodity Futures Trading Commission (CFTC) and the U.S. Securities and Exchange Commission (SEC). The main principles were established for these venues by the CFTC which proposed in December 10, 2010 a guidance on such venues and was introduced to the Federal Register on January 7, 2011 (details will be discussed below).

Subsequent to the introduction of the SEF, the CFTC has continued to finalize several execution rules in May 16, 2013 which include 15 core principles (see Commission, 2013): Core Principles and Other Requirements for SEFs; the "made available to trade" (MAT) provision; Block trade rules; Trading and product requirements; Compliance obligations; Surveillance obligations; Operational capabilities; and Financial information and resource requirements.

These also include the requirement of registration of a SEF such that they are required under regulation to demonstrate that they meet minimum trade functionality requirements such as having a LOB, and they offer impartial access to their markets.

Note, in this context we may think of an order book as an electronic trading facility, trading system, or platform in which all market participants in the trading system or platform have the ability to enter multiple bids and offers, observe or receive bids and offers entered by other market participants, and transact on such bids and offers.

12.1.5 Broker Crossing Networks and Systematic Internalizers

A Broker Crossing Network (BCN) is a network that provides a platform for mutual funds and institutional traders to conduct transactions without revealing their identity. Such alternative trading systems (ATS) arose to allow buyers and sellers to match up and conduct transactions without going through an exchange. They have been successful in allowing traders to gain large blocks of liquidity while keeping transaction costs to a minimum, see discussion in Bloomfield et al. (2015).

A BCN is usually an internal broker system that crosses client order flows, typically using some form of proprietary capital. Until recent regulations on securities exchanges started to emerge the BCN was often reported as OTC, and was able to therefore avoid pre-trade transparency requirements. However, under new regulations taking effect, investment firms that run BCNs will have to consider the options to either set up an OTF or register their operations as what is known as a Systematic Internalizer (SI); see discussions in Urrutia (2014).

Whilst BCNs are privately run crossing networks which match flow of clients in order to execute. Systematic internalizers are doing the same but the crossing is against the SI operator capital and not vs. other clients. In general one can consider an SI as "an investment firm which, on an organized, frequent systematic and substantial basis, deals on own account by executing client orders outside RM, MTF or OTF."

Importantly, under the new regulatory changes, to be discussed in the following sections the BCNs will change in that the new forms of such venues will not be able to cross their proprietary capital with client order flow on the same platform. In addition all flows within the OTF they set up will be subject to pre- and post-trade transparency. If they move to SIs then this has the following advantages under new regulations under proposal.

For equities the changes include that SIs are likely to be more commercially attractive as they can offer minimum quote sizes at least 10% of SMS with the previously in place retail size limit removed, see Securities and Authority (2015b). In derivatives there is additional flexibility when providing access in accordance with commercial policy provided that this is objective and non-discriminatory. In addition, SIs can establish non-discriminatory and transparent limits on the number of transactions they undertake to enter into with clients for any quote.

www.elsevierdirect.com

12.1.6 Dark Pools

Dark Pools (DPs) are trading venues which offer electronically off the book block trades usually at Mid price but at the moment can also cross on the Bid and Ask. The reference price is typically taken from the primary exchange. When referring to dark pool liquidity it can be considered as the trading volume created by institutional orders executed on private exchanges and unavailable to the public. The bulk of dark pool liquidity is represented by block trades facilitated away from the central exchanges. It is also referred to as the "upstairs market," "dark liquidity," or "dark pool"; see discussion in Buti et al. (2010).

The first incarnation of dark pool liquidity arose as far back as in 1986, when electronic exchanges were not largely prevalent and pre High Frequency Trading (HFT) and hedge fund algorithmic trading. The first DP started in 1986 with Instinet offering an after hours crossing (matching of orders) at the close price of the day. This system allowed participants to execute large chunks of block trades without market impact and pre-trade transparency. Shortly after this initial DP, the following year, ITG started Posit, which offers several matching options outside of the lit LOB at predefined known intra-day times by crossing at the Mid price of the market for the lit LOB.

With the onset of electronic exchanges, the need and desire to develop DPs intensified. The need for such off the book trading facilities was motivated by opportunistic legal trading behaviors being undertaken by High Frequency Trading (HFT) market participants in the lit book RM and MTF exchanges. HFT became so pervasive it grew increasingly difficult to execute large trades through a single exchange. Because large HFT orders had to be spread among multiple exchanges, it alerted trading competitors who could then get in front of the order and snatch up the inventory, driving up share prices. All of this occurred within milliseconds of the initial order being placed.

To avoid the transparency of public exchanges that may result in predatory actions on the part of HFT algorithmic investors and to ensure liquidity for large block trades, several investment banks established private exchanges, which came to be known as dark pools. For traders with large orders who are unable to place them on the public exchanges, or want to avoid telegraphing their intent, dark pools provide a market of buyers and sellers with the liquidity to execute the trade.

Following the initial success, in 2002 ITG developed Posit Now which allowed for a continuous crossing option (matching of bid and ask), and by 2004 there were several crossing platforms available for traders such as Instinet, Liquidnet, and Millennium.

Electronic dark pools continued to gain momentum through the years and now responsible for about 8 percent of all trading in Europe for instance. This has led to much more active scrutiny from the regulator, which results in new regulatory demands as part of MiFID II.

www.elsevierdirect.com

Although considered legal, dark pools are able to operate with little transparency. Those who have denounced HFT as an unfair advantage over other investors have also condemned the lack of transparency in dark pools, which can hide conflicts of interest. The SEC has stepped up its scrutiny of dark pools over complaints of illegal front-running that occurs when institutional traders place their order in front of a customer's order to capitalize on the uptick in share prices. Advocates of dark pools insist they provide essential liquidity, allowing the markets to operate more efficiently.

Under new regulations the dark pool universe will need to support the same order types and pricing and queue priority rules as a lit exchange, but will not publish publicly their order book hence giving no view to what orders are currently reside in the dark pool. Usually it will also require a larger minimum trading size.

In particular, trade reporting will be published with the maximum allowed delay in order to reduce market impact. The dark traded are considered to be OTC (Over the Counter) and are not contributing to the electronic daily volume traded on a stock.

Due to the nature of the liquidity inside the dark pool not being visible to the outside world, there is no way to guarantee an execution in the pool. It is now being put into more regulation and caps under MiFID II, which we describe below.

12.1.7 Hybrid Trading Systems

Hybrid Trading Systems (HTSs) comprise numerous other types of specialized venues. In general they are securities exchanges that facilitate trading through a blend of an automated electronic trading platform and a traditional floor broker system. They can include many forms for instance:

- *Continuous auction order book trading system.* A system that by means of an order book and a trading algorithm operated without human intervention matches sell orders with matching buy orders on the basis of the best available price on a continuous basis. In such a setup the information required to be made public includes the aggregate number of orders and the shares they represent at each price level, for at least the five best bid and offer price levels.
- *Quote-driven trading system.* A system where transactions are concluded on the basis of firm quotes that are continuously made available to participants, which requires the market makers to maintain quotes in a size that balances the needs of members and participants to deal in a commercial size and the risk to which the market maker exposes itself. In such a setup the information required to be made public includes the best bid and offer by price of each market maker in that share, together with the volumes attaching to those prices.

www.elsevierdirect.com

- *Periodic auction trading system.* A system that matches orders on the basis of a periodic auction and a trading algorithm operated without human intervention. In such a setup the information required to be made public includes the price at which the auction trading system would best satisfy its trading algorithm and the volume that would potentially be executable at that price.

12.2 Evolution of Equity, Commodity, Currency and Derivatives Exchange Reporting and Transparency Regulations

In this section we overview the substantial changes that are taking place globally in regard to derivatives reporting and exchange traded instruments. For many years there have been some form of reporting requirements for the financial industry when it comes to exchanges. However, recent regulations have significantly enhanced the relationships between reporting obligations and securities market practice. The principal reason for these new regulations is typically stated to be an increase in risk mitigation and reduction of information asymmetries between market participants, including regulators.

After the global financial crisis of 2008 there was an international push to develop an international regulatory program which was primarily driven by the G20 and enhanced at the 2009 Pittsburgh summit. With a universal focus on the core principle of increasing transparency and reporting requirements, markets have witnessed the emergence of Dodd–Frank (Commission, 2015b), the European Market Infrastructure Regulation (EMIR) (Authority, 2016), Markets in Financial Instruments Directive (MiFID) I, II (Commission, 2016b) and Regulation (MiFIR) (Securities and Authority, 2016a), Securities Financing Transactions Regulation (SFTR) (FIA.org, 2015), and Money Market Statistical Reporting (MMSR) (Bank, 2015b), which all contain some form of reporting obligations. Before discussing in more detail reporting requirements and the role that blockchain technology may play in such requirements, we first recall some basic fundamental aspects of these various regulations to put this reporting into context and provide a scope to the significance of such reporting undertakings. We begin by briefly recalling the main governing bodies responsible for writing and enacting the regulations in some key jurisdictions.

12.2.1 Global Regulatory Authorities and Recent Electronic Market Regulations

We begin by discussing a few key regulators of the stock markets (equities markets) and mention briefly other key market regulators for commodities, swaps, derivatives, and currencies.

Regulatory Institutions

The Stock traded markets, the commodities, and currency markets are regulated and governed by different authorities across the globe, some key examples of which are mentioned briefly below by jurisdiction:

- Globally there is the International Organization of Securities Commissions (IOSCO[4]) which was established in 1983. The mandate of IOSCO is to act as the international body that brings together the world's securities regulators. It is the global level standard setter for the securities sector. It works intensively with the G20 and the Financial Stability Board (FSB) on the global regulatory reform agenda. The membership of IOSCO is responsible for regulation of more than 95% of the world's securities markets in more than 115 jurisdictions (a complete list of all member types is provided at[5])
- In the USA the Securities and Exchange Commission (SEC[6]), established in 1934 after the 1929 Great Crash, is responsible for regulating the markets, enforcing its rules, investigating market abuse and inside trading. For commodities in the USA there is also the Commodity Futures Trading Commission (CFTC[7]) which oversees designated contract markets, swap execution facilities, derivatives clearing organizations, swap data repositories, swap dealers, futures commission merchants, commodity pool operators and other intermediaries.
- In the European Union, the European Securities and Markets Authority (ESMA[8]) is mandated to protect investors, verify orderly markets and take care of financial stability.
- In UK the Financial Conduct Authority (FCA[9]) is the legal prudential regulatory authority which is responsible for regulating the markets and the Prudential Regulation Authority (PRA) is responsible for regulation of banks, building societies, credit unions, insurers, and designated investment firms. The FCA was recently established on the 1st of April 2013 when it took over the previous responsibility for conduct and relevant prudential regulation from the Financial Services Authority. The FCA and ESMA works closely together.
- In Switzerland there is the Swiss Financial Market Supervisory Authority (FINMA[10]) that is responsible for market regulations.
- In Japan the Financial Services Agency (FSA[11]) is responsible for market regulations.
- In Hong Kong the Securities and Futures Commission (SFC[12]) is responsible for market regulations. There is also the Hong Kong Monetary Authority (HKMA[13]) which was established on 1 April 1993 from a merge of the Office of the Exchange Fund with the Office of the Commissioner of Banking. The HKMA has the responsibility of enforcing the Exchange Fund Ordinance and the Banking Ordinance and it reports directly to the Financial Secretary. It therefore maintains monetary and banking stability through activities such as maintaining currency stability within the framework of the Linked Exchange Rate system promoting the stability and integrity of the financial system, including the banking

www.elsevierdirect.com

system helping to maintain Hong Kong's status as an international financial center, including the maintenance and development of Hong Kong's financial infrastructure managing the Exchange Fund.
- In Asia Pacific a few of the bigger market regulators involve Australia's regulator known as the Australian Securities and Investments Commission (ASIC[14]); and in Singapore the regulatory body is the Monetary Authority of Singapore (MAS[15]).

Regulatory Guidance, Rules, Directives, and Laws

From these regulatory authorities and working commissions there is a range of different regulatory rules and guidance, some key examples of those which pertain to recent electronic market reporting requirements, of focus in this chapter are briefly outlined below. We include brief discussion on:

- European Market Infrastructure Regulation (EMIR) [short for Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories entered into force on 16 August 2012]. The key requirement is to increase the transparency of the Over the Counter (OTC) derivatives market. EMIR establishes new regulatory requirements on all types and sizes of entities that enter into any form of derivative contract. The new regulatory requirements are separated into three main categories: transaction reporting, clearing, and risk mitigation.
- Markets in Financial Instruments Directive (MiFID II) with some of its key goals including to move trading of standardized derivatives on to exchanges or other organized trading venues as part of OTFs in order to capture smaller broker-to-broker networks. In addition it aims to significantly enhance pre- and post-trade transparency and transaction reporting. A particular focus on commodity and high frequency trading including potential position limits or forced reduction of positions.
- BASEL II/III with one of the aims, in the context of this paper, being to increase capital for trading book positions and introduce new liquidity rules to require larger holdings of a limited pool of assets which must also be used to satisfy likely collateral rules.
- Fundamental review of trading book which is expected to reduce or remove capital and financial accounting distinctions between trading and banking book.
- Market Abuse Directive (MAD) which currently covers disclosure of interests, reporting of suspicious transactions, maintenance of insiders' lists and accepted market practices. It is now extended to also include derivatives and commodities with additional features relating to data sanctions and HFT activities. Can affect MTFs and OFTs as well as OTC.
- Dodd–Frank Act has one of its key objectives being to perform OTC trade standardization and to introduce SEFs for swap market exchange trading. In addition, all derivatives trades should be cleared through CCPs, with all trades reported to trade repositories following confirmation.

- Principles for Financial Market Infrastructures (PFMI) is a new proposal brought out by the Bank of International Settlements (BIS) through the Committee on Payment and Settlement Systems (CPSS) with the goal to enact through IOSCO a more demanding international standard for payment, clearing, and settlement systems, including central counterparties. The PFMI will aim to ensure that infrastructures supporting global financial markets are more robust. The principles apply to all systemically important payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories (collectively "financial market infrastructures" (FMIs)).
- Settlement Under Target2 Securities (T2S) and Central Securities Depositories Regulation (CSDR). The T2S regulation is a response by the ECB to trigger fundamental changes in the post-trade processing, far beyond the initial scope of pan-European settlement in central bank money.
- Basel III (CRD IV), AIFMD, and UCITS V are all depository banking regulations but they will not be discussed in detail in this paper.

In the following subsections we briefly outline some of the new emerging key reporting requirements made under these regulations, before explaining how blockchain technology may aid in facilitating venues to meet these requirements efficiently.

12.2.2 MiFID I

In November 2007, Markets in Financial Instrument Directive (MiFID) 2004/39/EC came into force in the European Union, and changed the fundamental structure of the markets. The key aspects of MiFID I were to increase regulations and obligations of brokers and operator in the market, and of platform providers. Auditing data was to be saved on orders, pre- and post-trade transparency was expected via bid–ask and trade publications, and best executions policy.

MiFID was introduced under the Lamfalussy procedure of Baron Alexander Lamfalussy, which was designed to accelerate the adoption of legislation based on a four-level approach. There are three other "Lamfalussy Directives," including the Prospectus Directive, the Market Abuse Directive, and the Transparency Directive. Skinner (2007) MiFID was intended to replace the Investment Services Directive (ISD), which was adopted in 1993, see Commission (2015a).[16]

This regulation aimed at creating a single market for investment services and activities in order to attempt to increase competitiveness in EU markets. The original regulation made some progress in this regard, but during the financial crisis of 2008 it became apparent that issues still required consideration in regard to exchange regulations,[17] see Commission (2011b).

MiFID was written prior to EMIR and overlaps with EMIR's derivatives trading and reporting obligations in many respects. However, one key aspect of reporting that MiFID conflicts with EMIR's requirements is with regard to the use of Legal Entity Identifiers (LEIs). Firms can comply with MiFID using BICs and other recognized and standardized counterparty IDs, which however may result in non-compliance with EMIR which required the use of LEIs as will be discussed in more detail below. A matching table reconciliation process can be developed, again this is an aspect that blockchain can readily address.

Two levels of the directive were proposed as follows:

- *Level 1*: The MiFID Level 1 Directive 2004/39/EC aimed to set out a detailed framework for the legislation as well as amend Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC and repeal Council Directive 93/22/EEC, Investment Services Directive (ISD) originally adopted in 1993.
- *Level 2*: There were 20 articles in this component of the directive containing the technical implementation measures.

MiFID applies to all firms providing "investment services and activities" in the 31 European countries covered, and includes non-European companies doing business in Europe. Under MiFID there is a distinction made between "investment services and activities" and "ancillary services," as detailed in Annex 1 Sections A and B of the MiFID Level 1 Directive. If a firm performs investment services and activities, it is subject to MiFID in respect to both of these and also of ancillary services.

The extent of MiFID was large, as it covered almost all tradable financial products with the exception of certain foreign exchange trades; however, this has since been captured in new extensions to the regulation which are discussed below. However, the original MiFID regulation did capture commodity and other derivatives such as freight, climate, and carbon derivatives, which were not covered by ISD regulations.

12.2.2.1 Key Components of MiFID I

Under MiFID there are three trading platforms: MTFs, RMs, and SIs with a threshold test in order to register as an SI. In addition, there are requirements on central clearing where investment firms have the right of access to CCPs

MiFID Passports: firms covered by MiFID were authorized and regulated in the country in which they have their registered office. Upon authorization the MiFID passport came into force and could be used to provide services to customers in other EU member states, not in the jurisdiction/state in which the service was provided. This was a substantial change from

previous ISD regulation. In conjunction with this new regulation, a significant anticompetition change occurred in which requirements of the "concentration rule" under ISD were removed. This removed the ability of member states of the EU to require investment firms to route client orders through regulated markets in their jurisdictions.

Categorization of Clients: MiFID required firms to categorize clients based on their level of protection with regard to products they may be exposed to in the markets; they had to be in one of three types: eligible counterparties, professional clients, and retail clients.

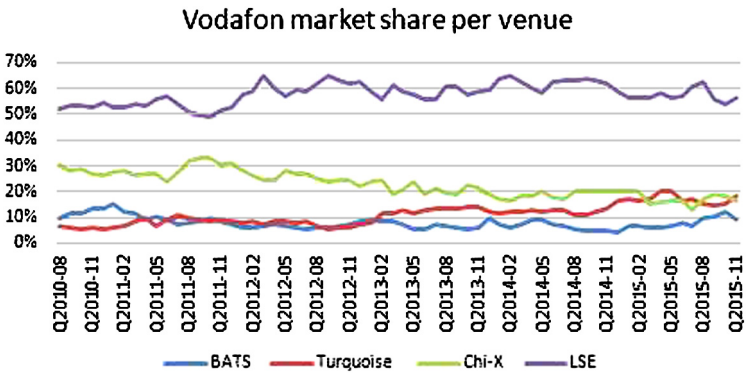
Order Processing and Transparency: MiFID introduced requirements of the specified information to be recorded when accepting client orders. This was target at the notion of best execution practice to safeguard clients when it comes to order prioritization and aggregation. In addition there were new requirements on pre- and post-trade transparency under MiFID. With regard to pre-trade transparency two types of market operator were affected, those performing continuous order-matching who had now to make, for all liquid assets, aggregated order information available at the top five levels of the book on both bid and ask; and for those operating in quote-driven markets the requirement was the level 1 bids and offers of the market makers which had to be reported. Upon a trade execution there were also additional transparency requirements under MiFID which included requiring firms to report the price, volume, and time of all trades in listed shares, even if executed outside of a regulated market.

We note that under MiFID when it comes to transparency regulation it is quite similar to the market transparency directive Reg NMS in the United States. Both MiFID and Reg NMS require detailed information to be captured from client orders. Both regulations require pre- and post-trade transparency. MiFID requires firms to capture data from pre-trade order books, trades executed on multiple venues, and multiple pricing sources. Post-trade reporting and trade matching are required to ensure end-to-end capture of each trade, venue, and counterparty a firm deals with. We discuss briefly Reg NMS below.

In particular, these new reporting requirements affected significantly the OTC derivatives markets, since eligible OTC derivative contracts were suddenly required to be traded through an electronic trading venue, cleared through a CCP, and be subject to transaction reporting requirements.

As part of the transparency requirement, the new venues were required to publish an open Lit book. This also meant that financial institutions needed to collect pricing data from all MTFs as part of the best execution policy. Opposed to the US where one ticker tape published an aggregated book, in the European Union each Venue publishes its own book, which makes

it harder for providers to collect the data simultaneously and trade according to the multiple books.



Best Execution of Trades: MiFID also added the notion of legally requiring best execution. This concept is challenging to disambiguate in some cases but in principle it requires firms to make all reasonable steps to obtain the best possible result in the execution of an order for a client. A core challenge is that the measure of best execution reflects not just price but also other key trade features such as costs, speed, likelihood of execution, and likelihood of settlement, etc.

The appearance of the MTFs required an order book that will consolidate the data of both primary exchange and the MTFs and part of the best execution regulatory requirements. Best execution means that the broker must show that it tried to execute not just at the best price, but also taking into account the trading costs, trading speed, and the likelihood of fills and other factor which effect the trade. Best price should be achieved no matter where this price is, i.e. if the price on MTF X is better than the price on the primary exchange, the broker is obliged to try and execute at the price of MTF X, but also take into account the cost of trading at venue X opposed to venue Y. Since there is no consolidated tape in Europe, some members with direct links might see different prices than others at some point.

Systematic Internalizers: under MiFID the SI firms were to be treated as small exchanges and therefore subject to pre-trade and post-trade transparency requirements.

Market fragmentation: MiFID's goal was to primarily increase transparency for prices. This was to be achieved through the fragmentation of trading venues. However, with this fragmentation requirements also came significant overheads for firms as they suddenly had obligations to collect information from a multitude of MTFs, SIs and other exchanges from the EU region which resulted in a significant challenge when it came to transparency pre- and post-trade reporting and best execution.

www.elsevierdirect.com

With regard to the success of fragmentation aspects of MiFID it is clear that both in lit and dark order books there has been a substantive change in activity. For instance, it is well documented that equity market trading has fragmented across a range of venues.

In the MiFID II impact assessment (Commission, 2011a) there were identified 231 trading systems in the EU which included 139 MTFs and 92 RMs and 12 SIs. To understand the influence this had on particular member states, after MiFID we saw that in the UK, after MiFID there are now seven distinct equity trading platforms (RMs and MTFs) which include: the London Stock Exchange, Chi-X, Turquoise, BATS Europe, NASDAQ OMX, NYSE Arca, and the Plus Markets. In other EU members, post MiFID in Germany 25% of trading in DAX 30 stocks began to appear outside the primary exchange of the Deutsche Borse, similarly in significant trading volume on CAC 40 stocks began to occur outside Euronext.

However, after around the time of the financial crisis, there has been a rise of the dark venue books. The formal dark market increased from 3 to 12 venues between 2008 and 2010 with the main venues being Chi-Delta and Turquoise Dark.

Although it is clear that increased competition has arisen with so many new trading venues arising under fragmentation directives, there have been some additional significant challenges introduced especially in regard to MiFID reporting requirements. As discussed, in order to comply with MiFID, firms must collect information from a multitude of trading facilities. All these sources have different identifiers and formats, data quality and technical access/integration requirements. MiFID is therefore a very costly and complicated regulation to obey, and even up to 2014 many firms remained non-compliant with all of MiFIDs regulatory requirements.

Furthermore, there are conflicts between MiFID and EMIR relating to derivatives reporting, the European Union is considering replacing both MiFID and EMIR with a new regulation called MiFID II or MiFIR. At this point there is a high level of skepticism in the financial community that European regulators will be able to write these regulations without further disrupting the derivatives markets.

12.2.3 EMIR

In this section we focus on the sub-component of EMIR termed the "Reporting obligation" that has been enacted since 12th of August 2014. The reporting requirements are largely stipulated under legal regulation according to EMIR Article 9, EMIR RTS 143/2013 (Article 3 on reporting exposure), EMIR RTS 1247/2013 (Article 5 and Annex 1 which set out the data fields and delay for reporting exposures), and ESMA Q&A TR Question 3 – details on reporting collateral and valuation. EMIR was created by the European Union to stabilize European

and global markets by requiring reporting and standardization of OTC derivatives markets. Note, under Article 2 of EMIR one can consider an "OTC derivative" or "OTC derivative contract" as a derivative contract for which the execution does not take place on a regulated market or on a third-country market considered as equivalent to a regulated market.

12.2.3.1 Scope of EMIR

The scope of EMIR is substantial in the EU region with it affecting all entities "established" in the EU, which includes banks, insurance companies, pension funds, investment firms, corporates, funds, SPVs, etc., that enter into derivatives, no matter the purpose. Under EMIR such trading counterparties have the obligation to report derivatives trades, valuation and collateral data to a designated Trade Repository (TR). Both counterparties must report; however, one party (delegor) may delegate its reporting obligation to the other party (delegee). In this event the delegor is still responsible for the data quality, and must monitor the data submitted by the delegee to a TR. The TRs in scope include: DTCC Derivatives Repository Ltd. (DDRL); Krajowy Depozyt Papierów Wartosciowych S.A. (KDPW); Regis- TR S.A.; UnaVista Ltd.; CME Trade Repository Ltd. (CME TR); and for commodities, credit, equities, interest rates only the ICE Trade Vault Europe Ltd. (ICE TVELL). Note, that under EMIR a trade can be reported to multiple TRs. The consequence of this is that it has caused significant data challenges with regard to compliance and data quality/reconciliation.

We note that from a legal perspective the exact scope of the financial instruments covered by EMIR is set out in Annex I, Section C, points (4) to (10) of MiFID (EU Directive 2004/39EC).

Generally EMIR includes the following categories of instrument (obtained directly from[18]):

- Options, futures, swaps, forward rate agreements and any other derivative contracts relating to securities, currencies, interest rates, or yields, or other derivatives instruments, financial indices or financial measures which may be settled physically or in cash;
- Options, futures, swaps, forward rate agreements and any other derivative contracts relating to commodities that must be settled in cash or may be settled in cash at the option of one of the parties (otherwise than by reason of a default or other termination event);
- Options, futures, swaps, and any other derivative contract relating to commodities that can be physically settled provided that they are traded on a regulated market and/or an MTF;
- Options, futures, swaps, forwards and any other derivative contracts relating to commodities, that can be physically settled not otherwise as mentioned in C.6 and not being for commercial purposes, which have the characteristics of other derivative financial instruments, having regard to whether, inter alia, they are cleared and settled through recognized clearing houses or are subject to regular margin calls;
- Derivative instruments for the transfer of credit risk;

- Financial contracts for differences;
- Options, futures, swaps, forward rate agreements and any other derivative contracts relating to climatic variables, freight rates, emission allowances, or inflation rates or other official economic statistics that must be settled in cash or may be settled in cash at the option of one of the parties (otherwise than by reason of a default or other termination event), as well as any other derivative contracts relating to assets, rights, obligations, indices, and measures not otherwise mentioned in this Section, which have the characteristics of other derivative financial instruments, having regard to whether, inter alia, they are traded on a regulated market or an MTF, are cleared and settled through recognized clearing houses or are subject to regular margin calls.

The reporting frequency under EMIR differs from its counterpart in the US the CFTC / Dodd–Frank regulations. In the EU under EMIR the derivatives trade reporting frequency is an end-of-day snapshot reported by T+1. However, in the US there is under Dodd–Frank an intraday reporting requirement.

12.2.3.2 EMIR Reporting Information: LEI, UTI, and Required Data Fields

EMIR requires reporting of the transaction details for both exchange traded derivatives (ETD), which are not explicitly defined under EMIR, and for OTC derivatives. For example, the derivative contracts traded on MTFs are OTC derivatives in the context of EMIR. The minimum required reporting information, as stated explicitly on,[19] includes two distinct categories:

- *Counterparty data*: name, domicile, ID of the counterparty (set out in the Annex I, Table 1, Commission Delegated Regulation (EU) No. 148/2013 of 19 December 2012);
- *Common data*: type of contract; maturity; notional value; quantity; settlement date, etc. (set out in the Annex I, Table 2, Commission Delegated Regulation (EU) No. 148/2013 of 19 December 2012).

We begin by first describing the LTI and UTI and how they can be generated in a manner to satisfy regulations. As part of this reporting data, under EMIR, there is the consideration of the Legal Entity Identifier (LEI) and the Unique Trade Identifier (UTI). The LEI is a unique sequence of numbers and letters that identifies the counterparties, CCPs, beneficiaries and brokers. The UTI identifies a specific trade and is generated under certain rules provided by ESMA. Counterparties are required to agree on the form of UTI to be adopted.

The key quantities to be reported to TRs under EMIR will be discussed in this section. First we recall the basic mechanism proposed for LEI and UTI creation. The Commission Delegated Regulation (EU) No. 148/2013 specifies that in the absence of a Trade ID agreed at the European Level, a unique code should be generated and agreed with the other counterparty

(Table 2, field 8). The maximum length of a Trade ID should not exceed 52 characters (Commission Implementing Regulation (EU) No. 1247/2012), and no additional character padding is required should a shorter Trade ID be utilized.

Consequently, a single Trade ID should be applicable to any one derivative contract that is reported to a trade repository under EMIR and that the same Trade ID is not used for any other derivative contract. Furthermore, such unique identifiers should be applicable in other required reporting jurisdictions. There has been a consultation and question and answer published guidelines from ESMA and this discussed suitable mechanisms for creating the Trade IDs. The Trade ID should be formed by the concatenation (without separators) of three elements outlined in several methods of construction below. ESMA states that they consider any of the following methods of Trade ID construction to meet the requirements for reporting under EMIR (Securities and Authority, 2016b):

- *Method 1*:
  - The characters 'E01'. The characters '000' will also be permitted but only for derivative contracts executed prior to 12 February 2015.
  - The MIC code (ISO 10383) of the applicable trading venue.
  - A unique code generated by that trading venue or by a CCP used by that trading venue to clear the derivative contract that is within the remaining 256 characters.
- *Method 2*:
  - The characters 'E02'.
  - The (20 character) Legal Entity Identifier of the generating entity (normally one of the parties to the trade).
  - A unique code generated by the unique Trade ID generating entity, that is within the remaining 256 characters.
- *Method 3*:
  - The characters 'E03'.
  - A unique code generated independently by both counterparties based on the pre-agreed set of information about the trade in such a way that both counterparties will arrive at the same code and that it would be unique with respect to any other report. The information used should include Common Data from Table 2 of the Commission Delegated Regulation (EU) No 148/2013 and the Legal Entity Identifiers of the two counterparties and be within the total of 256 characters.

With regard to Method 1, if the code is generated by the CCP and if derivative contracts executed on that trading venue could be cleared by more than one CCP, then it is required that protocols are established to avoid different CCPs generating the same value to ensure codes remain unique across TRs.

www.elsevierdirect.com

The other fields of information required to actually be reported include the following breakdown. In particular under EMIR financial counterparties (FCs) and non-financial counterparties (NFCs) above a regulatory specified clearing threshold must report on a daily basis the collateral and valuation data relating to their open trades and positions to an ESMA authorized TR. In particular they must report data relating to Counterparty Data fields 17 to 26 inclusive which includes information on Valuation data and Collateral data as outlined below:

- *Field 17*: Mark to market valuation of the contract, or mark to model valuation where applicable under Article 11(2) of Regulation (EU) No. 648/2012.
- *Field 18*: The currency used for the mark to market valuation of the contract, or mark to model valuation where applicable under Article 11(2) of Regulation (EU) No. 648/2012.
- *Field 19*: Date of the last mark to market or mark to model valuation. The valuation should be performed on a daily basis.
- *Field 20*: Time of the last mark to market or mark to model valuation.
- *Field 21*: Indicate whether valuation was performed mark to market or mark to model.
- *Field 22*: Whether collateralization was performed. Options: Uncollateralized; One-way Collateralized; Partially Collateralized; Fully Collateralized.
- *Field 23*: Whether the collateralization was performed on a portfolio basis. Portfolio means the collateral calculated on the basis of net positions resulting from a set of contracts, rather than per trade.
- *Field 24*: If collateral is reported on a portfolio basis, the portfolio should be identified by a unique code determined by the reporting counterparty.
- *Field 25*: Value of the collateral posted by the reporting counterparty to the other counterparty. Where collateral is posted on a portfolio basis, this field should include the value of all collateral posted for the portfolio.
- *Field 26*: Specify the value of the collateral for field 25.

12.2.4 CFTC and Dodd–Frank

The Chairman of the CFTC, Garry Gensler is quoted as summarizing the CFTC Dodd–Frank act as "*The Wall Street reform bill will – for the first time – bring comprehensive regulation to the swaps marketplace. Swap dealers will be subject to robust oversight. Standardized derivatives will be required to trade on open platforms and be submitted for clearing to central counterparties. The Commission looks forward to implementing the Dodd–Frank bill to lower risk, promote transparency and protect the American public*".[20]

Under the U.S. Dodd–Frank Act the Commodities Futures Trading Commission (CFTC) was mandated to create new market structure and trade reporting rules for the U.S. derivatives market. CFTC derivatives regulations differ substantially from EMIR rules in Europe.

The actual legal documents pertaining to the Dodd–Frank act involves 38 distinct areas of regulation of the swaps market place, see,[21] that were identified by the CFTC jointly with a public consultation process.

The regulatory rules pertaining to reporting standards that are the focus of this chapter are contained in the following subset of Federal Registry legal rules and regulations (which may not represent a complete set of all such regulations but is sufficient for purposes of this chapter):

- 17 CFR Part 46: Swap Data Recordkeeping and Reporting Requirements which was effective from August 13, 2012;
- 17 CFR Parts 1, 3, and 23: Swap Dealer and Major Swap Participant Recordkeeping, Reporting, and Duties Rules; Futures Commission Merchant and Introducing Broker Conflicts of Interest Rules; and Chief Compliance Officer Rules for Swap Dealers, Major Swap Participants, and Futures Commission Merchants which all became effective from June 4, 2012;
- 17 CFR Parts 4, 145 and 147: Commodity Pool Operators and Commodity Trading Advisors which became effective from April 24, 2012;
- 17 CFR Part 45: Swap Data Recordkeeping and Reporting Requirements which became effective from March 13, 2012;
- 17 CFR Part 43: Real-Time Public Reporting of Swap Transaction Data which became effective from March 9, 2012;
- CFTC 17 CFR Part 4 and SEC 17 CFR Parts 275 and 279: Reporting by Investment Advisers to Private Funds and Certain Commodity Pool Operators and Commodity Trading Advisors on Form PF with effective date March 31, 2012;
- 17 CFR Parts 15 and 20: Large Trader Reporting for Physical Commodity Swaps with effective date September 20, 2011;
- 17 CFR Part 44: Reporting Certain Post-Enactment Swap Transactions with effective date December 17, 2010; and
- 77 FR 53870: Availability of a Legal Entity Identifier Meeting the Requirements of the Regulations of the Commodity Futures Trading Commission and Designation of Provider of Legal Entity Identifiers To Be Used in the Recordkeeping and Swap Data Reporting.

There are three significant differences between the CFTC Dodd–Frank regulations and those of the EMIR European counterparts. The first is that under CFTC regulations, counterparties to a derivative trade have the obligation to report the trade to an approved Swap Data Repository (SDR) which is the US equivalent of a TR in Europe. Under the Dodd–Frank framework an a priori agreed single party must report the trade to an approved SDR. Unlike the four frameworks for reporting arrangement mentioned above for EMIR, in which delegated reporting is not a legal requirement, in the US this is a different matter. Under Dodd–Frank, delegated reporting is standard.

The second significant difference is that in the US, under the CFTC regulations mentioned, derivatives reporting must be done on an intraday basis "as soon as technically practical" as opposed to the EMIR specification of end-of-day reporting only on a T+1 basis.

The third significant difference is that unlike EMIR in which trade reporting requirements apply to all market participants, in the US the CFTC Dodd–Frank framework only applies to the largest financial institutions which on the sell side includes banks with in excess of $50 billion in assets and the buy side it includes market participants such as mutual funds and institutional investment fund groups. In addition, hedge fund will usually utilize Prime Brokers for their derivatives trade reporting and significant Asset Management firms with captive broker-dealers will also report their derivative trades to an SDR.

CFTC derivatives trade reporting regulations cover the majority of derivative products with the exception of those already covered by SEC reporting requirements which include equity swaps and bond swaps which are already reported to a repository attached to a Central Counterparty (CCP) or exchange plus clearinghouse where the trades are executed and cleared such as CME.

12.2.4.1 Reporting Specifications of the CFTC Dodd–Frank Regulations

The final rules of the CFTC Part 45 Rules on Swap Data Recordkeeping and Reporting Requirements was made available on January 13, 2012 when the Commission published in new part 45 of its regulations final rules establishing swap data recordkeeping and reporting requirements applicable to swap dealers, major swap participants, and their counterparties, as well as to registered SDRs, DCOs, designated contract markets, and swap execution facilities ("SEFs").

In the regulation it is required that "*With respect to recordkeeping, part 45 requires SDs and MSPs to keep records of all activities relating to their business with respect to swaps, and requires non-SD/MSP counterparties to keep records with respect to each swap in which they are a counterparty. Required records must be kept by all swap counterparties throughout the existence of a swap and for five years following termination of the swap. In the case of an SD or MSP, the records must be readily accessible throughout the life of the swap and for two years following its termination, and retrievable by the SD or MSP within three business days during the remainder of the retention period.*"[22]

Two aspects of data are required to be electronically reported under part 45 on an SDR: the data at creation of the swap; and the data through the continuation of the swap over its existence until its final termination or expiration.

- Creation data required to be reported pursuant to part 45 includes both primary economic terms ("PET") data and confirmation data for a swap.

- Continuation data required to be reported includes all changes to primary economic terms and all required valuation data.

Under Federal Register /Vol. 77, No. 113/Tuesday, June 12, 2012/Rules and Regulations Exhibit A, Exhibit B, Exhibit C and Exhibit D there are tables outlining the reporting requirements in terms of fields to be considered under Dodd–Frank. For instance under Exhibit A some of the fields required include

- LEI of reporting counterparty and non-reporting counterparty;
- Indication of whether the reporting counterparty is a major swap participant with respect to the swap;
- Indication of whether reporting and non-reporting counterparties are each U.S. persons;
- Type of swap such as multi-asset or mixed swap;
- Counterparty purchasing protection and the selling protection;
- Details of location and type such as contract type, execution time stamp, execution venue, clearing indicator and clearing venue;
- Contract details such as start date, maturity, termination or end date, payment frequency;
- Market details such as price, notional amount and the currency in which notional amount is expressed, amount of currency of any upfront payment.

12.2.5 MiFID II and MiFIR

On 20 October 2011, the European Commission adopted formal proposals for a "Directive on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council" (MiFID II Directive), and a "Regulation on markets in financial instruments (MiFIR)", which would also amend the proposed European Market Infrastructure Regulation (EMIR) on OTC derivatives, central counterparties and trade repositories. Both MiFID II and MiFIR entered into force on 2 July 2014. Under these new regulations there are fewer exemptions and they also expand the scope of the original MiFID to increase the number of companies and financial products captured under the regulation. Both MiFID II and MiFIR are set to take effect in January 2018.

While MiFID I's effort was more on market fragmentation, and opening the Lit markets to other trading venues besides the primary exchanges, MiFID II is more concerned on dark pools and hidden liquidity, stability, and resilience of the markets, and increased order trailing, transparency, and auditing.

The core aims of the MiFID II regulation are targeted at a reduction of systemic risk and to further maximize transparency in markets and in order to ensure robust levels of investor protection. A core focus from MiFID II is the OTC markets for which there will be new extended

pre- and post-trade transparency requirements such as those that are currently applicable to equity markets to non-equity and equity-like products.

Similarly to EMIR regulation there is a mandatory on-platform trading obligation that is applicable to the same market participants as in EMIR. In addition, MiFIR transaction reporting requires position reporting to trade repositories and several of the post-trade obligations in MiFIR reflect EMIR concepts, such as open access, indirect clearing, compression.

12.2.5.1 Brief Summary of MiFID II and MiFIR Trading Venues

Under MiFID II there is a new category of trading venue introduced, which is specifically designed to capture organized trading outside of RMs, MTFs and Sis. Furthermore, under MiFID II there is an elimination of the BCN. We briefly discuss the changes to each asset class below.

Equities: shares that are admitted to trading on a RM, MTF, or SI are covered by MiFID II and MiFIR. Note, the trading obligations do not apply to trades that are non-systematic, ad hoc, irregular, and infrequent or that don't contribute to price discovery.

Derivatives: those traded on a trading venue that are sufficiently liquid and declared subject to the trading obligation are covered in MiFID II and MiFIR. They must now be traded on a RM, MTF, or OTF venue. The trading obligation test is formulated to determine the eligibility of this mandatory trading requirement. It is expected that the only derivatives contracts that will in future continue to trade OTC are those that do not meet the test of being "clearing eligible and sufficiently liquid."

However, any derivative contracts that are not subject to the trading obligation are still subject to transparency reporting requirements and so they may be traded on a trading venue or OTC via a SI.

Commodity Derivatives: in regard to commodity and energy products there is a new range of regulations to capture previously exempt participants under MiFID (Article 2 (1)(k)). It is now required that if such exempt participants derive their main business consisting of trading on own account in commodities and/or commodity derivatives, they will now be required under regulation to prove that their trading activities are ancillary operations to their main business and that they are dealing on their own account based on two tests: whether the activity demonstrably reduces the risks attached to commercial activity or treasury financing activity; and the capital employed for carrying out the activity.

For instance, if a participants pass this test, but they still trade wholesale electricity and gas products, they will instead need to comply with regulation known as REMIT, discussed

briefly below. Any participant in this category not passing these two tests will need to become MiFID II compliant.

Commodity derivative traders will need to comply with new requirements on position reporting and limits. Traders will need to make available position reports to trading venues (on an on-going basis), and trading venues will need to monitor this and enforce position limits where necessary.

Transaction reporting requirements under EMIR and MiFIR will also cover exchange traded and eligible OTC derivative contracts, setting up a web of reporting requirements that traders will need to comply with. Reporting requirements are discussed below.

12.2.5.2 Transparency & Transaction Reporting Under MiFIR

Under MiFID II and MiFIR transaction reporting requirements have significantly increased in the level of detail and the quality required of this information has also intensified. Furthermore, reporting requirements under MiFID II will be dramatically widened in scope, and necessitate significant changes to business processes and technology systems. Pre- and post-trade requirements will apply to equity-like and non-equity products. Transaction reports will be required for these products (including emission allowances), and more details will need to be provided, including the identity of the trader or the algorithm responsible for the execution decision, and any client details on whose behalf the trade was made.

With regard to the dark pools MiFID II introduces caps and waivers. In addition, post-trade data for auditing and proving best execution is growing from about 20 to 80 fields, including trader identifier date in order to be able to trace bad trading to their origin (more in section 1.2.3). There are also misc. changes on the micro structure of the market regarding HFT and tick sized allowed on dark pools.

There is a requirement of continuous liquidity during the trading period. Furthermore, annual reporting of trading strategies is required to the required authorities. There will be a shift in OTC derivatives which will now need to be traded 'on-exchange' with similar clearing obligations as found in EMIR regulations. All commodities will require position reporting and limits will be enforced for positions on trading venues. Access to index and benchmark data as well as CCPs will be subject to non-discrimination clauses. Furthermore, a new regime for data consolidation and reporting which includes Consolidated Tape, APAs and ARMs will be introduced.

Advice provided by financial professionals will need to report if their advice is independent and in addition a ban will take effect on independent advisers receiving or giving third party fees, commissions or other monetary benefits.

Under MiFID II it is now required that firms report to the public the top five trading venues available for order executions and in addition trading venues are to publish data relating to the quality of execution in their venue. The pre- and post-trade reporting requirements discussed in MiFID and EMIR are now extended under MiFID II to include non-equity instruments and such requirements will apply to all OTFs.

Furthermore, explicit details relating to the individuals responsible for the execution, including executing algorithms are to be reported along with details of end clients on whose behalf orders are executed. The reporting is required to be performed by one of the three parties, the Investment Firm, the Trading Platform, or an ARM.

The new MiFIR directive requires pre- and post-trade reporting requirements. The transparency for pre-trade includes reporting data such as Bid and offer prices and depth of trading. This must be undertaken by all Trading Venues, Investment Firms, SIs. The reports are to be made to the public via a Trading Venue and must be made on a continuous basis during business hours. Such reports affect, as stated, Equities, OTC Derivatives, and Exchange traded Derivatives with exemptions for: Illiquid instruments; Block trades; and Trades above a size specific to the instrument.

The post-trade transparency requirements of MiFIR include reporting of data such as price, volume and the time of the trade. The required participants to make such reports includes Trading Venues and Investment Firms and all such reports should be made available to the public via an APA as soon as possible. The instruments considered include the same subset as those in pre-trade reporting requirements of MiFIR.

12.2.5.3 Dark Caps and Large in Scale Waiver (LIS)

MiFID II introduces capping on dark trades which is one of the biggest changes suggested under this new regulation. A 4% cap will be introduced to any equity on a single dark pool, and 8% cap on any single stock in ALL dark pools. Based on data collected over 12 months, a stock that breached the limit will be banned from trading to 6 months.

One of the waivers for dark trading is the large in scale waiver. This waiver means that trading a block in a specific stock which is more than LIS value for this stock, would not count into the caps on the dark pools. The LIS value is published per stock on the ESMA web site. We expect this to also increase the large blocks traded in dark pools.

www.elsevierdirect.com

Annex II: Orders large in scale compared with normal market size, standard market size and deferred publications and delays

Table 1: Orders large in scale compared with normal market size for shares and deposiraty receipts.

Average daily turnover (ADT) in EUR	ADT < 50 000	50 000 ≤ ADT < 100 000	100 000 ≤ ADT < 500 000	500 000 ≤ ADT < 1 000 000	1 000 000 ≤ ADT < 5 000 000	5 000 000 ≤ ADT < 25 000 000	25 000 000 ≤ ADT < 50 000 000	50 000 000 ≤ ADT < 100 000 000	ADT ≥ 100 000 000
Minimum size of orders qualifying as large in scale compared with normal market size in EUR	15 000	30 000	60 000	100 000	200 000	300 000	400 000	500 000	650 000

12.2.5.4 Record Keeping

MiFID II requires from venues to record many more data and fields then previously required. For full requirements, look at Regulatory Trading Standards (RTS) 24. Some of this data is only available by the order initiator, hence this participant (or a broker) will also have to send this data to the trading venue. This is divided to Trade reporting and order reporting, which require different data sets.

Data fields from 21 under MiFID I to 65 under MiFID II (correct to May 2016), this data includes details such as The Participant and identification code, the investment decision (Algo/Trader) for orders and executions, passive or aggressive decisions and more. Parts of the data are identification data needed for the trader and decision maker, these data points are highly sensitive, such as address and national insurance number of the traders.

This data should be saved securely of course and does not have to be passed over the wire via Fix or similar protocol on each order, but rather via a short code; we will suggest a way if using Block chain in order to do this.

12.2.5.5 Standardization of Reporting Under MiFID II and MiFIR

The adoption of standard LEIs and the recognition of overlapping requirements by EU authorities are major steps towards more consistent reporting practices; however, the most significant milestone in the harmonization roadmap is the adoption of ISO 20022 as a methodology for standardizing the reporting of market and transactional data to competent authorities, as outlined in MiFID II/MiFIR. Under these requirements, reports must be submitted in the ISO 20022 format one working day after the transaction.

www.elsevierdirect.com

This reporting must be undertaken by the regulated financial institution itself, by the approved reporting mechanism (ARM) acting on its behalf, or by the trading venue in whose system the transaction was concluded. A similar concept of responsibility is found in EMIR where trade repositories take the place of ARMs.

MiFID II/MiFIR-related reporting obligations cover virtually all instruments except those explicitly covered by other EU reporting regimes (i.e. EMIR for derivatives contracts) or instruments that will be covered by other regimes in the future (i.e. SFTR for securities financing transactions).

The introduction of distinct reporting obligations, which often require similar data, underscores the need to agree on a set of business elements derived from a central data repository that can be reused to comply with different regulatory requirements across multiple markets. This would guarantee the consistency in terms of format and content for data reported under various regulatory requirements and jurisdictions.

Time and effort spent on reconciliation and maintaining dual reporting data repositories then could be allocated to conducting intelligence analytics and data quality reviews. The amount of time currently spent on data collection and reconciliation was highlighted in a 2015 Federal Reserve regulatory reporting survey, which found that financial institutions in the USA spend 50 percent of their time preparing their regulatory reports versus performing analysis or reviews.

12.2.6 REMIT

REMIT (Regulation on Wholesale Energy Markets Integrity and Transparency). REMIT is a European regulation requiring the reporting of derivatives trades on physical commodities. REMIT is a highly transformative regulation for commodity producers, hedgers, and traders which interacts with EMIR and MiFID.

REMIT Market abuse provisions for electricity and gas markets based on MAD Wholesale energy markets use both derivative and commodity trading; therefore, the approach to market manipulation and insider trading should be aligned and compatible between markets Obligation to provide details of wholesale energy transactions to ACER Reporting may be made via third party, trade reporting system or organized market (RM, MTF or OTF) Reports made under MiFID or EMIR do not need to be double reported.

12.2.7 Reg NMS

Regulation National Market System (Reg NMS) is a set of rules that were introduced by the SEC (17 CFR PARTS 200, 201, 230, 240, 242, 249, and 270, [Release No. 34-51808; File

www.elsevierdirect.com

No. S7-10-04], RIN 3235-AJ18: REGULATION NMS), which looks to improve the U.S. exchanges by increasing fairness in price execution as well as improve the displaying of quotes and amount and access to market data. Under Reg NMS there are four core components:

- The Order Protection Rule which aims to ensure that investors receive the best price when their order is executed;
  - In particular, it requires that "*trading centers to establish, maintain, and enforce written policies and procedures reasonably designed to prevent the execution of trades at prices inferior to protected quotations displayed by other trading centers, subject to an applicable exception. To be protected, a quotation must be immediately and automatically accessible.*"[23]
- The Access Rule which aims to improve access to quotations from trading centers in the National Market System;
  - It requires "*requires fair and non-discriminatory access to quotations, establishes a limit on access fees to harmonize the pricing of quotations across different trading centers, and requires each national securities exchange and national securities association to adopt, maintain, and enforce written rules that prohibit their members from engaging in a pattern or practice of displaying quotations that lock or cross automated quotations*."[24]
- The Sub-Penny Rule aimed at setting lower quotation increments for all stocks over $1.00 per share to at least $0.01; and
- Market Data Rules which aim to allocate revenue to self-regulator organizations that promote and improve market data access.
  - This requires "*that update the requirements for consolidating, distributing, and displaying market information, as well as amendments to the joint industry plans for disseminating market information that modify the formulas for allocating plan revenues ('Allocation Amendment') and broaden participation in plan governance ('Governance Amendment').*"[25]

Part 3 of Reg NMS relates to market transparency regulation for equity securities and requires a significant amount of data all the way from pre-trade bid/ask prices through to post-trade reporting and reconciliation. The counterparty identification requirements are significant for broker-dealers and other major equity market participants. Reg NMS overlaps with CFTC / Dodd–Frank and SEC rules related to derivatives, already discussed above.

12.2.8 Settlement Under Target2 Securities (T2S) and Central Securities Depositories Regulation (CSDR)

In some respect we have discussed so far the "Sell Side" of the market participants who operate under EMIR, Basel III, Dodd–Frank and SFTR. There is then also the "Buy Side" of the

market. These are operating under AIFMD, UCITS V and CSDR. Both the Sell and Buy sides then fall under the broader scope of MiFID II.

The European Central Bank (ECB) TARGET2-Securities (T2S) is a pan-European platform for securities settlement in central bank money and represents one of the largest infrastructure projects initiated by the Eurosystem to date. In effect T2S is a European regulation which is intended to integrate and harmonize the highly fragmented securities settlement infrastructure in Europe where there are 35+ Central Securities Depositories (CSDs). T2S is being driven by the need to reduce costs of settlement and to optimize liquidity and capital management across the EU. In total there are 24 T2S harmonization activities, see details in Annex 2 of the Fifth T2S Harmonization Progress Report.

T2S is the predecessor of the TARGET2 (T2) initiative, which was created to streamline cross-border payments, T2S aims to achieve similar efficiencies in the cross-border securities settlement process, Bank (2015a) and Clearstream (2014). In Bank (2015a) it is stated that "*T2S is the future IT platform of the Eurosystem for the settlement of securities transactions in central bank money, and is set to start operations in June 2015. The platform will help overcome the current fragmentation in the securities settlement layer of the European post-trade landscape, thus making an important contribution to the establishment of a single market for post-trade securities services.*"

T2S effectively forces asset services, custodians, clearing houses, and payment processors to adopt common trade and counterparty standards. T2S is therefore highly interrelated with EMIR and MiFID as all three regulations cover shared derivatives data. It is aimed at establishing a single harmonized venue where almost all securities circulating in Europe can be settled with standardized communication protocols and harmonized market practices.

Specific details of the standardization of messages for reporting are available in T2S UDFS v.1.2.1 in Section 3.3 of UDFS.[26] The market participants affect in T2S will be required by regulation to communicate with the T2S technical platform using a set of ISO 20022 compliant messages of which there will be 130 message types in total, see the catalog in Section 3 of UDFS v.1.2.1.8.

T2S will operate a real-time gross settlement (RTGS) system with the securities leg through participating CSDs and cash leg through TARGET2 cash accounts at participating national central banks.

Under new Central Securities Depositories Regulation (CSDR) guidance, it is emerging that any transaction flow that could be settled at a CSD, but is instead settled on intermediaries books will require clear regulatory reporting. As a result, regulators will require reporting on any transaction flow as well as corporate actions, again a significant aspect of regulatory reporting of transactions and market participants, see discussions in Commission (2014).[27]

Note as part of these reporting considerations it is detailed in Bank (2009) that T2S will require the following static data requirements including: Parties reference data; Securities reference data; Securities accounts reference data; T2S dedicated cash accounts reference data; Access rights management; Message subscription configuration; Network configuration; Reports configuration; Attribute domains management; Scheduling configuration; Market-specific attributes configuration; Restriction types management; Conditional securities delivery configuration; Billing configuration; and Configuration parameters; see more details in section 1.6.3.3.1 "Static data 3 objects" of 4CB (2012).[28] Several other reporting requirements are discussed in T2S which can be found in Bank (2012).

12.3 The Role of Blockchain Technology in Electronic Exchanges

There are a range different blockchain architectures and the aim of this section is to illustrate how such structures can be relevant to electronic exchange reporting under the new exchange transparency and reporting requirement regulations discussed previously in this paper.

Discussions on blockchain technology are provided in Peters and Panayi (2015) and Peters et al. (2015). In general the terminology of this new field is still evolving, with many using the terms block chain (or blockchain), distributed ledger and shared ledger interchangeably. Formal definitions are unlikely to satisfy all parties — but for the purposes of this report, the key terms are as follows which we briefly define below, before going into more detail on some aspects in subsequent sections.

Blockchain. A blockchain is a type of database or ledger that takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows blockchains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions. There are many ways to corroborate the accuracy of a ledger, but they are broadly known as consensus (the term 'mining' is used for a variant of this process in the cryptocurrency Bitcoin) — see below. If participants in that process are preselected, the ledger is permissioned. If the process is open to everyone, the ledger is unpermissioned — see below. The real novelty of block chain technology is that it is more than just a database — it can also set rules about a transaction (business logic) that are tied to the transaction itself. This contrasts with conventional databases, in which rules are often set at the entire database level, or in the application, but not in the transaction.

Permissionless Ledgers. In the case of an unpermissioned or permissionless ledger, such as the one utilized in Bitcoin, there is no single owner — indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for

everyone in possession of the ledger to have identical copies. This creates censorship resistance, which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state. Unpermissioned ledgers can be used as a global record that cannot be edited: for declaring a last will and testament, for example, or assigning property ownership. But they also pose a challenge to institutional power structures and existing industries, and this may warrant a policy response on governance considerations.

Permissioned Ledgers. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors — government departments or banks, for example — which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. Requiring many government departments to validate a record could give a high degree of confidence in the record's security, for example, in contrast to the current situation where departments often have to share data using other means such as physical copies. A permissioned ledger is usually faster than an unpermissioned ledger.

Distributed Ledgers. Distributed ledgers are a type of database that is spread across multiple sites, countries or institutions, and is typically public. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum. A distributed ledger requires greater trust in the validators or operators of the ledger. For example, the global financial transactions system Ripple selects a list of validators (known as Unique Node Validators) from up to 200 known, unknown or partially known validators who are trusted not to collude in defrauding the actors in a transaction. This process provides a digital signature that is considered less censorship resistant than Bitcoin's, but is significantly faster.

Shared Ledgers. A shared ledger is a term coined by Richard Brown, formerly of IBM and now Chief Technology Officer of the Distributed Ledger Group, which typically refers to any database and application that is shared by an industry or private consortium, or that is open to the public. It is the most generic and catch-all term for this group of technologies. A shared ledger may use a distributed ledger or block chain as its underlying database, but will often layer on permissions for different types of users. As such, 'shared ledger' represents a spectrum of possible ledger or database designs that are permissioned at some level. An industry's shared ledger may have a limited number of fixed validators who are trusted to maintain the ledger, which can offer significant benefits.

www.elsevierdirect.com

Smart Contracts. Smart contracts are contracts whose terms are recorded in a computer language instead of legal language that can be designed to enact legal contracts or regulations. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system in response to changes in the ledger, in real time. The potential benefits of smart contracts include reduction in contracting, enforcement, and compliance costs; consequently it becomes economically viable to form contracts over numerous low-value transactions. The potential risks include a reliance on the computing system that executes the contract.

12.3.1 Brief Overview of Some Basics of Blockchain and Related Technologies

Just like many other technologies for the Internet, blockchains rely on public key cryptography to protect users from having unauthorized persons take control of their accounts. The private and public key pairs enable people to encrypt information to transmit to each other, where the receiving party would then be able to determine whether the message actually originated from the right person, and whether it had been tampered with. This is critical when one needs to communicate to a network that a transaction between two parties has been agreed. In addition, the presence of an ability to identify the integrity of the data is also critical for applications we will consider as discussed further below.

In this section we don't enter into a detailed discussion on the basic details of cryptographic properties of blockchain and its construction via hash functions as the reader can find this detail in alternative chapters in this book. We note that detailed discussions on the different types of hash function may be found in the overview of Carter and Wegman (1977). Instead we briefly explain the basic notion of a hash function. The basic idea behind a hash functions use is to facilitate an efficient means for searching for data in a set of records. In its most basic form, a hash function is any function that can be used to map data of arbitrary size to data of fixed size where the output is a bit-string known as the hash value, hash code or hash sum. These hash values are stored in a tabular form known as the hash table and this is used as an efficient indexing mechanism when performing searches. Detailed discussions on the different types of hash function may be found in the overview of Carter and Wegman (1977).

It turns out that when one combines hash functions and hash tables with cryptographic techniques, the resulting cryptographic hash function is directly applicable to establishing security and privacy protocols required for blockchain ledger technologies. In this context one can think of a cryptographic hash like of a signature for a text or a data file. It is secure since the cryptographic hash function allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value.

www.elsevierdirect.com

There are several variants of the cryptographic hash function and each have different cryptographic features, see discussion in Chapter 7 of Franco (2014). These may often include considerations of one-wayness (i.e. preimage resistance) where knowledge of the hash value still makes it computationally highly improbable to find out the input data (a key element of proof-of-work aspects); weak and strong forms of collision resistance, the first of which means that given an input, it will be computationally improbable to find another input with the same hash value and stronger form states that it will be computationally improbable to find two input data with the same hash value. Note, computationally improbable means here that no known algorithm can recover the input message from the hash within a time that is related polynomially related to the size of the input.

A popular example of such hash functions is the SHA256 hashing function which in some instances, like bitcoin, is applied twice. The SHA256 algorithm comes in several forms and is part of the SHA-2 class of hash functions, see discussions in Matusiewicz et al. (2005), but generally it generates an almost-unique, fixed-size 256-bit (32-byte) hash security. Large classes of hash functions are based on a building block of a compression function, see discussions on this in Merkle (1980), Coron et al. (2005).

We note that within the blockchain structure there is also included information related to the digital time stamp, which records the temporal existence of a particular blockchain ledger item at a given instance in time. It could be utilized to symbolize that a contract between two agents is initiated or completed, that transactions of some form materialized or that payments/e-property were transferred ownership, etc. Typically a digital time stamp also contains information relating to the hash created from the activity of securing the particular data/information entered into the ledger. This allows time stamping to occur with an element of privacy for the data being secured and entered on the blockchain ledger. In addition, just recording the hash is a more parsimonious representation of the information being secured or recorded.

There exist parties such as Time-Stamping Authorities (TSA) that can provide a trusted third party arrangement to provide a secure and safe cold or secured live storage of information relating to the blockchain ledger recording. This digital notary signs with a private key for this data to be recorded and the time when this data was communicated to the authority. Then the signature address would be sent back to the original owner of the data. This simplified form is often performed in blockchain technologies using more advanced approaches such as a TSA collecting and securing in encrypted storage several agents data sets from within a fixed time period, then taking all data from this period and providing a time stamp, and hashing all this data together via a method such as a Merkle tree, see Merkle et al. (1979), Merkle (1980). Then the resulting hash, for instance the root of the Merkle tree, would be hashed together with the final hash of the previous time period and then published in the blockchain ledger.

www.elsevierdirect.com

12.3.1.1 Permissioned and Permissionless Blockchains

In the prototypical example of a blockchain, the Bitcoin network, the blockchain used is 'permissionless'. Permission refers to the authorization for verification, and in a permissionless blockchain anybody can join the network to be a verifier without obtaining any prior permission to perform such network tasks. Because these verifiers are vital to the operation of the network, their participation is encouraged and often incentivized. This requires a mechanism to incentivize agents to participate, the most common of which is known as Proof-of-Work.

Consensus within the network is achieved through different voting mechanisms, the most common of which is Proof-of-Work, which depends on the amount of processing power donated to the network, see discussions in Peters et al. (2015). The notion of Proof-of-Work allows the network to secure against malicious attempts to tamper with the blockchain structure due to the computational power that has already been applied to create the blockchain ledger entries. If an attacker wished to tamper with the blockchain, they would have to commit a computational effort equivalent or greater than all the power spent from the reference point they wished to alter to the present time. In addition, they would have to achieve this at a faster pace than the current legitimate network processing of new blockchain entries. Proof-of-work concepts can come in many forms, for instance they may rely on solutions to a computationally hard problem, a memory intensive problem or a problem that may require user interventions. To be practically useful for a blockchain technology, such problems must be computational challenging to solve, but efficient to verify a solution once obtained. Although these algorithms are vital in ensuring the security of the network, they are also very costly in terms of computation.

A permissionless blockchain is advantageous in that it can both accommodate anonymous or 'pseudonymous' actors and protect against a Sybil (i.e. identity-forging) attack (Douceur, 2002). On the other hand, the incentive mechanism has to be carefully developed in order to ensure that verifiers are incentivized to participate. This is an important consideration that should be further considered for the proposed blockchain architectures discussed in this paper. Besides Bitcoin, examples of permissionless blockchains include Ethereum,[29] the platform that is intended to provide access to smart contracts on the blockchain, as well as offer blockchain as a service.

In contrast to permissionless blockchains, the category of permissioned blockchains has a set of trusted parties to carry out verification, and additional verifiers can be added with the agreement of the current members or a central authority. Such a configuration is more similar to a traditional finance setting, which operates a Know Your Business (KYB) or Know Your Client (KYC) procedure to whitelist users that are allowed to undertake operations in a particular space. As noted in Peters and Panayi (2015), permissionless and permissioned blockchains are fundamentally different in both their operation and the range of activities that

they enable, some of which we review here in the context of the proposed application to facilitating transparency and reporting for electronic exchanges.

Permissioned blockchains are intended to be purpose-built, and can thus be created to maintain compatibility with existing applications (financial or otherwise). They can be fully private (i.e. where write permissions are kept within an organization), or consortium blockchains (where the consensus process is controlled by a pre-selected set of nodes).[30] Because the actors on the network are named, the intention is that they are also legally accountable for their activity. In terms of the transactions these blockchains handle, it will be predominantly off-chain assets, such as digital representations of securities, rather than on-chain assets, such as virtual currency tokens.

An advantage of a permissioned blockchain is scalability. In a typical permissionless blockchain, the data is stored on every computer in the network, and all nodes verify all transactions. It is obvious that once the number of transactions increases substantially, the users that are able to perform this type of processing and verification will decrease, leading to more centralization. In a permissioned blockchain, only a smaller number of preselected participants will need to operate, and if these come from large institutions they will be able to scale their computing power in line with the increase in the number of transactions.

However, because of the smaller number of participants, it is much easier for a group of users to collaborate and alter the rules, or revert transactions. In addition, it is easy for them to reject transactions and in this sense it is not 'censorship resistant' as a permissionless blockchain would be. Examples of permissioned blockchains include Eris,[31] Hyperledger,[32] Ripple[33] and others.

12.3.1.2 Smart Contracts on Blockchains May Provide Automated Oversight on Transparency and Reporting

A new range of what are known as second generation blockchain applications are starting to emerge in industry applications. One of the most prominent of these includes digitizing asset ownership, intellectual property, and smart contracts. The latter usecase is particularly interesting, as one can encode the rules of a contract in computer code, which is replicated and executed across the blockchain's nodes. Such a contract can be self-enforcing, monitoring external inputs from trusted sources (e.g. the meteorological service, or a financial exchange) in order to settle according to the contract's stipulations.

These second generation blockchain technologies enable not only the execution of simple transactions, but the carrying out of computation on a network, where e.g. payments become conditional on the state of some internal or external variables (much the same way as financial derivatives have a payout that is a function of an underlying financial instrument). This is the

basis for 'smart contract' technologies, which we shall see can be important building blocks for these new application areas. As a consequence of these second generation technologies, a number of developments in this field have begun to appear which include third party data ledgers (Martel et al., 2001), e-contracts/smart contracts and virtual contracts (Buterin, 2014; Kosba et al., 2015; Swan, 2015), e-assets or remote asset title transfers (Halevi et al., 2011) and further applications, discussed in Czepluch et al. (2015).

In principle such contracts could eventually enact an automation of regulatory rules on transparency and regulatory reporting requirements for pre- and post-trade executions on the different types of exchange venues discussed earlier in the paper.

The concept of smart contracts has been considered as early as 20 years ago by Szabo (1997), although we have only recently had concrete blockchain-based implementations. These blockchains extend the functionality of the network, enabling it to move from achieving consensus on data streams, to achieving consensus on computation (Kosba et al., 2015). An example is Ethereum, which intends to provide 'built-in blockchain with a fully fledged Turing-complete programming language' (Buterin, 2014).

Smart contracts can feature loops and have internal state, so a much richer array of transactions becomes possible. In addition, they are permanent (i.e. they remain on the blockchain unless they are instructed to self-destroy), and are able to be reused as building blocks for a more complex service. One of the leading smart contract applications is known as Ethereum. It can be seen as a platform for deployment of Internet services, for which such smart contracts are the building blocks. Because of the Turing-completeness of the in-built contract programming language, and the fact that computation is executed on every network node, it could have been possible for one to create an infinite loop, i.e. a contract that never terminates, which could bring down the network. To protect against this, programmable computation in Ethereum is funded by fees, termed 'gas', and a transaction is considered invalid if a user's balance is insufficient to perform the associated computation (Wood, 2014).

There are still potential issues to be resolved, however, before smart contracts can reach widespread adoption. One is scalability, as it is infeasible to expect that as the number of contracts and users grows, every single node has to process every transaction. The second is code correctness, as both the developers and users of the smart contracts have to be confident that the contract performs its intended use, and does not entail excessive fees due to unnecessary computations. Finally, there is the issue of the relationship between an electronic smart contract and its legal counterpart. How can one perform court enforced legally binding contracts on a distributed and decentralized system potentially over multiple legal jurisdictions?

Thus far, smart contracts are not legally enforceable, although there have been efforts in the direction. Eris industries have recently proposed the idea of dual integration, or 'ensuring a

real world legal contract overlay fused onto a specific smart contract.'[34] Other initiatives include CommonAccord,[35] which attempts to create templates of legal texts and thus create contracts in a modular fashion. The objective is to remove ambiguity as much as possible, having the smart contract accurately reflect the written legal contract, so that it can be actionable in the real world.[36]

12.3.2 Overview of Blockchain Emerging in Electronic Exchanges

It is now the case that several major electronic exchange venues and clearing houses are exploring the capabilities of blockchain technology for trade processing. An example of this was the US stock exchange provider Nasdaq launching a blockchain prototype last fall known as Linq.[37] They can be quoted as stating that they believe that "*blockchain holds potential for 99% reduced settlement time and risk exposure in capital markets.*"

As of Dec. 30, 2015 Linq blockchain ledger was used successfully to complete and record a private securities transaction which represented the first of its kind using blockchain technology. This transaction marked a real demonstration of this conceptual technology in real use case and therefore represents a major advance in the application of blockchain technology for private companies.

In creating this "transaction" under Linq the issuer was able to digitally represent a record of ownership, while significantly reducing settlement time and eliminating the need for paper stock certificates. Furthermore, elements of trade reporting are starting to be considered in applications like Linq. For instance, in addition to its equity management function, Nasdaq Linq also provides issuers and investors an ability to complete and execute subscription documents online. Other applications of Linq include the use of blockchain for trade settlement transactions in public electronic exchanges. It is argued by Nasdaq that "*blockchain technology has the potential to assist in expediting trade clearing and settlement from the current equity market standards of three days to as little as ten minutes. This technology could allow issuers to significantly lower the risk and the administrative burden of what is largely a manual and multi-step process today*."[38]

Various other important use cases are being explore with payment systems, credit card systems, banking systems, and exchanges. Below we mention 10 major stock and commodities exchanges that have so far publicly announced their intention to explore blockchain technologies.

There are also industry working groups being initiated such as the Post-Trade Distributed Ledger (PTDL) Group which was an initiative launched in 2015 by a number of banks, clearing houses, and exchanges. It currently has around 37 financial institutions as members, with

www.elsevierdirect.com

its organization committee being composed of CME Group, Euroclear, HSBC, the London Stock Exchange and UniCredit with additional active members such as LCH.Clearnet, Societe Generale, and UBS.[39]

Furthermore, there was a recent unveiling of the Global Blockchain Council (GBC) which is a 46-member consortium of start-ups, financial firms, and technology companies that was established to review the technology and its impact.[40] This consortium includes Dubai Trade, Dubai Gold and Commodities Exchange, Emirates, Moe Levin and Dubai Department of Economic Development and falls under the strategic direction of UAE leadership. It is quoted by HE Mohammed Al Gergawi, Vice Chairman and Manging Director of Dubai Future Foundation that "*...blockchain technology, which is expected to have a market value of USD 290 Billion by 2019, will contribute massively in elevating the level of the smart services provided to citizens from cost, time and efficiency perspectives...*"[41]

The following core exchange groups are looking at ways to adopt blockchain technology[42]:

- *Australian Securities Exchange (ASX)*. ASX group have reportedly invested more than $10m in industry start-up Digital Asset Holdings in January as part of its R&D efforts towards blockchain initiatives. ASX has also publicly revealed that it would aim to develop a new post-trade settlement system to be developed by Digital Asset using a distributed ledger architecture.
- *CME Group*. This group was one of the initial founders of the "Post-Trade Distributed Ledger Working Group" via its investment arm, CME Ventures. It has been reported that CME Group has contributed to funding rounds raised by distributed ledger startup Ripple, blockchain investment conglomerate Digital Currency Group and Digital Asset Holdings.
- *Deutsche Borse*. This group operates the primary Stock Exchange in Frankfurt, Germany. This group also participated in the funding round of Digital Asset Holdings with $60m funding.
- *Dubai Multi Commodities Center*. This is part of the GBC developed in the UAE. The DMCC is a special economic zone and commodities center that oversees trading of precious metals and other tangible goods. The new initiatives starting from this GBC and the DMCC include:
  - "FlexiDesk" which is the first pilot project of the GBC which involves cooperation between BitOasis and DMCC to find practical applications for Blockchain technology. The project is aimed at facilitating DMCC's transactions in line with Dubai Plan 2021 by accelerating services and achieving high efficiency at lower costs; and
  - "Trade Flow" which is the second project by DMCC that will provide digital financial transaction services using Blockchain technology. The project will also help significantly reduce costs, increase operations security, unify transactions procedures.

- *Japan Exchange Group (JPX)*. This group announced its interest in blockchain technologies with the news it had formally partnered with IBM as a user of its Blockchain-as-a-Service (BaaS) offering. The initial reports are that the JPX group is studying proof-of-concept for blockchain technologies use in creating new systems for the trading of low-liquidity assets. Further collaborations in this regard are also taking place with JPX and Nomura Research Institute who are investigating how such technologies may apply to securities markets.
- *Korea Securities Exchange*. The KSE announced it would aim to launch an over-the-counter trading platform using blockchain technology.
- *London Stock Exchange (LSE)*. This group was also one of the founders of the previously mentioned Post-Trade Distributed Ledger Working Group. It has been actively linked with startup R3. In addition, LSE is one of the initial clients of IBM's Blockchain-as-a-Service (BaaS) offering alongside Kouvola Innovation and Japan Exchange Group.
- *Nasdaq*. This group was the first US stock market operator to take a blockchain proof-of-concept live when it debuted its private shares trading platform, Linq, in 2015. It also has a partnership with the blockchain solutions provider Chain. Further developments from Nasdaq include working to develop a trial with the Nasdaq OMX Tallinn Stock Exchange in Estonia.
- *New York Stock Exchange (NYSE)*. This group have made two important announcements publicy about blockchain technologies. The NYSE invested in bitcoin services firm Coinbase as part of its $75m Series C funding round. In addition the NYSE are in the process of launching a bitcoin pricing index, a competitor to CoinDesk's Bitcoin Price Index (BPI).
- *TMX Group*. This group runs the Toronto Stock Exchange and has actively explored avenues with smart contracts and recently hired Anthony Di Iorio, one of the co-founders of the Ethereum project, as its first chief digital officer.

We see that blockchain technologies are expected to make a significant impact on several aspects of automation in electronic exchanges, below we discuss a few important cases that pertain to satisfying the regulatory standards on transaction transparency and pre and post trade reporting.

12.4 Blockchain Architecture for Order Record Keeping and Transaction Reporting

Transaction reporting under new EMIR regulations, as discussed in the previous sections, is becoming significantly more demanding in terms of data, storage, event processing and time sequencing. The increasing amounts of data that are to be reported could of course be saved

www.elsevierdirect.com

in a traditional relational database, NoSQL database like MongoDB or alternatively, we will suggest that it instead starts to be incorporated onto a blockchain ledger record.

As discussed in the introduction to blockchain concepts above, one may think of a Blockchain as acting in a similar fashion to a database but containing different features. In this section, what we are suggesting here is how to harness the built-in security and immutability features of the block chain in order to support key regulatory features.

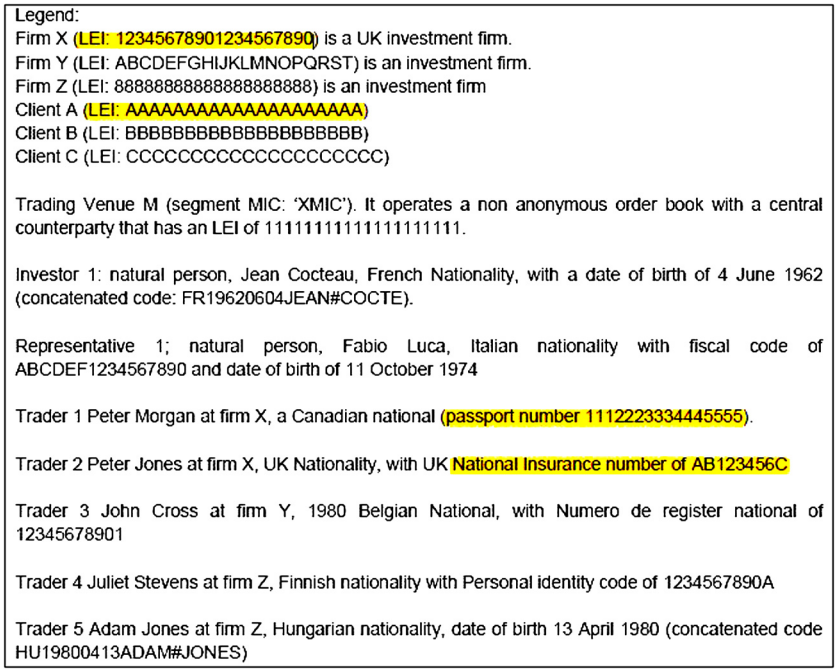
In particular, in this section we will present two use cases of Blockchain technology for transaction reporting, also looking at current frameworks which can be used for these cases. In practice, a specific implementation is a valid option for these architectures features, but we feel that using an already used framework makes these cases closer to a product. We prefer to discuss a generic structure that is more product agnostic and therefore can be adapted to particular needs as required, for details on alternative product specific architectures of blockchain that can also be used to implement transaction reporting we refer the interested reader to Peters and Vishnia (2016).

12.4.1 Entity Identification Requirements

As described in the ESMA consultation paper, "Guidelines on transaction reporting, reference data, order record keeping & clock synchronization" (Securities and Authority, 2015a), there is an increased number of fields to be reported, these include fields 7 to 24 which are directly related to entity identifications. Buyer, seller, and buyer and seller decision makers' identification codes along with their full name, Date of Birth, and Country code for buyer and seller data need to be included in the transaction report. If the decision maker was an Algorithm, it must also be identified by a unique code. Buyers and sellers can either be reported as legal entities, and use their LEI code as identifier. The LEI must be obtained before the transaction (ultimately, when the client is on board) and to be maintained. For the non-legal entities, the identification code will be constructed from the country identifier and passport number/national insurance number (see annex ii ESMA/2016/1064 Securities and Authority, 2016c). The personal data will need to be collected from Human Resources databases, and verified by the reporting company.

This data is by its very nature both personal and sensitive and it therefore needs to be stored, accessed and modified in a secure reliable manner (see Fig. 12.1). Storing the data in a secure hashed blockchain can solve many concerns for the protection and prevention of any personal traders data leakage that should remain private.

We suggest a semi-public blockchain, where Entity identification data is encrypted and stored on the chain, and a unique Id is generated and returned to be used by the trading entity as the


Legend:
Firm X (LEI: 12345678901234567890) is a UK investment firm.
Firm Y (LEI: ABCDEFGHIJKLMNOPQRST) is an investment firm.
Firm Z (LEI: 88888888888888888888) is an investment firm
Client A (LEI: AAAAAAAAAAAAAAAAAAAA)
Client B (LEI: BBBBBBBBBBBBBBBBBBBB)
Client C (LEI: CCCCCCCCCCCCCCCCCCCC)

Trading Venue M (segment MIC: 'XMIC'). It operates a non anonymous order book with a central counterparty that has an LEI of 11111111111111111111.

Investor 1: natural person, Jean Cocteau, French Nationality, with a date of birth of 4 June 1962 (concatenated code: FR19620604JEAN#COCTE).

Representative 1; natural person, Fabio Luca, Italian nationality with fiscal code of ABCDEF1234567890 and date of birth of 11 October 1974

Trader 1 Peter Morgan at firm X, a Canadian national (passport number 1112223334445555).

Trader 2 Peter Jones at firm X, UK Nationality, with UK National Insurance number of AB123456C

Trader 3 John Cross at firm Y, 1980 Belgian National, with Numero de register national of 12345678901

Trader 4 Juliet Stevens at firm Z, Finnish nationality with Personal identity code of 1234567890A

Trader 5 Adam Jones at firm Z, Hungarian nationality, date of birth 13 April 1980 (concatenated code HU19800413ADAM#JONES)

Figure 12.1: Sample identity data from ESMA consultation paper.

Id sent over FIX messaging (Community, 2016). For the transaction reporting entity, when a transaction report is created, it will retrieve the data by using the transmitted unique Id. Only permissioned entities will be able to insert and retrieve data from the chain. We will describe in detail a full work-flow for this proposed solution architecture.

12.4.1.1 Legal Entity Identifier (LEI) and User Identifiers

The Legal Entity Identifier (LEI) is a 20-character, alphanumeric code (based on ISO 17442), to uniquely identify legally distinct entities that engage in financial transactions in any jurisdiction. The Global LEI system has three tires of operations, the regulatory oversight committee (LEI ROC),[43] The Global Legal Entity Identifier Foundation (GLEIF),[44] and Local Operation Unit (LOU). In 2014 all three tiers were endorsed by the FSB and the G20. According to last statistics from GLEIF (August 2016[45]) a total of 458,760 LEI's were issued, a quarter of which are in USA.

The LEI had been mandatory for reporting derivatives transactions under ESMA, and MiFID II will also require investment firms that execute transactions in financial instruments on behalf of a client firm, to include that client firm's LEI within the transaction report sent to the competent authority. If there is no LEI, for example if the sender is a trader X, a unique id like

the national insurance number/passport with name and address will need to be stored and sent instead. We have discussed in previous sections the details of such data under the MiFID II and MiFIR regulation discussions above. Under MiFID II, the broker will need to store and map this data. The categories for the saved data include:

- Identification of the investment firm executing a transaction (LEI);
- Designation to identify natural persons;
- Details of the identity of the client and identifier and details for the decision maker;
- Identification of person or computer algorithm responsible for the investment decision; and
- Identification of person or computer algorithm responsible for execution of a transaction.

12.4.1.2 Entity Identification Blockchain

We suggest a governed hybrid blockchain, maintained by either the regulator or a consortium of investment firms that will incorporate all relevant data into the chain, assigning and managing the unique identifiers for traders and offering a reliable and secure way to update the data and to retrieve the personal data on demand by authorized users. Comparing the chain to a database, it would be like having one initial row with initial fields like name, date of birth, zip code/postcode, current company, etc. filled, and for each update a new row will be included in the ledger, for example a marriage which involves surname change will result in a new row to be added to the database.

The centralized controlled block chain guarantees that all personal data is saved securely with encryption and is always available for back auditing. For example, if a trading company ceases to exist, and drops all its personal records, having all the relevant details of traders on the regulator chain makes sure that there will be no data loss or gaps, which will help trace users for any suspicious market behavior that may be considered during audits.

Let's consider Trader 1, Peter Morgan, Canadian who works at firm X. He registers his relevant personal data, name, DOB, nationality, passport number and other relevant data on the system. In the reply he receives a unique Identifier that will accompany him on whichever company he trades for transaction reporting. This unique Id is also the key to a private hash table controlled and managed by the consortium. on any trade Peter Morgan will do, this unique Id will be used to go later and retrieve the encrypted data needed to be added to the transaction report (see Fig. 12.2). We'll describe in more detail the actions that are being taken on the system.

Registration: The registration will be done via filling a form on a secure web page. In addition to the regulatory required data, the form will also include a username and password for

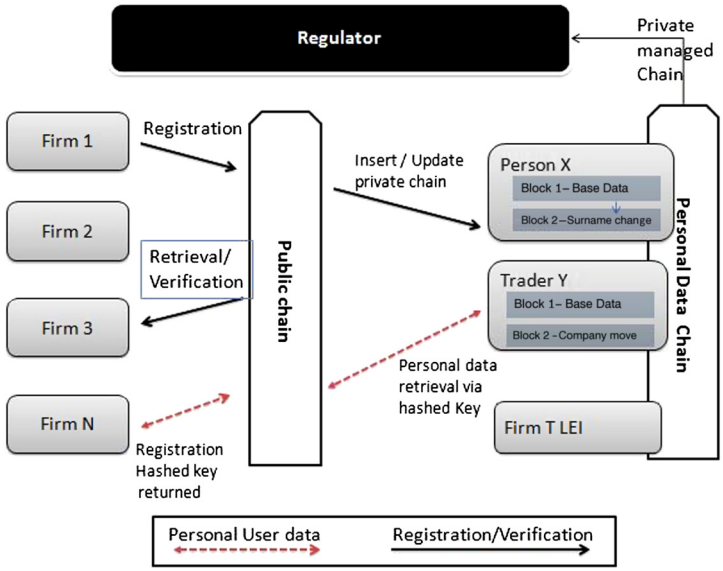


Figure 12.2: LEI system architecture.

later updating or retrieving lost credentials or unique Id. The data sent will be encrypted and saved on the private chain (Lazarovich, 2015).

Update: Some personal data, like date of birth or national insurance number will never change, but other fields like address, work place, passport number (on passport renewals), zip / post codes and surnames (via marriage for example) will need to be updated occasionally. With the login credentials created on registration, the user will be able to login to the system and update his/her private data. Each and every update will be timestamped, encrypted and added to the chain. By timestamping each update transaction we ensure that when backtracking, the relevant user details for the requested period will be retrieved.

Data Retrieval and Verification: The transaction reporting entity will use the unique Id generated when a user is first created in the system in order to retrieve the user data from the private blockchain. The encrypted private data will be fetched and decrypted via a hash function known only to the master of the private blockchain. For LEI the blockchain will verify that the LEI provided is a legitimate and registered LEI.

Loss of Unique Id: In the case of a user losing their unique Id (on moving company for example), they will be able to login into the system website with their user name and password created on first registration, and retrieve their unique Id. The user unique Id, which is stored

www.elsevierdirect.com

on a public distributed blockchain, is not private data by design, as it is transferred openly between different trading platforms and applications when trading via FIX for example.

12.4.2 Order Record Keeping and Auditing With Blockchain

As detailed in previous sections of this document, recent years have seen enhanced scrutiny and oversight by the regulators who are stepping up their demand for trade and transaction reports, transparency and best execution proof, order trail and auditing data. Trading venues and brokers have the obligation to provide reports with many more fields, capture a lot more events and store the collected data for a period of five years in an accessible secure manner. This is already producing massive data sets and the increasing requirements make analysts believe such data requirements for storage of trade activity are likely to continue to grow. The security and data integrity of these records is also a critical feature to be considered, see discussion on these matters in the context of blockchain in Peters and Panayi (2015).

The classic way to achieve the above reporting and storage requirements would be to store the data in a database, relational or a NoSQL database (Tauro et al., 2012) like MongoDB (Chodorow, 2013) via a big data warehousing solution. We will present here a novel architecture for storing the event capture data in a secure immutable way using Blockchain technology, which will provide the regulator with an easy access, on demand data queries without the risk of data tempered or lost, and for the reporting entities a common simple manner for storing the data and replying for regulator queries.

Reportable events and data points: Trading firms and venues will need to provide to the regulator, on demand under Securities and Authority (2015b), all relevant event capture data. This data can be an order event like Ack, Fill, Cancel, etc., market data points like bid/ask for best execution proofing, algorithmic trading decisions, order initiator and many more trading life cycle events (at time of writing a full event list is yet to be confirmed) (RTS 6 for Algo trading, RTS 24 for Venues). The data also needs to be timestamped and synced (RTS 25, Article 4 Securities and Authority, 2015b) with precision of at least one millisecond. This is a hard demand to follow when aggregating trading data from different systems. Of course, each trading entity will have different amounts of data to collect and store, but even for a medium size company this sums up to a very large set of data. Needless to say, all this data should be stored safely and securely and yet be accessible rapidly on demand to a select set of groups such as the regulator and the event capturing entity.

12.4.2.1 Architecture and System Design

In this section we develop two different architectures for storing event data and generating a by demand regulator report for trade reporting pre- and post-events. The difference between

the two architectures we develop lies in the way the two methods are governed. The first architecture is a centralized system, maintained by either the regulator or by a consortium/group of trading firms and venues while the other is a decentralized system, i.e. each trading entity manages and stores the captured data in their own way, and provides access or reports to the regulator by demand.

We will show how the data that is saved on the blockchain is verified and once inserted cannot be modified. As discussed in several articles and papers on the differences between blockchains and databases (Peters and Panayi, 2015[46]), one can say that there is no need to use blockchain technology as a distributed controlled database will suffice for this purpose and is a proven solution for holding large amounts of data. The main benefits presented here by using blockchain technology is the immutability of the data, the ability to validate it programmatically via Smart Contracts, and in the governed architecture proposal, the ease of data access for the regulator with the safety, security, and data separation in the ledger.

This by itself gives the regulator a guaranteed tamper-free audit system which cannot be modified intentionally without leaving a trace of the modification. This is a critical feature for data integrity which is discussed in detail in Peters and Panayi (2015).

One can easily think of a scenario where company A would want to delete/modify their historical trading trail in order to cover a wrongdoing of some sort, resulting in a moral hazard situation where data integrity protocols would be required and a strong governance framework involving scrutiny and oversight from external parties. Alternatively, the process we describe offers this in a more efficient and cost-effective manner. On the other hand, honest mistakes do happen, and trades can be busted/modified as part of a normal trading cycle (most common is cancellation of a trade due to various market reasons), we would want to support this functionality as well. In the coming sections we will propose a work-flow and an architecture built on blockchain technology which answers the event capturing and reporting regulatory demands under EMIR and MiFID II.

12.4.2.2 Centralized Governed Auditing Blockchain

Under EMIR and MiFID II market abuse regulations, all relevant trading events, trade data, and identification data should be captured and stored for five years and be made available for queries from the regulator within reasonable time. The regulator can ask the Broker to provide, in a specified predefined format by the regulator, all saved events by the broker for a certain period. For example, if on day X, the regulator thinks there was an un-orderly behavior or potential misconduct in a certain asset on day X-7, it can ask all brokers and venues that were active in this particular period to show as part of the audited events the activities and names on a set of specified periods. Note, the regulator will know who the relevant participants involved in this period are by using the trader identifiers. They will request these

www.elsevierdirect.com

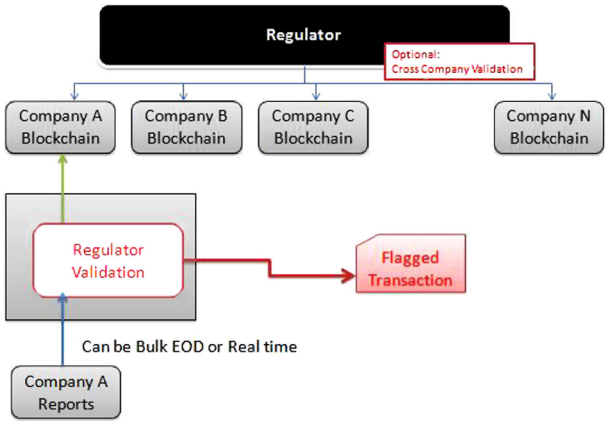


Figure 12.3: Centralized governed auditing blockchain.

individuals or groups to send all captured events, as allowed for under regulatory requirements in EMIR, by the participants for the requested period, in order for the regulator to fully re-construct the disordered period and decide whether there was a market abuse / bad algorithmic trading behavior, etc. and who was the entity causing the disorder in the markets.

To achieve this in an automated and efficient manner, we propose to build a centralized blockchain in which all event data from all participants is stored securely. The regulator will be the controller of the blockchain, and will have permissions to read freely from the blockchain. The contributors, on the other hand, will be able to write and amend their data, but will have access to read only for data that is published by themselves, see Fig. 12.3.

Inserting and Updating: We purpose two ways for a contributor to insert data to the blockchain. One is at the end-of-day as a bulk insert via a predefined protocol, and the other involves the contributor sending the data intra-day to the chain. In case there is an amendment to an event, or if some data was missing and needs to be inserted, the same mechanism will be used.

Reading: Both the controller and the regulator will have access to the full data in the ledgers. After authentication, the contributor will gain access to the data it uploaded to the system to generate reports of its own upon request from the regulator. Note this can be automated with on-chain functionality such as Ethereum smart contract structures, to produce and automatically report to the regulator required fields upon request.

Integrity Validation and Verifications: All events will be validated before being added to the chain, if any missing data in the capture event is present then the chain will reject the event

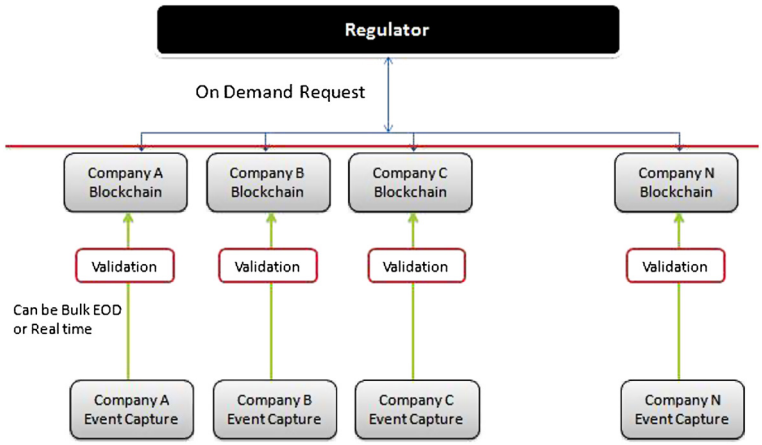


Figure 12.4: Decentralized trading entity audit chain architecture.

and report to the relevant contributor. In order to verify that all events have gone in to the chain, at the end of day / end of bulk load, the contributor will perform a check sum on the number of events they sent to the ledger.

Alerting: One of the possibilities enabled by a blockchain approach is the ability to validate the data entered on submission by running code on the node when data is entered, as this would enable one to flag suspicious activity almost in real time. This is opposed to just validating the integrity of the data as explained in the previous section.

12.4.2.3 Decentralized Trading Entity Audit Chain

In a Decentralized Audit Chain (DAC) architecture, see Fig. 12.4, each trading entity will be responsible for the capturing, storing and managing of the trade events required by MiFID II and EMIR. Using a private chain will ensure immutability and integrity of the data. Then, on demand by the regulator, the entity will send the requested report to the regulator of required trade pre- and post-reporting. The regulator can also request access to the chain in order to verify the integrity of the date themselves, as a second lay of data integrity and redundancy. There is in this case a risk of loss of data, for instance if a company goes bankrupt, and all its data storage is wiped. In order to avoid this the private blockchain will need to reside in a known cloud solution, one of the BaaS solutions presented in section 4.1.3 for example. An agreed, audited, and regulator approved governance structure can be established for oversight of this aspect.

Inserting and Updating: The trading entity will insert all of the required captured events, from market pre- and post-transaction trading activity, to a private chain either at the end of day or on each event in real time. Amends will be inserted sequentially.

www.elsevierdirect.com

Reading: The regulator will have a read-only access to the chain, where they can ask for a specific data in a predefined format. Although the reply is not required to be immediate, by allowing the regulator to request data independently from the chain, we automate the process and make it transparent and reliable.

Data Validation and Verifications: The data is saved on the private chain, with read-only regulator access. We suggest a daily/weekly validation request to check that data was loaded to the chain. The regulator can specify a bespoke contract per entity in order to ensure data validity. Using one of the BaaS solutions or Ethereum for example will ensure that there would be no data lost of loss either by mistake or by intention.

12.5 Conclusions

The ongoing evolution of regulatory requirements relating to transaction reporting pre- and post-trade that are emerging for electronic exchanges is critical for standardization, transparency, stability, and the ongoing integrity and operation of such financial market venues. The recent decade has seen the emergence of several new fragmentations of traditional trading venues, these having been discussed in detail and in response to these new venues, the regulations have evolved. This report also covers key aspects of such regulations with regard to pre- and post-trade reporting requirements.

To achieve these new requirements requires a significant investment in technology relating to data capture, data storage and reporting. This paper details several key components that exchange venues and market participants will need to address in emerging regulations. Then we proposed a novel set of blockchain architecture solutions that will address in an automated manner some key components of the regulatory reporting requirements.

References

4CB, 2012. T2S User Detailed Functional Specifications v.1.2.1. 4CB:UDFS, available at https://www.ecb.europa.eu/paym/t2s/pdf/UDFS_v1_2_1.pdf.

Authority, Financial Conduct, 2016. EMIR – Reporting obligation. Financial Conduct Authority, available at https://www.the-fca.org.uk/markets.

Bank, European Central, 2009. USER REQUIREMENTS – Chapter 16 – STATIC DATA REQUIREMENTS – T2S-07-0366. European Central Bank, available at https://www.ecb.europa.eu/paym/t2s/progress/pdf/urm_mtg9_annex5.pdf?ab791e95d955414cd71ab9a3ac1c59e8.

Bank, European Central, 2012. T2S USER REQUIREMENTS. European Central Bank, available at https://www.ecb.europa.eu/paym/t2s/pdf/URD_v5_02.pdf. Jan.

Bank, European Central, 2015a. Fifth T2S Harmonisation Progress Report. European Central Bank, available at https://www.ecb.europa.eu/paym/t2s/progress/pdf/ag/fifth_harmonisation_progress_report_2015_04.pdf.

Bank, European Central, 2015b. Money Market Statistical Reporting – OMCG Presentation. European Central Bank, available at https://www.ecb.europa.eu/paym/groups/pdf/omg/2015/20150609/Presentation_on_Money_Market_Statistical_Reporting.pdf?540a43eb9987afd41c754cc8ff0940fa.

BATS, 2011. BATS Global Markets agrees to acquire Chi-X Europe. BATS, available at http://cdn.batstrading.com/resources/press_releases/BATS_Chi-X_SPA_FINAL.pdf.

Bloomfield, Robert, O'hara, Maureen, Saar, Gideon, 2015. Hidden liquidity: some new light on dark trading. The Journal of Finance 70 (5), 2227–2274.

Buterin, Vitalik, 2014. A Next-Generation Smart Contract and Decentralized Application Platform. White Paper, available at https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

Buti, Sabrina, Rindi, Barbara, Werner, Ingrid M., 2010. Diving Into Dark Pools. Charles A. Dice Center Working Paper.

Carter, J. Lawrence, Wegman, Mark N., 1977. Universal classes of hash functions. In: Proceedings of the Ninth Annual ACM Symposium on Theory of Computing. ACM, pp. 106–112.

Chodorow, Kristina, 2013. MongoDB: the Definitive Guide. O'Reilly Media, Inc.

Clearstream, 2014. The T2S opportunity. Clearstream, available at http://www.clearstream.com/blob/68228/9f9261051598b77e44bddf291d655859/t2opportunity-pdf-data.pdf.

Commission, Commodity Futures Trading, 2016a. Commodity Exchange Act 7 U.S. Code A 7b–3 – Swap execution facilities, Commodity Futures Trading Commission. U.S. Code, Title 7, Chapter 1, § 7b–3. Commodity Futures Trading Commission.

Commission, European, 2011a. Impact Assessment. European Commission, available at http://ec.europa.eu/finance/securities/docs/isd/mifid/111020-impact-assessment_en.pdf.

Commission, European, 2014. Central Securities Depositories (CSDs). European Commission, available at http://ec.europa.eu/finance/financial-markets/central_securities_depositories/index_en.htm.

Commission, European, 2016b. Investment Services and regulated markets (MiFID 1 & MiFID 2) – Markets in Financial Instruments Directive (Directive 2004/39/EC). European Commission, available at http://ec.europa.eu/finance/securities/isd/index_en.htm.

Commission, U.S Commodity Futures Trading, 2016c. Designated Contract Markets (DCMs) – Part 38 of the CFTC's regulations, 17 CFR Part 38. U.S. Commodity Futures Trading Commission, available at http://www.cftc.gov/IndustryOversight/TradingOrganizations/DCMs/index.htm.

Commission, U.S Commodity Futures Trading, 2016d. Swaps Execution Facilities (SEFs). U.S. Commodity Futures Trading Commission, available at http://www.cftc.gov/Forms/index.htm#SEF.

Commission, European, 2011b. Proposal for a Directive of the European Parliament and of the Council on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council. European Commission.

Commission, European, 2015a. MiFID I legislation in force. European Commission, available at http://ec.europa.eu/finance/securities/isd/mifid/index_en.htm.

Commission, European, 2016. Regulation (EU) No. 600/2014 of the European Parliament and of the Council with regard to definitions, transparency, portfolio compression and supervisory measures on product intervention and positions. European Commission.

Commission, U.S. Commodity Futures Trading, 2013. Core Principles and Other Requirements for Swap Execution Facilities. Commodity Futures Trading Commission, available at http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister051613b.pdf.

Commission, U.S. Commodity Futures Trading, 2015b. Dodd Frank Act. U. C. F. T. Commission, available at http://www.cftc.gov/LawRegulation/DoddFrankAct/index.htm.

Community, FIX Trading, 2016. What is FIX? Fix Trading Community, available at http://www.fixtradingcommunity.org/.

Coron, Jean-Sébastien, Dodis, Yevgeniy, Malinaud, Cécile, Puniya, Prashant, 2005. Merkle-Damgård revisited: how to construct a hash function. In: Annual International Cryptology Conference. Springer, pp. 430–448.

Czepluch, Jacob Stenum, Lollike, Nikolaj Zangenberg, Malone, Simon Oliver, 2015. The Use of Block Chain Technology in Different Application Domains. lollike.org, available at http://www.lollike.org/bachelor.pdf.

Degryse, Hans, Van Achter, Mark, Wuyts, Gunther, 2008. Shedding Light on Dark Liquidity Pools. TILEC Discussion Paper: DP2008-039.

Douceur, John R., 2002. The sybil attack. In: International Workshop on Peer-to-Peer Systems. Springer, pp. 251–260.

FIA.org, 2015. Securities Financing Transaction Regulation (SFTR) and its impact on Commodities Markets. FIA.org, available at Securities Financing Transaction Regulation (SFTR) and its impact on Commodities Markets.

Franco, Pedro, 2014. Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley & Sons.

Gould, Martin D., Porter, Mason A., Williams, Stacy, McDonald, Mark, Fenn, Daniel J., Howison, Sam D., 2013. Limit order books. Quantitative Finance 13 (11), 1709–1742.

Gresse, Carole, 2015. Effects of lit and dark market fragmentation on liquidity. Available at SSRN 1918473.

Halevi, Shai, Harnik, Danny, Pinkas, Benny, Shulman-Peleg, Alexandra, 2011. Proofs of ownership in remote storage systems. In: Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, pp. 491–500.

Kosba, Ahmed, Miller, Andrew, Shi, Elaine, Wen, Zikai, Papamanthou, Charalampos, 2015. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. University of Maryland and Cornell University.

Lazarovich, Amir, 2015. Invisible Ink: Blockchain for Data Privacy. Ph.D. thesis. Massachusetts Institute of Technology.

Linklaters, 2016. Organised Trading Facilities. Linklaters.com, available at http://www.linklaters.com/Insights/MiFIDII/Pages/Organised_Trading_Facilities.aspx.

MaretWiki, 2016. Organized Trading Facility. Markets wiki, available at http://www.marketswiki.com/wiki/Organized_Trading_Facility [Online; accessed 24-August-2016].

Martel, Chip, Nuckolls, Glen, Devanbu, Prem, Gertz, Michael, Kwong, April, Stubblebine, S., 2001. A general model for authentic data publication. In: Algorithmica. Springer.

Matusiewicz, Krystian, Pieprzyk, Josef, Pramstaller, Norbert, Rechberger, Christian, Rijmen, Vincent, et al., 2005. Analysis of simplified variants of SHA-256. WEWoRC 74, 123–134.

Merkle, Ralph C., 1980. Protocols for public key cryptosystems. In: IEEE Symposium on Security and Privacy, vol. 122.

Merkle, Ralph Charles, Merkleerkle, Ralph Charles, Yerkle, Ralph Charles, Students, Ate, Pohlig, Steve, Kahn, Raynold, Andleman, Dov, 1979. Secrecy, Authentication, and Public Key Systems. Tech. rept. www.merkle.com.

Moloney, Niamh, et al., 2002. European Commission Securities Regulation. Oxford University Press, Oxford.

Panayi, Efstathios, Peters, Gareth W., 2015. Stochastic simulation framework for the limit order book using liquidity-motivated agents. International Journal of Financial Engineering 2 (02), 1550013.

Panayi, Efstathios, Peters, Gareth W., Kosmidis, Ioannis, 2015. Liquidity commonality does not imply liquidity resilience commonality: a functional characterisation for ultra-high frequency cross-sectional LOB data. Quantitative Finance 15 (10), 1737–1758.

Peters, Gareth William, Panayi, Efstathios, 2015. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. Available at SSRN 2692487.

Peters, Gareth W., Vishnia, Guy R., 2016. Overview of Emerging Blockchain Architectures and Platforms for Transparency and Pre and Post Trade Reporting from Electronic Exchanges. White Paper, ASTRI and Hong Kong Monetary Authority.

Peters, Gareth William, Panayi, Efstathios, Chapelle, Ariane, 2015. Trends in crypto-currencies and blockchain technologies: a monetary theory and regulation perspective. Available at SSRN 2646618.

Richards, Kylie-Anne, Peters, Gareth W., Dunsmuir, William, 2015. Heavy-tailed features and dependence in limit order book volume profiles in futures markets. International Journal of Financial Engineering 2 (03), 1550033.

Riordan, Ryan, Storkenmaier, Andreas, Wagener, Martin, 2011. Do multilateral trading facilities contribute to market quality? Available at SSRN 1852769.

Securities, European, Authority, Market, 2015a. Consultation Paper Guidelines on transaction reporting, reference data, order record keeping & clock synchronisation – 23 December 2015 – ESMA/2015/1909. European Securities and Markets Authority, available at https://www.esma.europa.eu/sites/default/files/library/2015-1909_guidelines_on_transaction_reporting_reference_data_order_record_keeping_and_clock_synchronisation.pdf. 12.

Securities, European, Authority, Market, 2015b. Regulatory technical and implementing standards – Annex I – 28 September 2015 – ESMA/2015/1464. European Securities and Markets Authority, available at https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-esma-1464_annex_i_-_draft_rts_and_its_on_mifid_ii_and_mifir.pdf. 11.

Securities, European, Authority, Market, 2016a. MiFID (II) and MiFIR – Markets in Financial Instruments Directive (2004/39/EC). European Securities and Markets Authority, available at https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir.

Securities, European, Authority, Market, 2016b. Questions and Answers Implementation of the Regulation (EU) No. 648/2012 on OTC derivatives, central counterparties and trade repositories (EMIR). European Securities and Markets Authority, available at https://www.esma.europa.eu/sites/default/files/library/2016_242_qa_xv_on_emir_implementation.pdf.

Securities, European, Authority, Markets, 2016c. Annex II – National client identifiers for natural persons to be used in transaction reports – ESMA/2016/1064. European Securities and Markets Authority, available at https://www.esma.europa.eu/sites/default/files/library/2016-1064_rts_22_annex_ii.pdf.pdf. ESMA/2016/1064.

Skinner, Chris, 2007. The Future of Investing in Europe's Markets After MiFID. John Wiley & Sons.

Swan, Melanie, 2015. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

Szabo, Nick, 1997. Formalizing and securing relationships on public networks. First Monday 2 (9).

Tauro, Clarence J.M., Aravindh, S., Shreeharsha, A.B., 2012. Comparative study of the new generation, agile, scalable, high performance NOSQL databases. International Journal of Computer Applications 48 (20), 1–4.

Urrutia, Juan Pablo, 2014. Living in the Post-MiFID II World. ITG – available at http://www.itg.com/thought-leadership-article/living-in-the-post-mifid-ii-world/.

Wood, Gavin, 2014. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper.

Notes

1. Boat Platform https://www.theboatplatform.com/.
2. http://ec.europa.eu/finance/securities/docs/isd/mifid/160518-impact-assessment_en.pdf.
3. http://www.cftc.gov/IndustryOversight/TradingOrganizations/SEF2/index.htm.
4. https://www.iosco.org/.
5. https://www.iosco.org/about/?subsection=membership&memid=1.
6. https://www.sec.gov/.
7. http://www.cftc.gov/index.htm.

8. https://www.esma.europa.eu/.
9. https://www.the-fca.org.uk.
10. https://www.finma.ch/en/Order=4.
11. http://www.fsa.go.jp/en/index.html.
12. http://www.sfc.hk/web/EN/index.html.
13. http://www.hkma.gov.hk/eng/about-the-hkma/hkma/about-hkma.shtml.
14. http://asic.gov.au/.
15. http://www.mas.gov.sg/About-MAS/Overview.aspx.
16. http://ec.europa.eu/finance/securities/isd/mifid/index_en.htm.
17. http://ec.europa.eu/finance/securities/isd/mifid2/index_en.htm.
18. http://www.emirreporting.eu/reporting-obligations/.
19. http://www.emirreporting.eu/reporting-obligations/.
20. http://www.cftc.gov/LawRegulation/DoddFrankAct/index.htm.
21. http://www.cftc.gov/LawRegulation/DoddFrankAct/Dodd-FrankFinalRules/index.htm.
22. http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2012-12531a.pdf.
23. https://www.sec.gov/rules/final/34-51808.pdf.
24. https://www.sec.gov/rules/final/34-51808.pdf.
25. https://www.sec.gov/rules/final/34-51808.pdf.
26. https://www.ecb.europa.eu/paym/t2s/pdf/UDFS_v1_2_1.pdf.
27. http://ec.europa.eu/finance/financial-markets/central_securities_depositories/index_en.htm.
28. https://www.ecb.europa.eu/paym/t2s/pdf/UDFS_v1_2_1.pdf.
29. https://www.ethereum.org.
30. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.
31. https://erisindustries.com/.
32. http://hyperledger.com/.
33. https://ripple.com/.
34. https://erisindustries.com/components/erislegal/.
35. http://www.commonaccord.org/.
36. http://p2pfoundation.net/Legal_Framework_For_Crypto-Ledger_Transactions.
37. http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=948326.

38. http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=948326.

39. http://www.coindesk.com/ptdl-group-37-members-post-trade-ledgers/.

40. http://www.coindesk.com/dubai-government-backs-expansive-blockchain-tech-research-effort/.

41. https://menaherald.com/en/2016/06/12/global-blockchain-council-meeting-introduces-seven-pilot-projects-four-new-members/.

42. http://www.coindesk.com/10-stock-exchanges-blockchain/.

43. https://www.leiroc.org/.

44. https://www.gleif.org.

45. https://www.gleif.org/en/lei-data/global-lei-index/lei-statistics.

46. http://www.multichain.com/blog/2015/10/private-blockchains-shared-databases/.

CHAPTER 13

Mobile Technology: The New Banking Model Connecting Lending to the Social Network

Paul Schulte

Contents

13.1 Technological Advances Making Cell Phones a Center of Financial Activity 332

13.2 Speed & Massive Data Create New Industries Overnight on Cell Phones: Alipay & Ant 334

13.3 Insurance Rapidly Changing, Too: Cellular Insurance Empires Being Created Overnight 336

13.4 Why Are Banks & Insurance Sitting Around? Because Regulators Forcing Them to 338

13.5 How Cell Phone Apps Are Taking Away Fees From Banks 341

13.6 Why Asia and Why Now? Asia Is a Tabula Rasa Where Young People Prefer Cell Phone Apps 343

13.7 Amazon, Alibaba, Alphabet, Apple Are the New Bank. These Platforms Threaten Banks 344

13.8 Payments Systems 346

13.9 Two Examples of This in the Emerging World are M Pesa and Its Asian Twin Bkash 347

13.10 The Jewel in the Crown for Financial Technology: SME Lending Through the Cell Phone 349

13.11 Why Is This a Private Equity Phenomenon? The US Jobs Act Is a Big Reason! 350

13.12 Big Data, Crowdfunding and the Small Enterprise (SME): The Magic Formula 351

13.13 Alibaba and Ant Financial's Cloud Business: The Future of Banking 353

13.14 Final Analysis: There Is no Such Thing as Private Information for Anyone 357

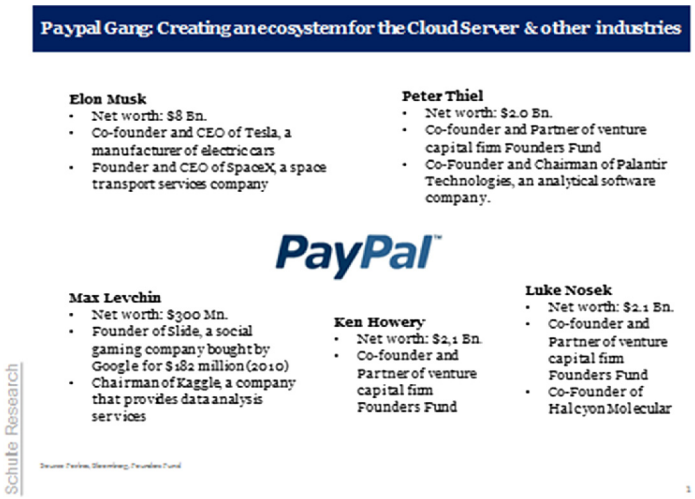
Further reading 359

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00013-9
Copyright © 2018 Elsevier Inc. All rights reserved.

13.1 Technological Advances Making Cell Phones a Center of Financial Activity

After they created Paypal, a few of the owners like Peter Thiel and Elon Musk realized that they had created a vast technological infrastructure which had a host of new potential applications in addition to the tasks required to create a secure payment system. So, they decided to spin out some of this technology and make new applications. Thiel and others have gone on to create many new companies which are engaged in payment systems, data collection, big data analytics, complex systems for trading various assets, quasi-bank lending systems, cybersecurity, credit card activity, and crowdfunding for projects. In similar fashion, the creation of a small company many years ago called Alipay has morphed into Ant Financial, one of the largest financial institutions with a value of $60 bn. And Ant Financial is a financial institution whose business is almost entirely on the cell phone.

The fortunes made from earlier companies like Paypal, Alipay and other payments companies have created a new center of economic gravity. This center of gravity for finance is the cell phone and the social network that the cell phone supports. They have created a new environment for funders with a lot of money who have seen fortunes made from crowdfunding and peer-to-peer funding because banks are in no shape to lend. Ideas are meeting people at a time when great talent is either leaving banks in disillusionment or they are being pushed overboard to cut costs. Money is meeting optimism and talent in institutions which obey the law at a time when interest rates are zero and people are competing against banks which have been torpedoed by angry regulators, hungry prosecutors and upset shareholders. Simply put, a smart man or woman sitting in an investment bank in a career track which is going nowhere has great incentive to go out and make it on his or her own in ways that were undreamt of before. Of course, not all will make it big. But some will.



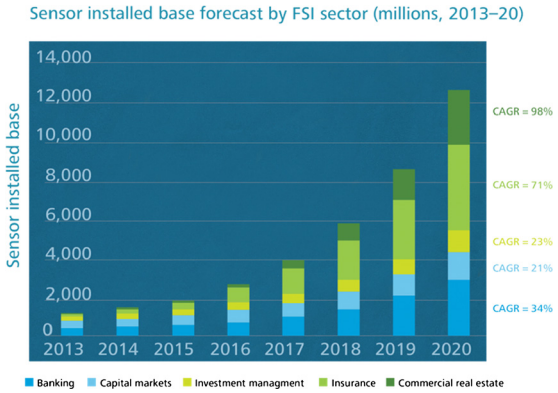
www.elsevierdirect.com

So, we have a perfect storm of energy, momentum and money swirling around creative centers in the Bay area, Bangalore, Berlin, Beijing and other cities while banks are bogged down by compliance, shrinking margins, prosecutions, massive fines, poor morale, negative interest rates, and high costs. The buzz in the world of technology and bandwidth has created a need for speed and bandwidth. It seems that the only thing holding back greater innovation in the phone or the PC is technology. So, firms who know there is profit in speed have brought about astounding advances in speed and bandwidth as witnessed by the chart below. Think about how much we can do on the phone that was impossible only three years ago. From 2014 to 2018, companies like Cisco estimate that the traffic that flows through the cell phone system will increase by 6x – not 60% but 6 times what it was in 2013.

Parameter	2000	2014	2018 Forecast	2000-2018 Improvement (x times)	2014-2018 Improvement (x times)
Global Fixed Internet IP Traffic Petabytes / mth	75	42,000	86,500	1,100	2
Global Mobile Data Traffic Petabytes/mth	<1	2,500	15,000	16,000	6
Processor-No. of Transistors (mns)	21	5,000	80,000	4,000	16

This highway which is not only forcing sudden change on banking but every industry – is being built at speeds undreamt of just a few years ago. This offers vast scope for new types of companies and new types of data management to emerge which can allow local commercial banks to widely distribute financial products and collect money safely and securely. It will allow marketing companies to create entirely new campaigns through social networks. It allows retail to create personalized products and bypass the physical store. It will allow clothing brands to advertise their clothes in 3 D with virtual reality. It allows manufacturing to lower costs, create rapid ubiquity anywhere in the world and at any time – and have perfect fidelity in the ever-cheaper products it sells globally. Education companies can create digital education tools which can reach hundreds of millions of people with no schools. And cell phone financial services can foster innovation, connect anyone in society to any financial transaction – anytime and anywhere. And they will be able to connect cell phone censors to a vast array of censors which are becoming nearly free and ubiquitous. This is causing financial technology to morph into a whole new world of the Internet of Things.

www.elsevierdirect.com



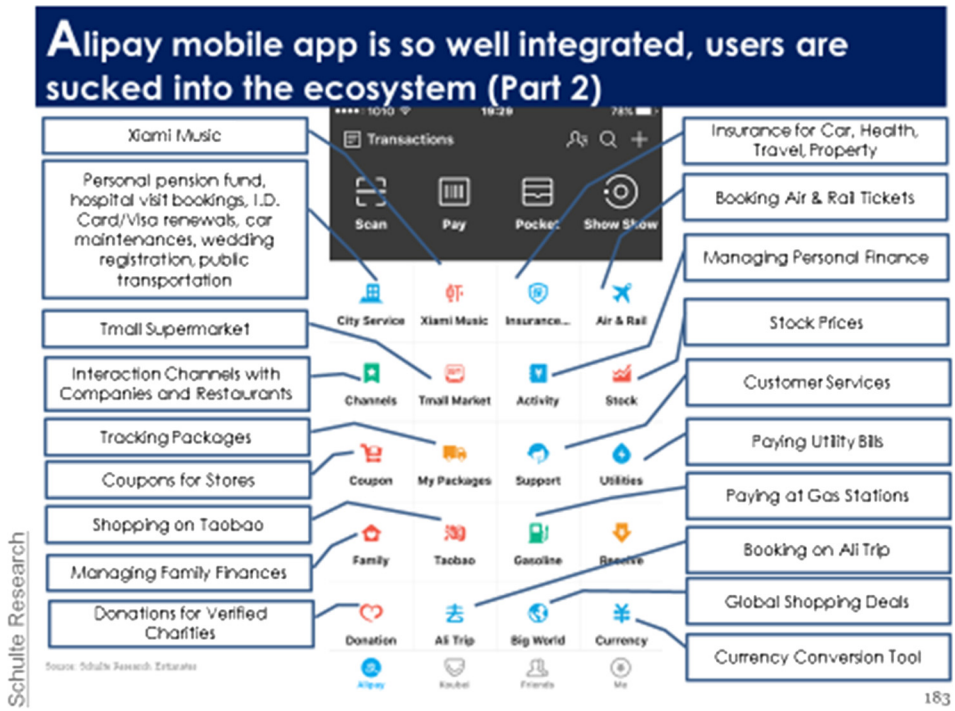
13.2 Speed & Massive Data Create New Industries Overnight on Cell Phones: Alipay & Ant

This need for speed – and ubiquitous information on anything and anywhere – is now wedded to an entrepreneurial class with lots of equity funding to create solutions to unmet needs at far lower prices with far lower costs with more information and data than ever before. This is, in essence, the dilemma of the bank. These companies are reducing complexity by consolidating many functions into one "go to" conduit – the cell phone. They are increasing productivity by eliminating mail and turning the bank branch a museum piece – similarly to the phone booth of old. These companies are increasing the speed and manipulation of data with instant reporting, something most banks have not yet figured out. They are creating clever programs to alert users of financial services about bogus fees being charged by the bank. They are reducing transaction costs and creating greater profitability per transaction, something the high costs banks cannot fight. These new technology companies are saving time, reducing paper trails and eliminating both real and bogus fees which the banks have considered the privilege of an elite few. In essence, financial technology in banking services as well as insurance has now found a back door to the fortress that was "the bank" and is exploiting it in every area. Meanwhile, the banks are unaware of the intrusion and are acting as if all is well when the status quo is changing by the day.

These advances in speed, bandwidth and new products at the same time now allow all of us to do things in small groups which were barely possible with large organizations eight years ago. In the past 15 years, fixed Internet traffic has increased by an astonishing 1100 times. Mobile phone data has increased 16,000 times. These numbers are expected to increase by multiples again as we head into the end of the decade.

The illustration of just how comprehensive these systems have become in a very short time is below – and this is just one small slice of the Alipay/Ant Financial system. The first of

these is entertainment, which includes purchases of movie tickets, games, music, as well as streaming of shows and movies. While many westerners may only watch a few minutes of streaming or YouTube on their phones, it is common in the Asian scene for people to watch a full-length movie on their phone. Secondly, there is a full range of products (most of them owned and managed by Alibaba) in the area of personal finance. This includes retirement accounts, investments, credit score, and insurance. The range of insurance products is staggering – air, transport, car, package return, life, health, "hot day" insurance (37-degree insurance)... on and on. The third area is on the day to day life of a person and this include local and regional transport (taxi, rail, train, bus) and utility payments (gas, electricity, water). As we will see later, this array of product availability will offer city planners great data sets to build smart cities which are more efficient, more eco-friendly and offer better transport timetables, distribution of utilities, and better layout of physical infrastructure to make life more livable.



When we consider how this technology is available to one and all through the cell phone, there are other ancillary industries who want a piece of the pie that has been traditionally reserved for the bank. Telecom companies are becoming quasi-banks. Firms like PCCW, Smartone, PLDT and KT are developing financial applications on their services and receiving

fees. IT firms like Google and Facebook are eating into banking services. Facebook may be creating a new way to connect marketing, funding, advertising, and customer loyalty in new ways which were undreamt of just a few years ago. Apple now has Apple Pay. Credit card firms like Visa, Mastercard and American Express are now reaching out and grabbing traditional banking activity by having cards which are connected to banking accounts and have exclusive arrangements with retailers such as Walmart. Indeed, banks are under threat on all fronts.

Further reading: Schulte Institute for Financial Innovation report: IOT & financial technology: Will the engineers eat the bankers? (Available in "Public Downloads" section at http://www.schulteinstitute.org/)

13.3 Insurance Rapidly Changing, Too: Cellular Insurance Empires Being Created Overnight

This is not just happening in the financial industry. Take insurance for instance. Insurance has not changed in hundreds of years since the East India Company divided up losses among merchants who were transporting goods from Asia to London. The lengthy forms people are forced to fill out today for any type of insurance have not changed in decades. Meanwhile, insurance apps are exploding that offer multiple customized products which can be processed in seconds. In addition, online insurance companies have access to a staggering array of censors that offer information on the security of buildings, the way in which oil platforms are kept safe, how we safely heat our homes, the temperature pipes in the winter and attics in the summer; even how, where and when we drive – and how much time we spend looking at devices when we are driving. Just about every part of life can be measured in ways undreamed of just a few years ago. The chart below shows the ubiquity of censors over the next few years. The prices of these are collapsing and the capacity to install them is virtually limitless. This is a new way to determine risk of fire, accident, exploding frozen pipes, heart attack, diabetes, car collision, oil rig fires, warehouse storage safety and many other risks in life. The chart below shows that we will see a 6-fold increase in the amount of information about our physical lives which will be collectible not only over the phone but also from censors in just about every physical manufactured object.

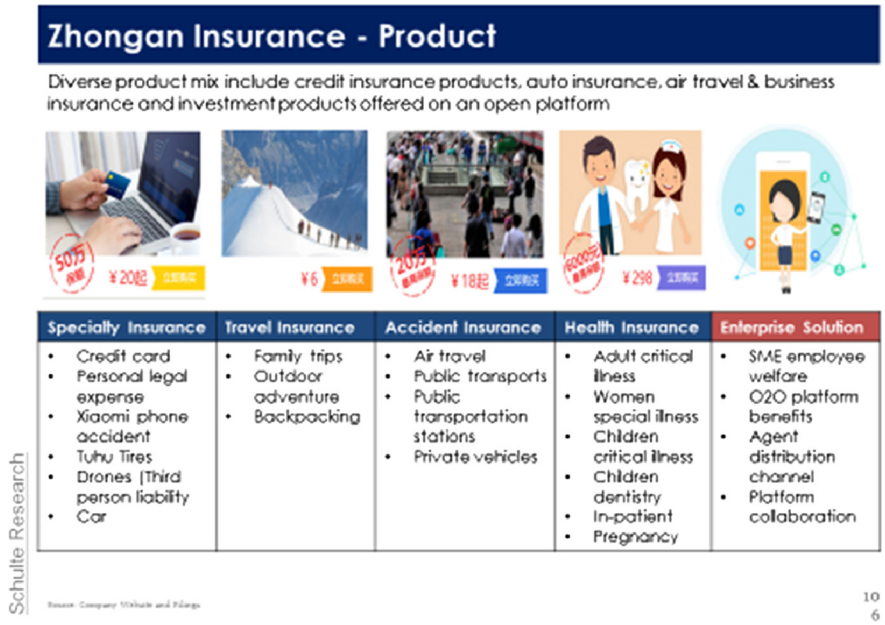
Case Study 1: Zhong An Insurance. The biggest on-line insurance company nobody ever heard of

Financial crises cause central banks to drop interest rates (in many countries, rates are in negative territory) and capital becomes very cheap for those with access to it. So, capital becomes

very cheap relative to expensive labor. Where is labor more expensive than in banks and insurance companies? Wages in banks are among the highest, especially in investment banks. So, anyone with a viable product which is a replacement for a product offered by an investment bank (or an insurance company) will very likely be able to provide this product or service to current customers of the banks at a fraction of the price.

Furthermore, these people have access to cheap real estate relative to the very expensive real estate of the banks, which are always in the premium "central business district". The case of Zhong An above is a perfect case in point. It now has 400 million customers and ZERO agents. They have sold almost 5 billion policies without a single insurance agent or a vast array of offices that is occupied by hundreds of agents.

The illustration below shows the vast scope of Zhong An. ALL of these products are available on the cell phone. ALL of them can be purchased without talking to a single agent. ALL of them are available through one consortium. The illustration below shows the vast scope of products available. In addition, the data behind the products comes from hundreds of millions of people and, therefore, can be distributed to millions of people with highly accurate risk parameters on each person. This level of detail in terms of how different people behave differently is unprecedented and can replace much of the historical methodology which is obsolete.



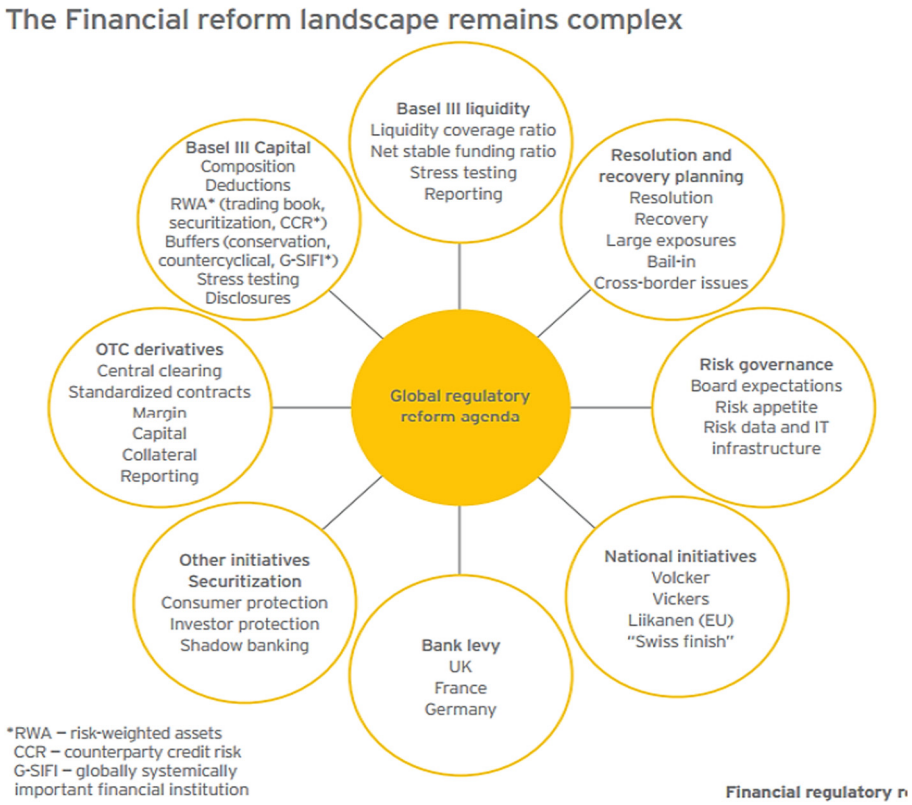
www.elsevierdirect.com

The first category of insurance is specialty insurance. This includes credit card theft and fraud, legal insurance for personal online theft, cell phone damage, tire damage to your car, damages from accidents with drone cameras, and automobile insurance. One can see how these insurance products blend into each other. Insurance can be purchased for multiple types of insurance. These include backpacking, outdoor adventure like skydiving, rafting, ocean journeys and many other types of insurance. The accident and health insurance products are more standard and include air travel and travel in other people's cars. The interesting new product – insurance for each time you buy a train or public transportation ticket – is insurance against an accident in public transportation. Imagine how CNY 1 adds up for millions of travelers each day.

Further reading: Schulte Institute for Financial Innovation report: Insurtech: Is Traditional Insurance on the verge of extinction? (Available in "Public Downloads" section at http://www.schulteinstitute.org/)

13.4 Why Are Banks & Insurance Sitting Around? Because Regulators Forcing Them to

The chart below shows the issues at hand for banks globally. They have regulatory issues with compliance with Basel III being implemented now. Basel IV is around the corner. They have issues with derivatives. They need to pay attention to liquidity considerations which make it hard to lend. They need to adhere to many local regulatory issues. They need to make sure that any technology advances they do make are cleared by regulators. They need to adhere to new rules for consumer and investor protection. In addition, the US banks need to adhere to regulations and new rules (which require constant interpretation in all jurisdictions in which they operate) from an assortment of alphabet soup agencies. These include the CFTC, the Comptroller of the Currency, the SEC, FINRA, the Federal Reserve, the FDIC and the Office of Research at the Department of the Treasury. These are seven agencies with various kinds of teeth to cause damage to banks as well as to impose fines and/or imprisonment. No wonder banks are simply not in a very creative mood at the moment!



Another very thorny issue which is preventing banks from jumping onto the bandwagon of innovation and creativity with regard to the cell phone is that the tax man needs more revenues everywhere and there is little patience for banks which have made great sums by being in the business of tax avoidance. The Swiss banks come to mind on this. US banks, in particular, are under great administrative strain as they force their American customers everywhere to comply with onerous administrative guidelines on any kind of transaction of even a few thousand dollars. The Foreign Account Tax Compliance Act makes many international financial institutions nervous about working with individual Americans or American financial institutions. It is not exaggeration that if an American seeks out a private bank in Asia, they will be met with a cold shoulder. Foreign banks who have solid high net worth businesses are shunning Americans because they are afraid of unintended violations of law amidst the mountain of paperwork required for every transaction. Foreign banks are terrified after watching Standard Chartered receiving a fine of $300 million for a minor breach of money laundering.

A poorly understood but very important change in regulation has to do with subsidiarization. Excessive loan/deposit ratios have caused countries to become dependent on whimsical

wholesale funding from the overseas branches of international banks (also called universal banks). Regulators in several countries have caught on to the danger of large amounts of loose capital coming in one moment and then leaving the next. So, regulators are now telling banks that they can only lend inside a country if they set up a subsidiary, capitalize it and then fund themselves only with whatever deposits they can scrounge up inside the jurisdiction. This means that wholesale banking will die on the vine. I personally think this is a good thing because it will prevent sudden financial meltdowns.

This should not be seen as capital controls. It is the opposite. Regulators are saying, "Please come to our country and do business with us. The only catch is that you can lend only as much as you can create in LOCAL CURRENCY deposits." This creates great scope for local banks to utilize new financial technologies to compete with global banks in new areas.

So, we can see that the tax man, the sheriff, the DA, the attorney general, class action lawyers, and regulators are making life for banks very difficult, indeed. I have gone through these many roadblocks because so many people ask all the time why the big international banks are just sitting around and watching so many of their divisions being picked off or closed one after the other. In summary, these banks are dealing with 'hard to change' DNA issues, regulators, class action suits, prosecutors, legacy derivative issues form the crisis, Basel III compliance, new rules on global tax reporting, a US Treasury Department crackdown on conduct in the Middle East, and subsidiarization rules.

As a result, global banks are behaving like a person who has suddenly and unexpectedly walked into a brushfire. They are very busy fighting fires with regulators, prosecutors, lawyers, compliance officers, social responsibility panels, human resources and other entities which are both external and internal. How can they focus on their core businesses, never mind adopt new and often untried technologies which smaller and nimbler banks or fin tech companies are adopting in a very aggressive way? And virtually none of these large financial technology companies have committed any kind of crimes. So, the regulators are giving them far more room to maneuver compared to banks.

Furthermore, local banks are free of one heavy burden that larger banks have. Global banks like HSBC and Standard Chartered operate in more than fifty countries and they must make sure that technologies they adopt are suitable for various jurisdictions which may have utterly different views on client confidentiality, disclosure, customer protection, capital commitments and so forth. So, implementation of new initiatives can be problematic and cumbersome.

As an example of how and why some large institutions may lack the "DNA" to change, one senior IT specialist at a major European bank told me that when he created one line of code, **it takes two weeks to get approval**. In a world where one initiative needs thousands of lines of code, it is virtually impossible to be adroit and aggressive in a new industry such as financial

technology where there are many hungry and aggressive upstarts. Being an upstart is the nature of the beast in financial technology and new innovations are coming at a fast pace. As an example, while some global banks are still discussing the merits of aggressively implementing new deposit/checking/FX/stock activity on cell phones, smaller banks like Santander, BBVA, Commonwealth Bank of Australia, and BCA in Indonesia are aggressively moving forth.

The way in which banks are behaving relative to new technologies has all the signs of behavior we see in a sunset industry. Some of these banks have a siege mentality when it comes to new technologies. In addition, managers become risk averse as banks shrink divisions and create less room for promotion. So, managers become more conservative and make decisions that will please their bosses rather than create new business. Middle managers hesitate and ignore customers. New businesses prove too risky, since failure is a sure way to get thrown out. Office politics and short term-ism rule. Flexibility and aggressive moves to get new business are ruled out as too risky. Businesses go sideways. Profitability suffers. People become more risk-averse. A downward cycle is created from which it is hard to recover. (We will also see later that banks like Goldman Sachs have avoided this by aggressively changing and buying new technology in multiple divisions.) For a deeper discussion of this phenomenon of corporate risk averse behavior at a time when aggressive change is desirable, see Christianson's The Innovator's Dilemma.

Further reading on bank regulation: See Schulte, The Next Revolution in our Credit Driven Economy: The Advent of Financial technology, Wiley & Sons, 2015

13.5 How Cell Phone Apps Are Taking Away Fees From Banks

Many upstart companies are a small but they are quickly forming a constellation of meaningful revenue and creating ecosystems in order to accumulate a pool of big data to make robust conclusions about how risk-averse one person is from another. Startups also have access to new, cheap and powerful technology which makes small groups suddenly highly efficient and competitive. The equation for land, labor and capital now changes and allows small groups of entrepreneurs to go on the attack in virtually every area of a commercial or investment bank because they have reams of data which were previously only available to those with large amounts of money who could buy data expensive storage and algorithms.

The price for data analytic systems and data storage is collapsing. So is the price for sensors. So, more data can be collected from more places than ever before and it can be stored more cheaply than ever before. Almost all of these have as their ecosystem the mobile phone. There are, literally, dozens of well-funded companies which are challenging many parts of the

banks. The illustration below shows how many companies have cell phone services which are currently challenging the services that are offered on the cell phone portal of HSBC. There are 13 well-funded payments companies which are competing for this business globally. There are 8 offering competing loan structures or comparison loan platforms. There are 8 offering various forms of financing. There are 6 offering various forms of transfers. And 5 are offering mortgage deals. And these companies are the ones which have received funding in the range of $10–50 million. There are dozens behind these who wish to become larger in many different areas.



This revolution of the mobile phone with regard to banking services is also having a profound effect on traditional banking services as well as insurance. It is even calling into question the value of the physical bank branch network. If a new depositor can access his or her banking information on the phone, deposit money, conduct transactions, engage in foreign exchange movements or even make investment decisions, the physical bank branch becomes an unnecessary (and very expensive) trapping of the days of old. In addition, the surveys being done

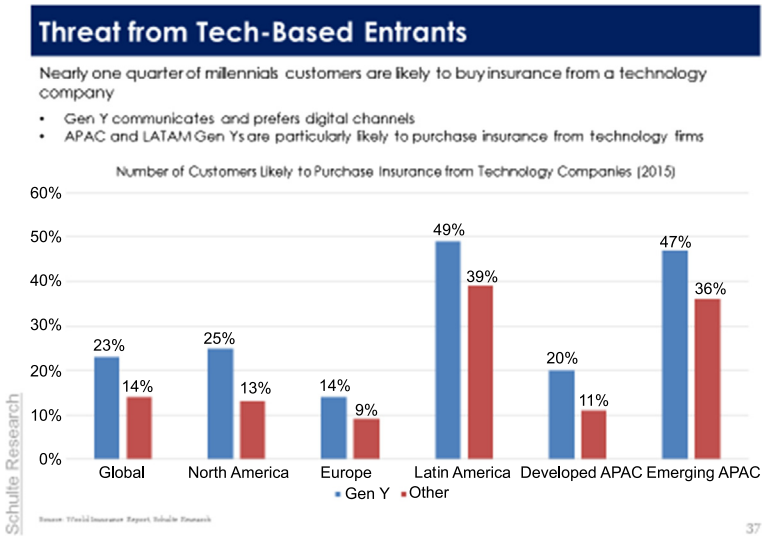
recently show that people visit their phone dozens of times each day and yet may visit their bank Internet site through their phone once or twice per week. This is causing people to gravitate toward cell phone apps and away from the traditional websites of banks. This is another way of saying that banks are increasingly finding it difficult to integrate their systems into the "social network" of people's lives. This social network includes sites like Wechat, Taobao, Facebook, Whatsapp, Paypal and many other commonly used sites found on the phones of most people.

Further reading: Please see the Schulte Institute for Financial Innovation: The Fin tech Bible: C 4. Payments Solutions. (Available in "Public Downloads" section at http://www.schulteinstitute.org/)

13.6 Why Asia and Why Now? Asia Is a Tabula Rasa Where Young People Prefer Cell Phone Apps

Nowhere is this truer than in Asia, where many of the traditional "trappings" of finance are absent. Many Asian countries have tens of millions of people who do not even have a bank account. Many countries have no entrenched credit card company who can impede progress. And many have entire parts of the country which do not even have bank branches. Therefore, there are fewer entrenched interests which are trying to hold back progress for the simple reason that they are themselves not ready for change. Asia will have two billion unique smart phone users by 2019, according to Manulife. These increasingly sophisticated cell phone users know what is available. They are increasingly intolerant of the painful experiences of banks and demand easy to use services on their OWN phone in their OWN system. They do not want to switch over to the system of the bank in order to make choices. People use their phone dozens of times each day. They might use their bank app once a week. They do not want a "one size fits all" approach. They want customized solutions to THEIR problems.

The chart below shows the profound difference between the preferences of Asians and their counterparts in the US and Europe. Half of Asians surveyed said they are likely to buy their insurance products online rather than an agent. This is bound to increase quickly. This compares to only 14% for Europeans and 25% for those in North America. Millennials have no need for agents and will become older and wealthier without seeing bank tellers, wealth managers or insurance agents.



13.7 Amazon, Alibaba, Alphabet, Apple Are the New Bank. These Platforms Threaten Banks

Now, let's take a look at the more traditional banking side of the business and the new technologies which are coming along and putting a dent into the traditional banking activity. Crowdfunding originally was a response to the effects of the global financial crisis. Banks were saddled with losses, fines, prosecutions, reduced capital and general fear of the market and loans dried up. So, ingenious people came along who tried to create new forms of credit. Crowdfunding is just one of these responses.

Crowdfunding has morphed into several variations on a theme. One of these is a system whereby consumers pre-purchase the initiators services of products which is widely used by artists, musicians and film producers. (Watch what Alibaba does with Lionsgate Films on this. The companies have agreed on pre-funded films which Alibaba will stream inside China. This is a new form of film-funding which is truly exciting and could alter the economics of film-making.)

Another is widespread equity funding of companies by individuals. This is true capitalism as it is a diversified group of people using nothing but cash to fund a good idea. There is no bank debt. There is no banker. It is a crowd of people who are willing to fund a good idea. (This is at the heart of Kickstarter and is true diversification.) Let's remember that stock markets are now just a big ETF where money that goes into equities is spread equally over all stocks in the Dow 30 or the S&P 500.

The table below shows a few of the leading contenders which have had a big influence in the world of crowdfunding.

Company Name	Largest Investor	What they do .	Who can it threaten?	Comment
Bilbus	Seedcamp	Financing, e-Invoicing, and cash flow forecasting. Strengthening working capital.	• White collar: Accounting professionals, Commercial bankers	• Will annihilate the back office
FeeFighters	Hyde Park Angels, (Acquired by Group in April 2013)	Helps compare payment providers to find the cheapest merchant account provider, or credit card processor.	• Square and other existing payment disruptors. • Beating banks but now these disruptor firms are cannibalizing each other	• Deflationary
FundingCircle	Union Square Ventures	Peer to Peer platform connecting investors with established business who want to borrow in the UK.	• Bank margins and the physical need for a banker.	• Deflationary
Iwoca	Talis Capital	Flexible funding structure for ecommerce sellers relying on credit score transaction data & business's selling accounts.	• Bankers and physical banks.	• Deflationary
Kabbage	Thomvest Ventures, David Bonderman,	Online provider for working capital to small business. Lends money by gathering data sources from eBay, Amazon, UPS, PayPal to determine loan amount.	• Bankers and physical banks.	• Smart. Celebrity funding list
Fund2Me	N/A	Allows entrepreneurs to list their ideas, and connect with investors for funding purposes. First campaign is expected to be launched in Dec 2013	• Bankers and physical banks.	• May attract small businesses from China to seek funding in Hong Kong through online investors.

From 2011 to 2013, the amount of funds raised by crowdfunding had grown from $1.5 bn to $5.2 bn. And the number of crowdfunding platforms had more than tripled. North America and Europe currently dominate, but Asia is, I believe, catching on quickly. These crowd-funded projects tent to be short in duration. They are launched quickly and usually completed in about 10 weeks. Some commercial bankers may want to say that this is only a drop in the bucket or that this is an untested fad which is bound to blow up. This view may be naïve. A multi-billion ecosystem is building up around these companies – and dozens more which is a new form of funding which also includes marketing, advertising and buzz for new products.

This new ecosystem is being created which involves funding, entertainment, marketing, advertising, and social networking. It integrates crowdfunding with Facebook and other crowd venues (such as Kickstarter and the ones named above) to create a way to fund new ideas for products which is tied into the advertising for the product, ideal demographics for the product, and a self-feeding buzz which can catapult a well-funded product using nothing but word of mouth and the ever-present "Like" button.

A fascinating documentary on this is a PBS Frontline show called Generation Like. (https://www.youtube.com/watch?v=1gmgXxB9QiA). These established companies and

upstarts which are helping to create demand for new products are morphing into a new ecosystem which involves value-added advertising, marketing, and social buzz from the social network of millennials. Unlike the banks, none of these companies are facing multiple criminal charges. They are using social media like Facebook to create sales for new ideas which would never be funded by bank credit. Furthermore, some brands are literally created overnight and receive funding overnight because millions of people on Facebook click "Like". In turn, these new companies create a generation of devoted customers who can bypass traditional financial services because they are technologically savvy and can use alternative means to spend, invest, and save their money.

13.8 Payments Systems

The traditional retail sector mentioned above (books, magazines, tacos, household items, luxury items, cosmetics, etc.) is in a tailspin because virtually anything anyone wants to buy anywhere in the world is available online for a lower price. Needless to say, this is all deflationary due to the hyper-efficiency with which companies like Amazon interact with these payment systems. The world of payments moves away from physical/retail activity with high rents to a private cyber-world of private purchases of ever cheaper items. All of this can be done more efficiently, more quickly and with instant global pricing comparisons and payments which will always search for the ever better discount. The long and short of this is that Amazon is becoming a bank and is doing so in a deflationary manner. And much of the information to allow this new ecosystem to flourish is found on the phone.

Company Name	Largest Investor	What they do.	Who can it threaten?	Comment
AliPay	N/A	Can provide 500 mn customers with all bank services without a physical bank. Allows individuals and businesses to execute online payments.	• Providers of individual payment systems (cards-only, online transfers.) PayPal.	• No legacy technology. Breaking the rules. • Keep an eye on Yuebao (collectively received RMB 6.6b in deposits from Alipay users)
Adyen	N/A	Improving the efficiency of online and credit card payments as well as offering face to face payments.	• Providers of individual payment systems (cards-only, online transfers.)	• Well established. Should be able to increase its marketshare.
BitCoin	N/A	Digital currency that allows P2P transactions. An alternative FX	• Central banks, real FX. • Macro-economists.	• Gimmicky?
Dwolla	Union Square Ventures, Village Ventures,	FX movement at low or no cost.	• Providers of payment systems, payment terminals	• 5 years old
Square	Starbucks Citi Ventures	Allows users to swipe credit card through the use of smartphones All in one payment, inventory management, ordering, item sharing.	• Providers of payment systems, solutions and terminals.	• Marquee list of participants. Have raised over $300 mn • Antifraud system that shows where the transaction was made.
TenPay	N/A	Bolting credit card API to the phone and bypassing cards.	• Providers of payment systems (cards-only, online transfers.	• No legacy history. Breaking all the rules.

www.elsevierdirect.com

Second generation payments have already begun and are moving the system in different directions, mostly through the cell phone. This is similar to the way in which funding is tying itself to social networks. These payments systems are also tying themselves to social networks. Not only are these companies such as Klarna, Venmo, and Stripe easier and cheaper to use than existing payments systems, they are now flexible enough to be attached to social network entities like Facebook where people can combine their social activity with their financial activity with the click of a button. The differences among and between checking accounts, savings account credit cards, and charge cards blur and companies can even offer a "bridge loan" in funding of purchases. See the table below for more details about how these companies operate. These companies have high margins and, despite being around for a few years, have strong profit generating power. Many banks are nowhere to be found in this area.

- **Venmo** is a payment app that you can send money instantly for free with social networking functions. Payments can me made with friends. Money can be held in a in Venmo account, or "cashed out" to a checking account.
- It is Fun, simple and fast. The goal: accepted like Visa and used like Facebook

---

- **Klarna** was founded in 2005 and it a Swedish-based e-commerce company that provides payment services for online storefronts. They assume stores' claims for payments & handle customer payments, thus eliminating the risk for seller and buyer.
- Most payment systems, like PayPal, require users to have money in their account or a credit card on file before they can buy. But, Klarna underwrites the financial risk for retailers until people pay for the goods, either right after checking out or when the product arrives in the mail.

- **Stripe** was Founded in 2009 and is an application programming interface that can be embedded on websites to accept payments. (no merchant account).
- Stripe charges 2.9% + $0.30 per charge, the same rate set by PayPal w/ no fees for setup, monthly use, minimum charges, validation or card storage.
- Stripe has $130 million in funding, and valued at $1.75 bn. Ex-Paypal investors

Further reading: See Schulte Institute for Financial Innovation paper Tech Bible P2P Lending (Available in "Public Downloads" section at http://www.schulteinstitute.org/)

13.9 Two Examples of This in the Emerging World are M Pesa and Its Asian Twin Bkash

M Pesa was created ex nihilo in Kenya about 10 years ago and, within a few years, became the center of an ecosystem for payments – without any banks branches. And it did it without any electricity or roads. Like Paypal and Alipay (Ant Financial), it then morphed into a much larger ecosystem for remittances, payroll, and payments for utilities such as clean water and solar power. In similar fashion, the Kemal brothers went to Nairobi and patiently sat there – and learned. They then returned to Dhaka and built a system for Bangladesh. When I interviewed Mr. Kemal, he made a few salient points. First, no system is entirely transportable. They are not fungible. Many alternations need to be made based on culture, technology, physical infrastructure, and entrenched interests. Second, once the systems are established, people

may use their cell phones for different purposes. One country may have a strong preference for use as remittance. Another for payments. Another for calling. And yet another for payroll.



Each countries' experience will be different based on lobbying power of existing players, government support from the top, existing technology, demographics and so on. GoJek is another phenomenon in Indonesia which is a pure cell phone business which can deliver just about anything to anyone anywhere by motorcycle. And it has a range of quirky services which can be brought to your home in a few minutes – from salonists and pedicurists to legal documents. This business is valued at $1.5 bn and there are limitless opportunities.

Then let's take Rakuten. It is the creation of Mr. Mikitani. It precedes Alibaba a bit, but I believe that much of the DNA of Alibaba came from Rakuten. Rakuten is the fourth biggest bank in Japan and few have even heard of it. It acts much like Alibaba in Japan. It does payments, deposits, investments, travel, and many more things. And almost all of this is over the phone.

It is important to remember that the systems of M Pesa and B Kash now command the financial systems of Kenya and Bangladesh, respectively, almost entirely over the cell phone. Neither of these companies has bank branches. They have no bank tellers and no SVP or managing directors in branches across the country. This is for the simple reason that the physical infrastructure is lacking in terms of roads, electricity, and MBA programs. Imagine what will happen in countries like Vietnam, Laos, Cambodia, Philippines, and Myanmar when these countries get going with cell phone technology. This phenomenon is just getting started.

Further Reading: Please see Schulte Institute for Financial Innovation report on Rakuten. (Available in "Public Downloads" section at http://www.schulteinstitute.org/)

13.10 The Jewel in the Crown for Financial Technology: SME Lending Through the Cell Phone

Most businesses are small businesses, but it's true. Of 27 million businesses in the United States, 21 million have less than five people. This means that almost 80% of the firms in the US are small businesses. Now, we add to this the statistic that banks reject 80% of small business applications. And let's add in the fact that loans to small businesses during the global financial crisis have fallen by 30%. We have a starved market where potentially millions of customers have no access to credit to start businesses. There are similar statistics in Asia. Many center around the reality that at least 80% of businesses are bypassed by traditional banks and most of these are forced to pay extortionate rates for business. These rates can be 15–20% per month. Name a business that has returns of 20% per month. Why is this? It is because for decades, loans to small businesses have been in the "too difficult" category. This SME technology is just starting and many companies like Kabbage are in the forefront of new lending with highly reliable data analytics.

Companies that have come forth to fill this enormous gap include Kabbage, Kickstarter Kiva, and Indiegogo. The illustration below shows their businesses, profiles, deal structures, and other data. Many people now call these people citizen lenders. Lending Club is a variation on this theme as it collects a pool of capital and is more like a private equity firm in that it offers an internal rate of return to those who fund the entity. Kickstarter, Indiegogo and Kiva do not have any sort of interest rate charged on funds. It is pure equity in return for a pre-arranged product, reward, or service.

The companies above have made terrific inroads into the world of crowdfunding. The amounts are low – only a few billion. But, these companies are a few years old. Furthermore, there are many more behind these four companies. Another which is growing quickly is Funding Circle which has now a lending portfolio of almost $500 million. It was only founded 16 quarters ago. And its current non-performing loan rate is 2.2%, on a par with the UK banks which have been offering loans for decades. Why is this happening? Dan Hyde in 'This is Money' said that a survey of almost 80% of borrowers prefer to go through peer-to-peer funding over banks if they are seeking a loan. This is important and banks should pay attention to what is a powerful global trend which is, I believe, only just starting.

There is another important reason why this is happening. An important theme of this book is the way in which banks have earned the enmity of the common man while other companies have come along over the past decade and earned respect. The effect of branding is extremely important. Financial technology companies have not only preserved their brand value but also have dramatically improved their branding while the branding of the banks has fallen sharply. For example, one survey from Accenture asked: "What company would you pick if it were a bank?" 50% of people polled would prefer companies like Square, Paypal and Apple also

www.elsevierdirect.com

preferred. One out of four people would prefer a branchless digital bank. More than 70% of people polled saw a bank as nothing but a transactional institution and had no personal ties to it. For now, anyway, the regulatory, legal, branding, and reputational winds are very definitely blowing toward financial technology and away from traditional banking. Many banks have tossed their reputations overboard in the past few years. At the Annual General Meeting of shareholders of Deutsche Bank, one disgruntled took the microphone and asked the assembled board of directors, "Is there any scandal in which Deutsche Bank is NOT involved?" That says it all.

Further reading: See Schulte Institute for Financial Innovation: See fin tech bible P2P Part B (Available in "Public Downloads" section at http://www.schulteinstitute.org/)

13.11 Why Is This a Private Equity Phenomenon? The US Jobs Act Is a Big Reason!

Access to Congress and steady behavior creates influence. According to the Silicon Valley Business Journal, in the latest election cycle, Silicon Valley's biggest political contributors gave more than $50 million in campaign donations, making this group one of the largest contributors in the country. Interestingly, the split was roughly 55% Democrat and 45% Republican. Of the 13,000 individual citizens who gave the most, almost one third of this group came from Silicon Valley. As campaign contributions shift away from banking toward financial technology, regulations will change. One example of this was the Jobs Act. Aimed at promoting private equity rather than bank debt as a means in setting up entrepreneurial activity, the Jobs Act passed in the House by a vote of 390 to 23. This bill legalized equity-based crowdfunding and was less than 50 pages.

In the past few years, there has been rapid progress in the area of regulations and laws on financial technology. The UK bas been in the forefront, especially in London where Mayor Boris Johnson pushed hard to make London a center for financial technology. Singapore followed soon after with a host of interesting and creative solutions to get companies to move to the island nation. Interestingly, though, the one country with one of the most liberal and imaginative policy frameworks for financial technology has been China. It is for this reason that companies like Alibaba are years ahead of many similar companies in the West. The government has been fundamentally supportive to these efforts.

See the Schulte Institute for Financial Innovation comparison of new laws and regulations for financial technology: US, UK, China, Malaysia, Singapore and India. (Available in "Public Downloads" section at http://www.schulteinstitute.org/)

13.12 Big Data, Crowdfunding and the Small Enterprise (SME): The Magic Formula

In the past two years or so, a new chapter is being written and financed by private equity. If there is a new capacity to sift through vast amounts of information – billions of bits of information on consumer habits in seconds. If there is a new source of gathering capital through crowdfunding, why not combine these together to create a new way of lending in ways that banks cannot do because they lack the flexibility, regulatory goodwill, innovation, and ingenuity to do this? In other words, if a company like Intuit or Indinero comes along and offers software to help companies manage their receivables or payables, won't this information which is shared with crowdfunders or smaller more flexible banks (and highly accurate) allow these institutions to gain confidence to lend to various companies since they will have a better picture of the liquidity conditions of a company? What if these companies went further and offered software to help these companies manage tax, payroll, and overall working capital considerations? All on the cell phone with multiple options for financing, vendors, and exchanges?

If these new-fangled finance companies who can gather pools of capital and also manage the real-time software which is a constant examination of cash management, then they can become a genuine partner of a logistics or manufacturing company and feel comfortable investing with them. They can have true and accurate information on taxes, payroll and working capital. Furthermore, these lending pools can bypass ratings agencies which have tarnished their reputations by spurious rating activity which helped the issuer more than the buyer of debt. This is precisely what is under way in a big way globally. The epicenter of this is in the United States, but it is spreading quickly to other parts of the world. I believe this phenomenon is only hitting Asia now. The one bank in Asia which is rapidly implementing this idea is Commonwealth Bank of Australia (CBA). CBA does not sell this software. It gives it to companies for free. In this way, both the company and the bank act as a partner and can have transparent information each day at 9 AM about the liquidity conditions of their company.

These smaller, entrepreneurial organizations now have the capacity, the technology, and wherewithal to break into the SME market. And they can do it because monolithic banks are in legal and regulatory quicksand. Think about it. The largest unmet need in the world is the small and medium sized enterprise. This is a company with between USD 500,000 and $8 million in revenues that has anywhere from 3 to 30 employees. There are millions of these companies, especially in the emerging world. And they are utterly blocked from bank credit for an assortment of reasons.

One of the reasons why growth is not higher in the emerging world is that there is a plutocracy of wealthy, landed gentry which have access to credit (it seems that it is only ever a small

number of families – between 8 and 20 – which control economics in the emerging world) and tens of thousands of small companies which are deprived of credit. These companies are forced to get credit from often unregulated financial entities or outright loan sharks. They pay extortionate rates of interest in the neighborhood of 30–40%. What if they bought software (or were given software) by a crowdfunder who could monitor and verify the weekly or monthly operations of this entity by watching its liquidity conditions, payroll, tax payments and working capital requirements. A crowdfunder (or a smart bank) could quickly command market share and clean up for one simple reason. These entities which could have comfort by analyzing (on a daily or weekly basis) the cash balances of a company could lend to these companies and charge interest rates of 15% or 18% with a high degree of certainty. The company doing the borrowing at 18% would see these rates as a tremendous relief compared to extortionate levels of borrowing rates of 40% which the company was paying in the past from very unpleasant loan sharks and the like. Everyone wins. Word will spread and others will join the bandwagon. Some of these small companies will become big companies and a virtuous circle will ensue. Ecosystems will form and banks will either be forced to change or will create the seeds of their own demise by refusing to grasp technological change.

Companies like Kabbage can go further and enter into the world of the individual. It can turn the analysis of data into a micro event and offer money to people based on elaborate analysis of their e-commerce activity. Kabbage can offer cash in one day. Companies like UPS have entered into agreements to allow Kabbage to examine shipping histories. Kabbage is growing at more than 250% pa and if it achieves some kind of critical mass, there is no telling what it can do with smart analysis of big data. The savings to the customer could be enormous.

Comparison of SME Lenders: Kabbage is new business model

SME Lenders	Kabbage	PayPal Working Capital
Loan Amount	$2K to $100K	8% of PayPal sales
Repayment	6 months	Daily, payments via Paypal
Repayment Method	Monthly	10% - 30% of Rev
Qualifications	Borrowers link online biz	Paypal user

Schulte Research

44

The growth rates for cloud traffic are astonishing not only for the US but also in China. As expressed in exabytes (10 to the power of 18 bytes or one billion gigabytes), the traffic from 2012 to 2014 doubled. It is expected to double again by 2016. This represents a 40% compound growth rate for the period of 2012 to 2016. For the period from 2012 to 2017, Asia is expected to have the fastest growth. This is largely in China. Of this the consumer and business will grow at about the same rate. Asia pacific is expected to grow from 505 exabytes to 1900 exabytes by 2017 – a fourfold increase. By 2017, it is interesting to note that Asia Pacific is expected to equal North America in exabyte traffic. On this score, let's compare the trends in the US to the trends in China.

In the US, the Paypal gang is busy ramping up the system to a new and stratospheric level of superpowerful data processing of everything that moves. They are working for the government, hedge funds, large banks, and consumer companies. A leading edge player here – and probably the best example of the future, is Palantir. Founded by Peter Thiel several years ago, Palantir has had explosive growth in the past three years. The initial funding for Palantir came from the CIA. The CIA's venture capital firm is called In-Q-Tel and it was one of the angel investors. Palantir provides software that can search, cross-reference, and interpret large amounts of data from many sources. Palantir's software has been used to detect fraud and insider trading by law enforcement agencies and banks. Its clients include US government agencies the CIA and FBI, Bank of America, JPMorgan Chase, and News Corp. In 2013, it has estimated revenues of $450 million. The current value of Palantir is estimated to be $9 bn. (Let's also keep in mind that Amazon has a $600 million contract with the CIA, presumably for international sales, since it is illegal for the CIA to operate domestically.)

The left hand is Palantir Metropolis. This entity is the financial services arm and provides powerful quantitative financial analysis software. This software distributes bank data in a centralized fashion to technical and non-technical users. Customers include banks and hedge funds. As an example, Steve Cohen at Point72 Asset Management (formerly known as SAC capital) hired Palantir to assist in its compliance and surveillance. It has an "Unauthorized Trading" algorithm which assigns riskiness scores to traders by examining correlations between key risk indicators in the context of overall trading activity. Citi uses Palantir Capital Market software to merge proprietary and vendor data into one platform for equity analysis.

Further Reading: See SIFI report on Alicloud (Available in "Public Downloads" section at http://www.schulteinstitute.org/)

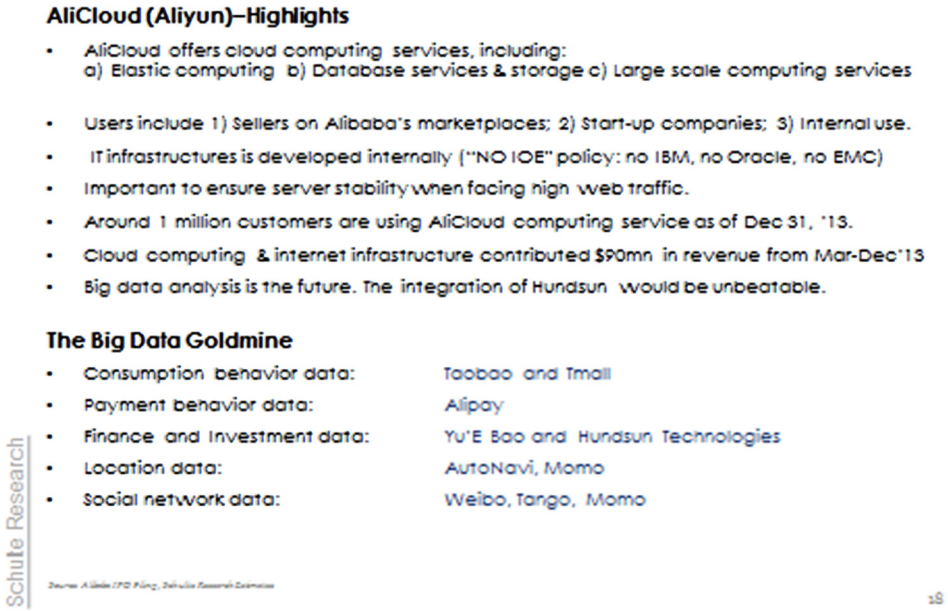
13.13 Alibaba and Ant Financial's Cloud Business: The Future of Banking

We go to the other side of the world and see that, in China, Alibaba is doing precisely this. It is aggressively morphing from a company which is a combination of Paypal, EBay and

Amazon into a company more like Palantir and Google. Alibaba is achieving this through a number of smart moves which may create one of the most interesting hybrid companies the world has ever seen. Alibaba can not only look like Amazon but also have shades of Palantir and also resemble the entertainment element of Disney. So, Alibaba is morphing into a four-headed creature which is in e-commerce, entertainment, banking, and information analysis.

The bread and butter of Alibaba is the equivalent of Amazon and EBay. Alipay is a separate entity but similar to Paypal. It is likely to list inside China and have an H share listing in Hong Kong in 2015. Like Paypal and EBay, it is probably wise to have a separate listing. This will allow it to have a higher valuation and they are, in fact, different businesses and belong apart.

Alibaba is gluing other interesting entities onto this framework which revolve around consumer behavior – driving, dating, learning, fun, languages, lifestyle, and buying goods that can be mailed by Alibaba to the home. The picture below shows how Alibaba is becoming a lifestyle company. This diagram shows how Alibaba is *already* like Google, Dropbox, eHarmony, Amazon, Twitter, Spotify, Orbitz, Uber and ING Direct. All of these functions are migrating to the phone.



www.elsevierdirect.com

Since its establishment only a few years ago, Alicloud (Aliyun) has more than one million customers and it has generated almost $150 million in revenue through the first half of 2016. Cloud computing and Internet infrastructure is a powerful combination. See the table above. With Taobao and Tmall, Alibaba has access to the spending habits and price points of hundreds of millions of Chinese people. With Alipay, Alibaba has access to the credit histories of hundreds of millions of people in literally thousands of cities across the country. With the dating service called Momo, Alibaba has access to preferences and demographic information of 140 million adults in nearly every city in the country. And with Weibo and Tango, Alibaba has access to a social network which makes Facebook pale in comparison.

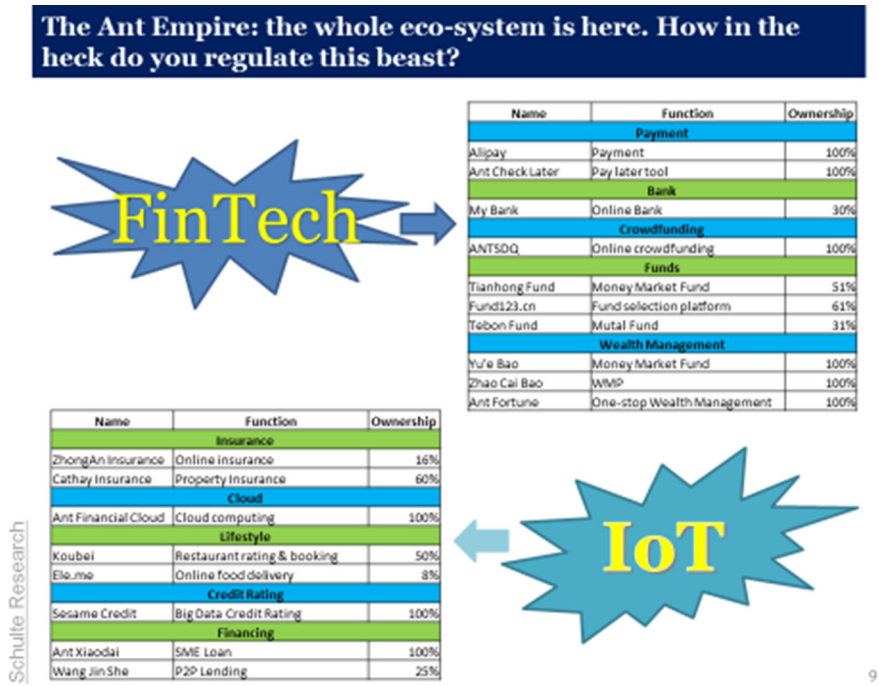
Inside China, the cloud market is growing at more than 40% per annum and now accounts for only 3% of the global cloud market. In this space, Alibaba has a commanding share. Tencent, Shanda and Baidu are all competing in this market. But the real competition here comes from Huawei. Huawei is the gargantuan technology company founded by a PLA Army colonel. Think of IBM, GE and Apple all in one company! Huawei is the real competition for Alibaba in this space. Time will tell just where this competition goes. So fat, the software infrastructure is 70% of the market. Infrastructure is about 20% of the market. In the software sector, Alibaba is the dominant player.

Additional reading: Please see Schulte Institute for Financial Innovation: Ant Financial

Case Study: Ant Financial

Alibaba (and Ant Financial) commands the field of financial technology and the Internet of Things in the first inning of this buildout. Estimates show that this business will be close to $1 billion business by 2018. This business will not only include data from hundreds of millions of phones. It will also include data from billions of censors from moving things such as cars, logistics, ships, refrigerators, food distribution and many other areas of life. This is known as the Internet of Things but is beyond the scope of this chapter.

The business lines of Ant Finance generally distinguish between the world of fin tech and the cell phone on the one hand and the world of moving people, places and things on the other with censors. Of course, there is an overlap (phones have between 12 and 20 censors each), but for the purpose of understanding the trends, we can make a difference here.



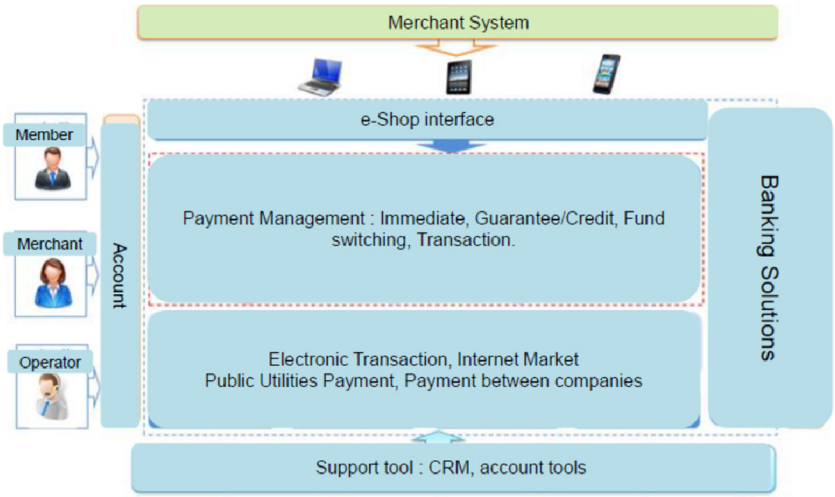
Name	Function	Ownership
Payment		
Alipay	Payment	100%
Ant Check Later	Pay later tool	100%
Bank		
My Bank	Online Bank	30%
Crowdfunding		
ANTSDQ	Online crowdfunding	100%
Funds		
Tianhong Fund	Money Market Fund	51%
Fund123.cn	Fund selection platform	61%
Tebon Fund	Mutal Fund	31%
Wealth Management		
Yu'e Bao	Money Market Fund	100%
Zhao Cai Bao	WMP	100%
Ant Fortune	One-stop Wealth Management	100%

Name	Function	Ownership
Insurance		
ZhongAn Insurance	Online insurance	16%
Cathay Insurance	Property Insurance	60%
Cloud		
Ant Financial Cloud	Cloud computing	100%
Lifestyle		
Koubei	Restaurant rating & booking	50%
Ele.me	Online food delivery	8%
Credit Rating		
Sesame Credit	Big Data Credit Rating	100%
Financing		
Ant Xiaodai	SME Loan	100%
Wang Jin She	P2P Lending	25%

This Powerhouse of Alibaba and Hundsun Combines:	
E-commerce:	home, clothes, books, beauty
Travel:	plane, hotel, car, boat information
Banking data:	liquidity, portfolios, insurance
Alipay:	habits, trends, lifestyle, demography
Big Data:	personal, corporate transactions
Financials:	futures, options exchanges
Entertainment:	crowd funding of shows, films, music

There really is no company like Alibaba and Ant Financial in the world. (After the IPO of Ant Financial IPO in early 2017, Alibaba will be a 33% shareholder of Ant – the controlling shareholder.) This company can conduct human queries on just about anything. How many insurance policies are there? How many cars did Chinese people drive last year and where? What kinds of movies do people want to see? Where do people want to go on vacation? What kind of analysis do investors in equities and fixed income like to use? How do Chinese construct portfolios for their future? In what way will Chinese use the futures and options markets? This is a unique and massive data on the largest population in the world. And it is generally closed. And this is just getting started!

Look at the chart below. It shows the power of the information that is part of the Hundsun infrastructure built over the past several years which conceivably (and in all likelihood is part of Alibaba's Cloud) will now be able to be mined by Alibaba entities. If one sees corporate transactions going on live, it is possible to get a good "real time" sense of where GDP is going. It is possible to get an up close and personal sense of consumption trends, entertainment likes and dislikes, fund flows with in the economy. It will be possible for government entities to track corrupt officials and their cash movements. It will be able to seek out money laundering. It will be able to have a reliable sense of funds flows among and between various asset classes. The opportunities for data analysis (for good and for worse) are infinite.



Further reading: Schulte Institute for Financial Innovation report: Alibaba report

13.14 Final Analysis: There Is no Such Thing as Private Information for Anyone

What we are seeing in front of us with Alibaba on the one hand and with Palantir/Amazon/Alphabet on the other is the largest and second largest economies in the world competing for data hegemony. Both of these entities are indisputably joined at the hip to the government of their respective countries. When I was traveling around the world presenting my clients with a bullish analysis of Alibaba in the Fall of 2014, I was presented with a perplexing question. Some investors asked whether it bothered me that Alibaba was so closely entwined with the Chinese government. When I laid out the intimate connection among and between Google,

Amazon and Palantir and the federal Government, there was a sheepish silence. This is because there is an inbred bias that China is the only country which watches and controls its people. There is a sense inside the United States that government intrusion into people's lives in minimal and lies within constitutional protections. If the Snowden Files taught us anything, it is that the government can issue hundreds of thousands of warrants on email and messages under the guise that a crime MIGHT happen. Almost none of these are contested. Some would say this is a violation of the Fourth Amendment which concerns illegal search and seizure.

As it is now, the development of the technological infrastructure in China is on a par with most of the OECD (if not actually ahead) and it has done this in a very short period of time. Interestingly, Alibaba has done in seven years what six or seven companies in the US have taken 15 years to achieve. Alibaba is EBay and it is Google and it is Amazon… and Uber, and eHarmony, and ING Direct. I think we should all watch next what Alibaba does in the distribution of pharmaceuticals within China. More importantly, I think the industry which Alibaba will dominate is the streaming of films. Alibaba has hooked up with both Sony and Lionsgate to distribute content in China. This may spell the end of cable within a few years as more movies are watched through Internet streaming and as new technologies enhance the experience of watching movies using a phone which can display the image on a wall as a projector or in a 360-degree experience.

The possibilities are endless and the competition is intense. But companies like Alibaba, Palantir, Google, Apple, and Amazon are first movers and have phenomenal cash piles to dominate any subsector they choose to enter. One chart to show the way in which industries can be overturned by rich and entrenched first movers is the way in which Apple is stretching its wings in many different areas. The illustration below shows what can happen if Apple decides to get into the credit card business with Apple Pay. It can disintermediate many companies and become a middleman among and between cards companies, merchants, banks, and the consumer.

Facebook will increasingly be used as a source of financial technology to raise money, transfer funds, settle accounts, pay bills and other activity. Alibaba will become a lifestyle/entertainment/bank company. It will look more like Disney and less like EBay. Facebook may become more like a multi-cultural virtual financial center where finance, buzz, brilliant marketing, and the "experience" can create "virtual" industries overnight. Airbnb will challenge hotels in every country in the world. Uber will change how we all get taxis in countries all over the world. Intuit, Kabbage and Indinero are companies which will change how small and medium companies raise money. Prosper, Kickstarter, and Zopa will alter how people fund projects and raise funds for philanthropic enterprises, charities and disasters. Palantir will change the way we understand the mining of data. Banks will struggle to keep up with

these phenomena but I am not hopeful. The cloud server is the center of this all. We need to take heed of the advice of Internet pioneer Jaron Lanier: "People who want to do well, as information technology advances, will need to double down on their technical education and learn to be entrepreneurial and adaptable. For, information and money are mutable cousins."

Further reading

Schulte, 2015. The Next Revolution in Our Credit Driven Economy: The Advent of Financial Technology. Wiley & Sons.

CHAPTER 14

Financial Inclusion, Digital Currency, and Mobile Technology

Vrajlal Sapovadia[#]

Contents

14.1 Introduction 362

14.2 Financial Exclusion 363

14.3 Demand Side Factors of Financial Exclusion 366

14.4 Individual Factors of Financial Exclusion 366

14.5 Environmental Factors of Financial Exclusion 367

14.6 Supply Side Factors of Financial Exclusion 367

14.7 Financial Inclusion and Institutional Support 368

14.8 Legislation and Government Policy in Financial Inclusion 369

14.9 Financial Infrastructure and Financial Inclusion 369

14.10 Digital Currency and Financial Inclusion 370

14.11 Mobile Payments and Financial Inclusion 371

14.12 Global Experience and Opportunities 372

14.13 Challenges and Solutions 378

14.14 The Outlook 382

14.15 Conclusion 383

References 384

Notes 385

[#] Vrajlal Sapovadia is Professor and Dean at School of Business & Entrepreneurship, American University of Nigeria. A Chartered Accountant and Ph.D. in Management Accounting, Dr. Sapovadia has authored 80+ publication including one in Harvard International Review.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00014-0
Copyright © 2018 Elsevier Inc. All rights reserved.

14.1 Introduction

It is paradox that in globalized world more than one third of its population is excluded from formal financial system. The body of evidence suggests that appropriate financial services can help improve household welfare and promote small enterprises. The financial exclusion is attributed to various reasons. Conventional financial system has several inherent limitations which lead to unserved population. Digital currency and mobile technology can spur penetration of financial system in such unserved population. The evidence shows that high cost for small ticket size financial transaction in conventional financial system makes the transactions unviable. Digital currency and mobile technology can cater the needs of small transaction at affordable cost. It can also help reducing time and make accurate and faster transactions in bulk. Many emerging economies like India, Brazil, Kenya, and Nigeria have embarked on mobile technology to overcome financial exclusion.

The concept of financial inclusion is the delivery of financial services at affordable costs to sections of disadvantaged and low-income segments of society. As per World Bank Report two billion people, or 38% of adults in the world, do not use formal financial services,[1] and 73% poor people are unbanked because of costs, travel distances, personal beliefs, and often difficult requirements involved in opening a bank account. This chapter highlights the role played by digital currency and mobile technology in improving financial access across the developing world, where majority of the disadvantaged people live. Mobile technology is penetrating across the globe. Nearly a third of all bank-account holders in sub-Saharan Africa reported having a mobile-money account. Yet in spite of this progress, problems persist. More than half of adults in the developing countries lack a bank account. Among the account holders, 46.5% are women against 53.5% men. This gender gap of 7% if narrowed will make more people bankable. Extending access to finance is the first building block for people to build a better life. Not only does it help families plan for long-term goals and emergencies, it also facilitates day-to-day living and yields positive results in many different ways, e.g. education, health, and employment. Digital currency and mobile transfer can help to cover unserved population under formal financial market.

Over the past few decades, different types of financial-services providers have offered new instruments, which have opened up possibilities for the financially excluded populace. The service providers include non-government organizations, cooperatives, community-based development institutions, commercial and state owned banks, insurance and credit-card companies, telecommunications and wire services, post offices, and other businesses that provide point-of-sale (POS) access. New business models and such service providers have, in many cases, become viable due to technological breakthroughs, including the worldwide spread of mobile phones, economies of scale, government support, and gradually penetrating digital currency.

www.elsevierdirect.com

As per 2016 World Development Report on "Digital Dividends" notes, digital finance is likely to play a key role in answering these questions. One of the main messages of the report is that digital development is not a matter of access alone. Digital connectivity is a key; but it is only a starting point for successful digital development. It is as important to strengthen other factors that interact with technology, such as creating awareness, train people, protection from frauds, responsible regulation and institutions; all that in order to make digital technologies work for the poor. The World Development Report calls these other factors the 'analog complements' to digital technologies, which fall into three categories: regulation, skills, and institutions. If there is strategic alignment of these factors in digital money market, it will help to realize financial inclusion goal. To realize financial inclusion, it is very important to understand why people are excluded from financial system.

Investments are needed to deliver digital payments in emergencies. Countries where crisis are most likely to occur are least prepared to deliver digital payments.[2] Mobile payments reduce government costs, time, efforts, and resources which can be channelized in other welfare programs to help economy and the society. It enhances convenience to the payee and payer. Physical transfer of money requires paper, fuel, transport infrastructure, storage space, and security. It is also subject to several types of vulnerability, like theft, embezzlement, fire, and physical erosion of currency notes. Keeping track and record is another challenge. Such records are easy to tamper with and require huge space and security mechanism to preserve it for years. Hiding the transactions and avoiding taxes are widespread practices in developing countries. The physical transactions are subject to manipulations, errors, and omissions. Mobile transactions overcome some of the challenges and help government to keep track of transactions, which may lead to higher revenue collection on account of taxes. The government can transfer money by using mobile payments, multiple transactions more accurately, and within less time and cost.

14.2 Financial Exclusion

Financial exclusion means financial services are not available or affordable to disadvantaged section of the society. It is important to understand reasons and composition of financial exclusions across clusters of population to offer appropriate approach to reduce such exclusion. This can help service providers to leverage on digital technology to penetrate in the market. The unserved clusters can be grouped region-wise, gender-wise, age-wise, rural vs. urban and around economic, cultural, and political structures. A person is considered financially excluded when they have no access to some or all of the services offered by mainstream financial institutions or a person does not make use of these services. The study 'Financial Services Provision and Prevention of Financial Exclusion' establishes a list of basic financial services considered essential to daily life; they are: a bank account to receive income; a transaction

www.elsevierdirect.com

account to make payments from; a savings account to store money; and access to unsecured credit to manage temporary cash shortages and unexpected expenses. Depending upon level of advancement of the economy, more financial services can be considered important financial services necessary in the market.

Economist.com published financial excluded population numbers in 2014. As per the report, Middle East and Sub-Saharan Africa are top in the list with over 80% and 60% population unserved respectively. More than 50% women in Asia (excluding East Asia), Latin America and Caribbean regions are out of financial services net. More than 40% males in these regions and Europe are also out of financial service net. Surprisingly barring OECD countries, more women are out of the financial service net compared to their counterpart men in all regions.

The Chart-I below gives a pictorial presentation of region-wise adult excluded population.



Source: Economist.com

Financial exclusion can be described as the inability of individuals, households or groups to access necessary financial services in an appropriate form. It can stem from problems with access facilities, price, marketing, financial literacy, or from self-exclusion in response to negative experiences, ideology, beliefs, or perceptions. Financial exclusion is evident in developed economies as well and it is a reality for many European citizens. Two in ten adults in the EU15[3] and almost half in the EU10 (47%) do not have a bank account, and many more have

no savings or access to credit. Financial exclusion significantly increases the risk of social exclusion and poverty. Microfinance, the provision of financial services such as microcredit (for business or personal use), savings, insurance and transfer services to low income households can be a tool for social as well as financial inclusion, as it helps to prevent and address all the aspects of exclusion like poverty, low income, lack of employment. These aspects are both major components of, and reasons for, social exclusion.

Financial service consumers are heterogeneous and the causes of exclusion are complex and varied. Accordingly, the approaches and technology can be molded for each group. Additionally, the number of consumers affected very much depends on the product sector. The Eurobarometer reports that 7% of the population in the EU15 are considered to be financially excluded, meaning that they have neither access to a transaction/deposit bank account, savings account nor revolving credit (European Commission Report, 2008). Levels of financial exclusion vary widely. The lowest rates occur in countries where the standard of living is universally high. In the EU15, Greece has the highest rate of financial exclusion, followed by Portugal and Italy. Luxembourg has the lowest rate, followed by the Netherlands, Denmark, and Sweden. It is possible that the Eurobarometer may overestimate levels of financial exclusion. National surveys have only been undertaken in some countries, but they generally indicate lower levels of banking exclusion than estimated by the Eurobarometer. This is probably because of problems in defining the different types of bank accounts in a way that can be applied across Europe, as well as differences in sampling and the timing of surveys.

Financial exclusion affects some groups of people more than others, and, on the whole, similar types of people are disproportionately affected regardless of the prevailing level of exclusion in their country. Generally speaking, people with low levels of income, less education, who are part of an ethnic minority or with a migrant background, and who are either very old (over 65) or very young (18–25) are more likely to be financially excluded than others. Women are twice as likely to find themselves completely excluded from financial services than men. People who are completely financially excluded are also more likely to be found in households with no wage earner or in single-parent households. As regards working status, students and unemployed people are most likely to be affected. The occurrence of financial exclusion is higher in rural than in urban areas, and is also higher in deprived areas. There is also evidence that financial exclusion is linked to people's knowledge of, and exposure to, financial services. Several factors are considered major causes of financial exclusion throughout the world. They can be broadly grouped into individual and environmental factors which can be subdivided into three categories: societal, supply, and demand factors.[4]

www.elsevierdirect.com

14.3 Demand Side Factors of Financial Exclusion

There are a number of barriers to access which can undermine consumers' willingness to engage with financial services and/ or affect capacity and ability to make effective, informed choices and decisions. These barriers include:

- ✓ low levels of consumer awareness of the need to plan and provide for the future, or shop around for better deals;
- ✓ low levels of financial literacy and capability;
- ✓ religious beliefs and cultural restrictions;
- ✓ language of individual and that of suppliers and market;
- ✓ consumer trust and confidence;
- ✓ inertia and behavior, and impact of external factors such as the property market.

The net result of these barriers is that consumers can 'self-exclude' to a large degree. This can be detrimental to consumers' own welfare but this has a double whammy effect as consumers have to be persuaded to save or invest through expensive advertising or incentives, or need the support of expensive advice and guidance – this has the effect of pushing up distribution and access costs which in turn makes it unprofitable for industry to serve larger numbers of less profitable consumers.

14.4 Individual Factors of Financial Exclusion

This group of factors includes income levels and other individual factors such as poverty, illiteracy, disability, religious belief, unemployment, and social group to which the subject belongs. The income levels and affordability are among the main contributory factors to the financial exclusion. Consumers on lower incomes may simply not be able to afford financial services or may be priced out of the market due to market practices such as risk-based pricing. The consumers with restricted mobility may make access difficult to banking services if bank branches are not within their reach.

The richest 20% of adults in developing countries are more than twice as likely to have a formal account as the poorest 20%. In India, some castes or classes are considered backward and individuals of these castes are more prone to exclusion to the forward caste or class. The caste is based on birth, so individual is unable to change it throughout the life. Literacy has significant impact on financial exclusion. More illiterate population is excluded than literate. People living in villages are more excluded than people living in towns and urban centers. The occupation in which a person is engaged also determines level of financial exclusion. More blue-collar workers are financially excluded than white-collar workers. Individual factors can be minimized by creating awareness and designing products to serve the clusters.

www.elsevierdirect.com

14.5 Environmental Factors of Financial Exclusion

This group of factors includes the broader socio-economic and demographic trends such as the ageing population, changing labor market structures, and political trends such as the transfer of risk and responsibility from state and employers to individuals.

Consumers are increasingly becoming expected to use the financial services industry to provide for the future, or protect themselves against risk. These trends may increase the risk that the needs of vulnerable consumers are not met or consumers fail to make sufficient provision for affecting reasons. The government and regulatory policy can have inadvertent consequences on consumers inadvertently contributing to financial exclusion or making it harder for consumers to provide for themselves.

A range of societal factors have been identified as having an impact on people's access to, and use of, financial services. A combination of low disposable incomes and the economics of access in retail financial services means that this group is not commercially viable for mainstream retail financial providers. Alternatively, consumers may face actual exclusion because of a disability. With the increasing diversity of financial institutions and services caused by the liberalization of financial services markets, it is hard to gain a general overview of the sector and the opportunities available. Studies also reveal a strong correlation between levels of income inequality (measured by the Gini coefficient) in a country and the incidence of financial exclusion. Furthermore, societal changes such as structural changes in the labor market and the rising number of single people and single parents, as well as other demographic evolutions, increase people's vulnerability to financial exclusion. The consumers who could afford to provide for their core financial needs but aren't doing so due to demand and supply side factors and barriers to access.

14.6 Supply Side Factors of Financial Exclusion

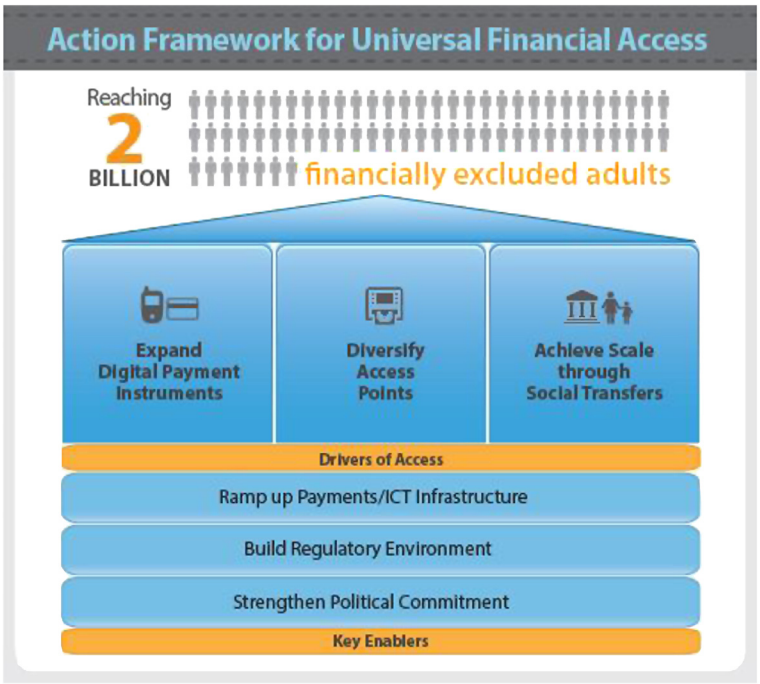
On the other side of the equation, a number of factors relating to the way the financial services industry operates and is structured means that consumers can be excluded or don't have access to fair and affordable products and services. The key barriers are:

- ✓ distribution inefficiencies and ineffective competition;
- ✓ oversupply in the market and diseconomies of scale;
- ✓ complex products;
- ✓ inefficient regulation;
- ✓ public policy interaction;
- ✓ poor logistic and infrastructure;
- ✓ mismatch with local language;
- ✓ basic economics of access.

www.elsevierdirect.com

14.7 Financial Inclusion and Institutional Support

Several governments and international institutes are working to strengthen digital money market in order to improve financial inclusion target. The World Bank Group President Jim Kim has issued a call for action to achieve Universal Financial Access by 2020 (UFA2020), i.e. basic access to the formal financial system, e.g. through debit cards or mobile money, should be possible for everyone. This can be achieved through ambitious country-led targets and reforms; through the use of technology, innovation, and data to transform business models; and through public- and private-sector initiatives to rapidly expand access to financial services. The critical reform envisaged includes allowing electronic-money and mobile-money products to be offered at affordable cost in possible all locations, particularly the remotes ones, policies to encourage digital transfer and government payments through technology enabled platform. The UFA2020 initiative is focusing on 25 countries where 73% of all financially excluded people live. India and China have the largest share of unbanked people. Together they account for some 32% of them. The rest of the top-priority countries are: Bangladesh, Brazil, Colombia, Cote d'Ivoire, DRC, Egypt, Ethiopia, Indonesia, Kenya, Mexico, Morocco, Mozambique, Myanmar, Nigeria, Pakistan, Peru, Philippines, Rwanda, South Africa, Vietnam, Tanzania, Turkey, and Zambia.



Source: UFA2020

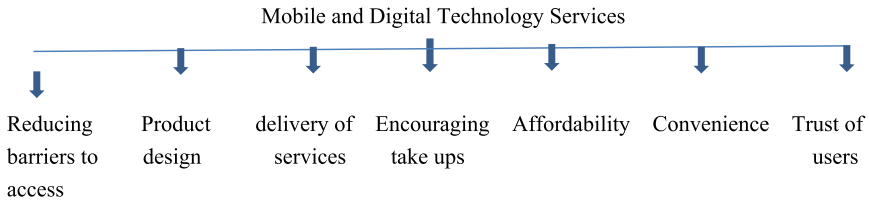
Despite transformative innovations in digital technologies, the digital divide is still substantial. What can be done to spread digital dividends – that is, the broader development benefits of digital technologies – more widely? How can digital technologies contribute to the World Bank Group's twin goals of eradicating extreme poverty and increasing shared prosperity? The World Bank is **working on a** closely related issue – the global divide in financial inclusion, and how to use digital financial technologies to close it.

14.8 Legislation and Government Policy in Financial Inclusion

Financial exclusion is influenced by government policy and practice in a range of ways. First, a payment benefit by cumbersome methods clearly encourages recipients to operate a cash budget. Secondly, there is evidence that regulation of financial services can cause or reinforce financial exclusion. Thirdly, suggestions for future welfare reform may well add to the problem of financial exclusion, rather than addressing it. On a more positive note, government policies can create a new market for financial services. The proposed 'stakeholder pension' is one such example. The requirement of various documents and procedures compels poor and illiterate citizens to avoid banking accounts. In many countries, the requirement of minimum balance, charges on transactions, and maintaining accounts are exorbitantly high. It is observed that depositing money is easy, but withdrawing money is very difficult and time consuming. The bank branches are opened where more affluent people are living, but banks are hesitated to open in remote areas, slums, and less secured areas. The government should ensure that mass can benefit from banking operations, so regulation should focus on inclusive banking (Sapovadia, 2015).

14.9 Financial Infrastructure and Financial Inclusion

The research suggests that possible solutions to financial exclusion should focus on four main areas: reducing barriers to access; product design; delivery of services; and encouraging take-up. Affordability of services, convenience and trust of users are equally important to include large population to use mobile and digital services for financial transactions. This may require action by government and financial institutions in partnership.



www.elsevierdirect.com

Product design should ensure for day-to-day money management the consumer required a simple account which would allow them easy access and to retain tight control over their money. It should offer basic money transfer facilities, including a facility for spreading the cost of bills. It would offer no credit facilities but have a 'buffer zone' to allow flexibility. Products offering longer-term financial security should be simple, certain, and transparent so that users 'know where they are' and the costs associated with regulation compliance are low. They should be based on regular and automatic saving and flexible, so that products can be retained even during times of hardship; and give restricted access to the money saved. To reduce the likelihood of people cashing in long-term savings plans because of short-term needs for cash, long-term savings products could be used as collateral for small loans.

The product should be at affordable cost giving options for spreading the cost of payments across the year. Wider acceptability is another issue that must be addressed. The people on the margins of financial services want to deal with organizations which are financially secure, trustworthy, and understand their needs. The organizations to provide the product and deliver it to the customer may be different. New technology offers some opportunities for product delivery at this end of the market. Electronic cards and electronic money transmissions are likely to be the most acceptable. Low levels of telephone and computer ownership among these households rule out solutions such as call centers, telebanking, and on-line banking, but the time is changing fast as telephone penetration ratio is improving.

The knowledge of financial products is remarkably low among households that are without them. The efforts to create awareness pertaining to product, utility, features, trustworthiness, prices, methods of using are vital to financial inclusion through mobile and digital currency. It may be compounded by marketing policies which reinforce the belief that financial services are also for the poor. Measures to encourage take-up must, therefore, tackle the widespread mistrust which such households have of many financial providers, particularly those which are geographically remote. Use of trusted intermediaries could overcome these barriers. Targeted marketing and delivery of new products as they become available would also increase take-up. Easy accessibility has other aspects, and hence, the language and cultural barriers faced by some potential users need to be taken into account.

14.10 Digital Currency and Financial Inclusion

A blockchain is a distributed database, introduced in Bitcoin, which maintains a continuously-growing list of data records that each refer to previous items on this list and is thus hardened against tampering and revision. The initial and most widely known application of block chain technology is the public ledger of transactions for bitcoin, which has been the inspiration

for other cryptocurrencies and distributed database designs. The decentralized publishable databases build trust amongst stakeholders and fix accountability.

Transactions are the content to be stored in the block chain. Transactions are created by participants using the system. In the case of cryptocurrencies, a transaction is created any time a cryptocurrency owner sends cryptocurrency to someone.

System users create transactions that are passed from node to node on a best-effort basis. The system implementing the block chain defines a valid transaction. In cryptocurrency applications, a valid transaction must be digitally signed, spend one or more unspent outputs of previous transactions, and the sum of transaction outputs must not exceed the sum of inputs.

The blockchain is beginning to financially connect more than 4 billion people in developing countries living at the base of the economic pyramid with diaspora communities in the US, Europe, and elsewhere. Such remittances are important for international migrants to maintain social relationships and social presence in their home communities. According to the World Bank worldwide remittances will be $700B by 2016 with traditional money transfer organizations charging fees of 10% or more and taking days to clear. Start-ups like BitPesa in East Africa and Rebit in the Philippines are leveraging the blockchain to facilitate these same remittances for fees of 3% or less with near-immediate transfer. In fact, in February 2015 BitPesa raised $1.1M USD in their second round from a roster of venture capital funds.[5]

14.11 Mobile Payments and Financial Inclusion

The mobile payments are becoming ubiquitous and pervasive. A TSYS study of UK finds that people born before mobile technology are also widely accepting mobile payment as an option. It also reveals that it is convenient and half of the users are feeling that the transactions are secured. The Mobile Network Operators (MNOs) transact mobile money business by number of ways. Mobile payments can be used to (i) transfer to self-account, (ii) transfer to third party, (iii) payment to billers, (iv) payments to retailers, (v) payment to government, (vi) receipt of payment, and (vii) receiving transactions-related information. One of the estimates claim at least 30 implementations in Africa where MNO-driven financial services are an important part of the financial inclusion landscape. Mobile money contribution may be small compared to current MNO total revenue but could be important for future revenue growth (Beard, 2015).

Mobile money success is highly dependent on the size of the MNO's voice customer base. The vast majority of mobile money customers are likely to come from the pre-existing voice base. Mobile money by itself has not been shown to be a powerful tool for voice customer growth and acquisition, so it is even more important to come in with a large pre-existing customer base. As a result, our basic modeling exercise shows that revenue potential is greatest for the largest MNO in a market, even when it is not the first mover.

www.elsevierdirect.com

Direct profit from mobile money depends on growth in "electronic-only" transactions. While there are other key drivers of direct revenue growth, the most significant driver is ultimately growth in electronic transactions per deposit or cash-in because of a simple combined effect: less use per transaction of cash-in/cash-out at agents, which is the lowest margin earning part of the business and more use per transaction of the electronic platform, which is the highest margin earning part of the business.

There are indirect benefits of mobile money to MNOs, but these only become significant when mobile money reaches scale. MNOs should account for savings from indirect benefits, especially when the business has "too many mouths to feed" in the value chain, either agents or bank partners or others. However, operators need to realize that these benefits are only significant at scale, which may be 20% of the voice base as active mobile money customers.

To capture long-term profits beyond domestic transfers, mobile money implementations will need to "leave money on the table" in the short term. We want all MNOs to scale in the way M-PESA Kenya has in the last four years, but that is clearly proving to be elusive. MNOs know that the prize is everyday small merchant payments (which is the larger payments market), where they seek to get a foothold with domestic transfers. But pricing schemes that make them competitive in the traditionally expensive domestic transfer market keep them out of the larger market of merchant payments. If they price lower, they will give up some profits from domestic transfers, but in turn open higher overall gains in the long term, as we illustrate in this presentation (Mbiti and Weil, 2011).

14.12 Global Experience and Opportunities

Several countries used different strategies to serve financial excluded masses. Asia, Africa, and Latin American nations used mobile and digital technology as financial inclusion tool. Forty percent of Indians currently do not have access to a bank, and most of these people belong to low-income or rural areas. Starting in 2005, the Reserve Bank of India (RBI) has recommended that banks increase access to banking services for the unbanked population using the mobile payment (m-payment) systems. With nearly 51% of the population carrying a mobile phone, private partners in India developed m-payment systems modeled after the M-PESA system to increase financial outreach by providing deposit and withdrawal services to clients. Interbank Mobile Payment System (IMPS) was launched, in which a mobile based funds transfer service for users registered with participating banks. MNOs and banks partnered to provide m-banking services all over India including Airtel's (MNO) "Mobile Money Transfer", and by other banks such as ICICI, HDFC, and

State Bank of India (SBI) have launched their own mobile payment services in partnership with several MNOs experiencing varying degrees of success. Despite these initiatives taken in India, the adoption of mobile payment technology, especially among the low-income population, has been cautious. This is primarily due to stringent regulations and marketing models aimed at acquiring the predominantly urban and technically advanced users. Additionally, transactions need to be conducted on a phone via an Internet connection, which is not only a relatively expensive service but also requires basic know-how about the Internet technology. While these systems have been adopted by approximately 15% of urban mobile users as of 2009, cash continues to be a predominant mode of transaction for unorganized retailers and their clients. In a survey conducted by the 2014 Intermedia Financial Inclusion Insight (FII) Survey it was revealed that 0.3% of adults use mobile money, compared to 76% in Kenya, 48% in Tanzania, 43% in Uganda, and 22% in Bangladesh. This result indicates a huge room for mobile payment business. The low mobile payment user is attributable to many factors, but major factor is government policies.

Regulations in India permit mobile transactions only if they are linked to a registered bank account, through which transactions take place. While it is a well-intentioned regulation to protect clients, this excludes the 40% unbanked population and may also be a deterrent for those uncomfortable with the banking system.

Another study conducted by CMF-IFMR found that the financial inclusion mandate by the RBI does not allow private partners to charge appropriate fees for zero-balance accounts targeted for the low-income populations. This has discouraged agents to offer diversity of financial products to low-income clients through the m-banking channel. To make the mainstream banking services available to all, RBI and government have been outlining many initiatives that could accelerate efforts on this. The years 2005 and 2006 witnessed two key initiatives of RBI to reinforce the financial inclusion drive by introducing 'no-frills' account and 'business correspondent (BC) model' of banking respectively. Customer Service Providers are responsible for direct interaction with clients and to take the BC services to clients on the ground (CMF-IFMR Newsletter Article, 2012; Nandhi, 2012).

Smartphones are not just useful for social media, videos, and taking selfies. They will now become an important part of your daily life by doubling up as a portal for making payments, sending and receiving money, etc. Ten of the country's biggest banks along with the Reserve Bank of India have just launched a Unified Payments Interface (UPI) – a mega app that will sit on your smart phone once you have downloaded it and dramatically reduce the cost and time taken for making simple payment.

www.elsevierdirect.com

UPI for mobile-based payments across banks

29 Number of banks that are part of the UPI network at present

117% growth in volume of mobile transactions in February 2016 over March 2015

175% Growth in value of transactions during the same period

	Feb-16		Mar-15	
	Volume in million	Volume in ₹ Crore	Volume in million	Volume in ₹ Crore
Mobile Banking	42.75	46,473	19.67	16,885
Growth (%)*	117%	175%	83%	398%
Mobile Wallets	49.02	2,251	46.11	1,082
Growth (%)*	6.30%	108%	227.70%	171%

* YOY GROWTH

SOURCE: RBI

The economic survey presented in Indian Parliament for 2015–16 budget states that use of mobile network can be the game changer tool for achieving financial inclusion target. It emphasized to take advantage of deep mobile penetration and agent network as it transfer money quickly, securely, and in convenient manner. It is important to note that mobile density in India rose to 82.5% in 2015.

Among 1.29 billion people, banking penetration is only 54 percent, and fewer than 10 percent of 650,000 Indian villages have a bank branch. Even in urban India, fewer than 35 percent of the working population with annual earnings below 50,000 rupees own a bank account. Strong policy makers like the Reserve Bank of India (RBI) are moving to policies that help drive financial inclusion. It has launched Interbank Mobile Payment Service (IMPS) to transfer money instantly between bank accounts within the country using mobile phones. Through the RBI and the National Payments Corporation of India, a widely distributed, readily accessible, and interoperable mobile payments network is being built to cover disadvantaged population in formal financial channels. The government of India has issued instructions to bring all Central Government schemes having a financial component under the direct benefit transfer (DBT) from April 2015, to plug leakages and to keep the subsidy bill in check. Similar mechanisms are used by many countries to help poor or those who face a probable risk of falling into poverty in the absence of the transfer by transferring cash through use of technology. The main objective of these programs is to increase poor and vulnerable households' real income and protect them from bribe seekers government servants.

Reserve Bank of India believes that to achieve financial inclusion, it is not possible to have bank branches in every village because that would be too expensive, but RBI is exploring other options like mobile branches and mini or micro branches… also by the end of July

2016, the Universal Payment Interface (UPI), which allows one to make payment from one bank account to another, will be in place. Ten of India's largest banks with RBI have launched UPI based apps, which will reduce time and cost in payments and third party transfers. Third party payments will become simple and easy to make, once you have apps on your smart phone. Thus mobile banking is considered as alternative to bank branch where opening of it would not be feasible. However, mobile payments cannot replace all functions of the branch. In November 2014, the RBI issued Payments Bank guidelines which allow companies like mobile operators, retail chains, and existing agent managers with significant distribution expertise to offer deposit accounts and payments as a stand-alone business.

The interface (UPI) allows you to add multiple banks and transfer money, even between payment wallets, for a fraction of existing costs. If your friend or colleague wants to return the money you had loaned him? Send an SMS to his bank with a request for payment. The SMS will be forwarded to the friend or colleague and if he approves, the bank will pay. The Immediate Payment Service (IMPS) that helps transfer a particular amount immediately, and of course, payment wallets that let you pay at a merchant store by scanning a Quick Response (QR) Code by using a smartphone. Banking has already shifted to your smartphone with feature-rich apps.

"Digital payments have been growing quickly in the country, but they are still a fraction of the overall payments. Most of the high-frequency small transactions are still in cash.

The ease and convenience of UPI offers will help individuals prefer to pay their maids, milkman, newspaper vendor, etc., digitally than in cash," says Sangram Singh, senior vice-president and head-cards & merchant acquiring business at Axis Bank. With UPI, an individual only needs make a unique virtual private address (VPA), simpler than signing up for an e-mail. If you are a bank customer, your VPA can be created like xyz@abank. If an individual wants to make a payment to her maid, she can simply type the VPA and initiate a transfer. "Few people remember their card numbers, account numbers and NEFT codes offhand. But the UPI address is easier to remember," says Ritesh Pai, senior president and country head-digital banking, YES Bank. (Rediff.com on 28 Aug. 16)

UPI is also the first of its kind system that will bring different financial institutions on one platform. The current payments systems in the country work in silos. For example, if you want to transfer money from one wallet to another, it's not possible. With UPI, such transactions also will become possible as it expands from banks to other financial intermediaries. It's even possible with UPI to download an app of one bank without being its customer and make transactions using a different bank. For example, you can download an Axis Bank UPI app without being its customer. If your bank is already part of the UPI, says Union Bank of India, you can start transacting with its account details. When a person is adding his other bank accounts in the app, he doesn't even need to know their details. The registered mobile

number is mapped to the UPI. Once you enter the name of the bank you wish to add, it automatically shows the account number of that bank. After authentication, it can be easily added. UPI transactions are already low cost (less than INR 0.45 for each). Once all financial institutions are part of the system, the cost of transactions would come down further. The UPI platform provides better security as well.

Digital currency is an Internet-based medium of exchange distinct from physical that exhibits properties similar to physical currencies, but allows for instantaneous transactions and borderless transfer-of-ownership. There are many private digital currency exchanges working to act as medium of transfer of digital currency. The scope of digital currency and surge in its price and users is phenomenal. University of Nicosia is offering master level course in digital currency.

Central banks typically take an interest in retail payments as part of their role in maintaining the stability and efficiency of the financial system and preserving confidence in their currencies. Innovations in retail payments can have important implications for safety and efficiency; accordingly, many central banks monitor these developments. The emergence of what are frequently referred to as "digital currencies" was noted in recent reports by the Committee on Payments and Market Infrastructures (CPMI) on innovations and non-banks in retail payments. A subgroup was formed within the CPMI Working Group on Retail Payments to undertake an analysis of such "currencies" and to prepare a report for the Committee.[6]

Looking to the excluded mass from financial service net, there is enough room for more players to fill the space by entering in unserved regions, clienteles with expended network and new products that befit requirements of poor. Financial inclusion is a key for development in Africa, Asia, and Latin America. "Mobile money in Latin America is an ecosystem play, there is more of a deliberate focus on integrating with different companies in the value chain," Mireya Almazán, Latin American Manager for GSMA Mobile Money for the Unbanked, said in recent interview (Heyer and Mas, 2009).

E-commerce in the region of Latin America is growing, having reached $69 billion in sales in 2013, and increasing at an annual rate of 45%, making it the fastest growing retail channel in the region. Brazil is the largest e-commerce market in Latin American Countries ($18.80 billion of sales in 2014), followed by Mexico ($6 billion) and Argentina ($4.67 billion). When e-commerce migrates to mobile, the need for mobile and digital wallets may also increase as a result. These wallets could increase their chances of success with value added services such as installment payments, which have been very popular in LAC, and Brazil in particular. Banks see potential disintermediation in the face of PayPal, says Javier Chavez Ruiz, CEO at Mexico Mobile Financial Solutions, and are looking to adopt their strategies to the digital payments reality accordingly.

Business models that align the service delivery characteristics of the Internet, mobile money, and blockchain remittances and other payment streams will provide the transactional rails upon which we'll see significant economic growth in Africa, Asia, MENA and Latin America. Digital finance and banking will do for the economic base of the pyramid in rural, agricultural areas what commercial banking did for the Industrial Revolution!

Nairobi based BitPesa is focusing on providing remittance services for the UK to Kenya at variable rate of 3% on transfers. Senders in the UK own or buy Bitcoin. BitPesa helps facilitate this process through information on its website. The digital currency is used as a means of exchange. Once a sender in the UK makes a transfer through BitPesa, the Bitcoins are immediately converted into Kenyan shillings so that people on the receiving end in Kenya don't have to use Bitcoin or even know that the senders have used it. Funds are only held in Bitcoin for a matter of minutes or seconds, which limits risks associated with fluctuating currency values. Kenyan shillings land directly into mobile wallets and bank accounts in Kenya, which recipients can use directly or convert to cash. There are many compelling reasons why digital currencies could significantly impact financial inclusion.

M-PESA is a mobile phone-based service for sending and storing money offered by Safaricom, Kenya's largest mobile service provider. Safaricom customers can register for M-PESA by visiting one of more than 10,000 merchants who act as "agents" for account opening, handling of deposits and withdrawals into the customer's virtual "wallet," and customer support. Customers can then use an application on their mobile phone to check their balance, send money to other people, pay bills, and purchase mobile phone airtime. Customer funds are held in a special trust account at the Commercial Bank of Africa.

Since its commercial launch in March 2007, M-PESA has achieved substantial scale along several key metrics. Nearly 7 million customers have registered with the service. An average of 150 million Ksh (US$1.96 million) is transferred through M-PESA per day, mostly in small amounts averaging just over 1,500 Ksh (US$20) per transaction. So far, the system has handled over 130 billion Ksh (US$1.7 billion).

For people living in rural areas or on less than $2.50 per day, mobile money is emerging as a common source of financial inclusion. Active mobile money accounts in Kenya, Tanzania, Rwanda, and Ghana among adults is 58, 34, 17, and 17% respectively while rural accounts respectively are 56, 55, 61, and 40%. In Ghana, rural access has doubled since 2010, and in Rwanda, people living below the poverty line are more likely to be active mobile money users than those with higher incomes.

Particulars	Kenya	Tanzania	Rwanda	Ghana
% of adults with required Id	81%	64%	87%	92%
% of adults with basic numeracy	90%	93%	87%	95%
% of adults who owns a mobile phone	74%	72%	47%	91%
% of adults who has sent/received text messages	69%	61%	37%	74%

Mobile money can deliver financial inclusion benefits only if a range of services are offered by providers and used by customers. Across Kenya, Tanzania, Rwanda, and Ghana, people still list domestic remittances as their top reason for starting to use mobile money. Forty-five percent of people use money for domestic reason. Rwandan mobile money users are the most likely to pay bills via their mobile devices, with 25% of active mobile money users taking advantage of this feature. While Ghanaians are financially active; for instance, 86% of active mobile money account holders save and they are generally not using their mobile money accounts for these purposes.

Digitizing existing payment streams that are currently occurring in cash is a significant opportunity for mobile money growth in Rwanda and Ghana. In both countries, these payment streams exist, but have not shifted to digital formats yet. Seventy-one percent Rwandan and 58% Ghanaians pay for insurance but only 0.1% use mobile money, so there is great potential for these services for mobile money transfers.

14.13 Challenges and Solutions

Since its inception, the digital financial services (DFS) industry has been subject to a wide range of frauds, across different markets and players of the ecosystems. The diverse nature and scale of these fraud cases have been evolving across markets. As a result, most digital financial services operators are now deploying in-house, dedicated fraud teams. Supply-side research by The Helix Institute of Digital Finance in Bangladesh and Kenya identified fraud as the biggest concern amongst agents, in 2013 and 2014. The recent surveys in both Tanzania and Uganda highlighted how prevalent it has now become 42% of agents and a little more than half of agents, respectively, indicate that either they personally, or one of their employees, have experienced fraud in the last year. In other markets, such as Zambia and India, it has been cited as one of the top challenges to an agent's business in 2014.[7]

DFS providers need sophisticated risk/fraud management systems (FMS). The FMS help service providers to understand the nature of frauds. A lot of data is generated from different systems in any DFS provider. FMSs enable fraud managers to use this data and design rules and algorithms to track the pattern of frauds. They enable them to set fraud rules which help in identifying collusion checks, velocity checks, threshold checks, black-list checks, new

subscriber checks, profile checks, SIM swap checks, etc. These systems help providers to understand fraud and track its evolution over time – thereby helping to manage them effectively and reducing revenue losses. Velocity and pattern detection tools, which are real-time, dynamic, efficient, and effective in finding patterns that point to fraud, add powerful capabilities for next generation fraud management.

Data is critical for monitoring and managing DFS fraud. Reliable data is generated through working with technology providers to build robust systems or tools that determine and track normal and abnormal behavior. Providers need to ensure robust prevention measures on the first line of defense is registration or account opening processes. Combining this with data-driven alerts can provide real-time, multi-channel defenses to address a wide spectrum of fraud threats. At the same time, more traditional "maker-checker" approaches to ensure segregation of duties, together with back-office monitoring and reconciliation teams, are key to maintaining the integrity of digital finance systems.

The fraudsters take benefits of vulnerability of service provider's weaknesses like lack of internal control. Providers need to ensure robust internal controls. They can be of two types: preventive controls and detective controls. Some examples of preventive controls can be measures like limiting number of transactions per day (value or volume), authentication of transactions, having passwords at different levels, providing limited access to employees, etc. These are generally low-cost solutions to the providers. Detective controls, on the other hand, are post facto. Typical detective controls are: understanding the patterns of transaction activity, reviewing high-value/high-volume transactions, monitoring log-in activity of employees, etc. These tend to be expensive, since DFS providers need to build systems for this. When any fraud happens, preventive measures offer the first line of defense.

Different providers have different organizational structures, which determine the number of stakeholders involved. Internally, managers, back-office support, customer service, and finance and revenue assurance teams must all be aware of fraud risk and encouraged to communicate any anomalies or suspicious activity to relevant internal parties. External communication to agents and customers is equally important for effective preventive control. Awareness creation among customers on how to avoid the risk of fraud is a critical preventive measure to reduce customer spoofing/phishing scams. Lastly, in the event of the detection of suspicious activity, clear internal procedures defining both how to escalate awareness and ensure immediate action, need to be in place. Whistle-blowing within institutions should also be encouraged.

DFS ecosystems continue to evolve; however, with this the scope for fraud is also growing. For DFS to realize its full potential, all stakeholders inclusive of regulators, donors, providers and their partners, as well as customers, have a role to play in combating fraud – and minimizing the risks of DFS being swept away by burgeoning typhoons of fraud.

www.elsevierdirect.com

Opening of Platforms and Application Programming Interfaces (APIs) can be used to synchronize such differences. APIs enable new applications to be built on top of pre-existing products, thereby capitalizing on the product's existing customer base. Open platforms and open APIs, which are still relatively rare, hold the potential to facilitate access to a broad range of products and services, and thus enhance financial inclusion. Digitally collected data, including e-commerce and mobile transaction histories, can complement or substitute traditional methods of client identification and credit risk assessment. Biometric data, such as fingerprints and iris scans, allow providers to meet due diligence requirements for customers with insufficient traditional forms of identification.

Better data collection and analytics inform more accurate customer segmentation and human-centered product design, such as clearer user interfaces or targeted alerts and notices to consumers. Removing barriers to financial access and inclusion, designing policy incentives to enhance inclusion, e.g. tax incentives and mitigating risks, such as fraud and mis-selling of inappropriate products, data security, and technical vulnerabilities around data sharing may boost financial inclusion. Inappropriate regulatory requirements create barriers to financial inclusion.

Data ownership has potentially large implications for development impacts. There is no clear uniform regulatory policy on the issue. The expansion of digital finance and the participation of specialized new players also create new risks that need to be identified, managed, and mitigated. Traditional financial regulation is often not designed to deal with these innovations. Yet, customers need to be protected from risks such as fraud and mis-selling, especially those who have little experience with the regulated financial sector. The emerging industry will crystallize equitable policy in due course.

Worldwide branchless banking is shaping up. In Latin America, particularly Brazil was a pioneer in branchless banking. According to a recent whitepaper on card and payment trends in Latin American Countries (LAC), Brazil has about 400,000 authorized agents, while in Peru banking agents now carry out 16% more transactions than bank tellers. In Mexico, agents are to be found in retail chains such as Oxxo, Soriana, and Walmart, and in Colombia, the number of banking agents is growing 44% annually, compared to just 6% for bank branches. As Mondato Insight noted last week, governments in some parts of Latin America and the Caribbean have embraced digital payments for bulk disbursements, such as social payments or conditional cash transfers, while the use of prepaid cards is also fairly widespread. Notable examples include Bolsa Familia in Brazil, Asignación Universal por Hijo in Argentina, Programa Juntos in Peru, Familias en Acción in Colombia, and Oportunidades in Mexico. The trend towards digitization has been gathering pace, partly in recognition of the potential efficiencies and improved access to financial services that they create. Since 2013, for example,

all Mexican government employees and social security beneficiaries receive their money via direct deposit.

Tigo has been the most successful company mobile money deployment in the LAC region to date, with deployments in Bolivia, El Salvador, Guatemala, Honduras, and Paraguay. Tigo Money in El Salvador, in particular, is one of Millicom's strongest deployments globally, where mobile money accounts for over 20% of Tigo's mobile subscribers base, and has been driven by bill payments and international remittance. According to Greg Reeve, COO, MFS and Ronald Alvarenga, Product & Commercial Director, Latin America at Millicom, the key to Tigo Money's success is that it has not relied on a one-size-fits-all commercial model in order to succeed: "We place a strong emphasis on identifying and implementing a bespoke strategy for each individual market in the region. More than this, Millicom has placed understanding the individual customer at the center of our Mobile Financial Services (MFS). We offer products and services that people actually want and need, tailored to their circumstances. In some markets it is money transfer, in others it is about paying your bills or collection services; in others it is receiving international remittances."

The government disbursements have been a significant driver for the growth of DaviPlata in Colombia in the four years since its launch. According to Hair Muñoz Gonzalez, Head of DaviPlata, the pillars of success have been the sustainable and profitable business model that is free for the user, the utilization of the language/slang of their clients, and the mobility of the service – allowing the user to do everything on their phone, without the need to go to an agent. When competing with cash, people comprehend the value-add of a mobile wallet only when the service is free. Understanding cultural differences and learning from their customers, rather than teaching them, has proven instrumental in DaviPlata's success, in Mr. Muñoz's assessment. Government of India has initiated its scheme to be operated using unique identification number and digital technology.

Majority of the banks are focused on developing solutions for their middle class and affluent customers, and offer at least some form of mobile banking. Even for this segment, however, the number of digital wallets available to consumers as e-commerce in LAC grows has been growing, and adoption rates are also trending upwards. Mercado Pago and PayPal are regional players, but there also exist a variety of smaller players across the continent, including Mondero in Argentina and, indeed, about a dozen wallets in Brazil, including Banco de Brasil's Stelo, b-Cash, Oi Carteira, and PagSeguro. These developments have not necessarily been to the exclusion of base of the pyramid customers. Most banks in the region have smartphone apps for their clients, while some banks, such as Davivienda in Colombia, are developing mobility strategies to enable all their clients to access services on smartphones. These mobile products allow customers to do everything online, without the need to go to a branch, thereby increasing the clients' user experience while also cutting operational costs. In Mexico, the

Banamex partnership with MasterCard and the BBVA partnership with Visa are both putting digital in the center of their strategies, with a focus on taking NFC/HCE services to market. Due to its large number of people at bottom of pyramid, economies of scale may be gained as there is enough opportunity to tap poor people in financial service net through digital technology and mobile payments.

14.14 The Outlook

The uses of smart phone and biometric or finger print based transactions are emerging in financial market, which may change the landscape of the industry. In India, digibank, a smart bank shrunk to fit into consumers' smartphone, is flexible, available and totally dependable with high standards of safety. digibank is brought by DBS Bank, one of Asia's leading financial institutions that's recognized as the 'Safest Bank in Asia' by Global Finance for seven consecutive years. A bank account can be opened hassle-free, with only one document, i.e. Aadhar card. digibank is India's first paperless, signatureless & branchless bank. The fingerprint reader-enabled smartphones are in the market; fingerprint-based banking is slowly gaining momentum. IndusInd Bank in India has been pioneer in this. From January 2017 onwards, all mobile phones manufactured in India should mandatorily have fingerprint reader. Hence, penetration will grow multifold (The Indian Express, July 2016).

The final two layers of the "India Stack" have great relevance to the future of banking. The Unified Payment Interface (UPI) layer, a product built by the National Payment Corporation of India (NPCI), a non-profit company collectively owned by banks and set up in 2009, will revolutionize payments and accelerate the move towards a "cashless" economy. So "pushing" or "pulling" money from a smartphone will be as easy as sending or receiving an email. This product from NPCI is the latest in several payment systems that they have developed, from the National Financial Switch, National Automated Clearing House, and RuPay cards, to the Aadhaar Payment Bridge, the Aadhaar-enabled Payment System and IMPS, a real-time payment system.

The move to a "cashless" economy will be accelerated by the Aadhaar-enabled biometric smartphones. So credential checking in banking will move from "proprietary" approaches (debit card and PIN) to "open" approaches (mobile phone and Aadhaar authentication). As such, the holy grail of one-click two-factor authentication, now available only to giants like Apple, will be available to kids in a garage to develop innovative solutions.

India goes from being a data-poor to a data-rich economy; in the next two to three years, the electronic consent layer of the "India Stack" will enable consumers and businesses to harness

the power of their own data to get fast, convenient, and affordable credit. Such a use of digital footprints will bring millions of consumers and small businesses (who are in the informal sector) to join the formal economy to avail affordable and reliable credit.

As data becomes the new currency, financial institutions will be willing to forego transaction fees to get rich digital information on their customers. The elimination of these fees will further accelerate the move to a cashless economy as merchant payments will also become digital.

This will also shift the business models in banking from low-volume, high-value, high-cost, and high fees, to high-volume, low-value, low-cost, and no fees. This will lead to a dramatic upsurge in accessibility and affordability, and the market force of customer acquisition and the social purpose of mass inclusion will converge.

These gale winds of disruption and innovation brought upon by technology, regulations, and government action, will fundamentally alter the banking industry. Payments, liabilities, and assets will undergo a dramatic transformation as switching costs reduce and incumbents are threatened. As the insightful report from Credit-Suisse has so well explained, there is a $600 billion market capitalization opportunity waiting to be created in the next 10 years. This will be shared between existing public and private banks, the new banks and new-age NBFCs. It may even go to non-banking platform players, which use the power of data to fine-tune credit risk and pricing, and make money from customer ownership and risk arbitrage.

Neon, a millennial-targeting smartphone-based bank that uses facial recognition technology to authenticate its customers, has launched in Brazil. The bank's iOS and Android app uses biometric facial recognition technology from US vendor Daon so that customers can ditch usernames and passwords and log in and authenticate transactions by taking selfies with their phones. The app will have the usual features associated with mobile banking, allowing users to check their balance, make transfers, pay bills, receive payments, categorize their spending habits, and create financial goals. Members also get two Visa-branded debit cards; a physical one for real-world purchases and a virtual one for online payments.

14.15 Conclusion

Financial services are backbone of the society. They have pervasive effect on life of the citizens and hence bearing on all socio-economic indicators. Effective financial services are good for the citizens, society and governments. Various circumstances have kept many people out of net of financial services which has created a gap between those who are in the financial services net and those who are not. This gap is good opportunity for business, civil societies, and governments to fill. No one approach or instrument can fill the gap. Digital currency and

www.elsevierdirect.com

mobile technology is most potential instrument to cover non-served population in financial service net. Different approaches, technologies, and products are used across the globe. One size does not fit all in all circumstances and time. Some of them have effectively worked in particular region or segment of customers. There are still many challenges, which hopefully overcome as successive governments and business managers learn from experience and employ better approaches. The governments are expected to make appropriate regulations to make product more affordable, fraud-proof system, protect consumers interest, prevent consumer exploitation, establish accountability, pro-women, and poor and rural population policy, business friendly policy, and reasonable taxes. Businesses are expected to make universal and easy access, friendly product design, affordable prices, and transparent services. Civil societies are expected to create awareness, raise voice for the consumers' rights, advocate right policies, create pressure groups, and bridge the trust gap between stakeholders. Education and Research institutes are expected to conduct market and technical research to propose appropriate product design, business strategies to reach unserved population, and to serve better the existing consumers and to reflect right feedback of the consumers.

References

Beard, Morgan, 2015. U.K. Consumer Mobile Payment Study. TSYS Report.

CMF-IFMR Newsletter Article, 2012. A closer look at the financial viability of the Business Correspondent Model, October 2012.

European Commission, 2008. Financial Services Provision and Prevention of Financial Exclusion.

Heyer, Amrik, Mas, Ignacio, 2009. Seeking Fertile Grounds For Mobile Money: Mobile Money For The Unbanked. Gates Foundation Working Paper, September 2009.

Mbiti, Isaac, Weil, David N., 2011. Mobile Banking: The Impact of M-PESA in Kenya. NBER Working Paper, June 2011.

Nandhi, Mani, 2012. Impact of EKO's SimpliBank on the Saving Behaviour and Practices of Low Income Customers: The Indian Experience. CMF-IFMR Working Paper, October 2012 (IMTFI Funded Project).

Sapovadia, Vrajlal, 2015. Legal Issues in Digital Currency, Hand Book on Digital Currency. Elsevier Publications. May 2015.

The Indian Express, July 2016. The Coming Revolution in Indian Banking, Increasing Penetration of Smartphones, Aadhaar-Linked Bank Accounts and a Host of Powerful Open and Programmable Capabilities is Set to Create The 'Whatsapp Moment' for Indian Banking;
http://www.cgap.org/;
http://www.socialwatch.eu/wcm/financial_exclusion.html;
http://inclusioncentre.co.uk/wordpress29/the-financial-inclusion-challenge/the-causes-of-financial-exclusion;
https://www.jrf.org.uk/report/understanding-and-combating-financial-exclusion;
http://www.economist.com/news/economic-and-financial-indicators/21648642-financial-exclusion;
http://www.worldbank.org/en/topic/financialinclusion/overview#1;
http://www.worldbank.org/en/topic/financialinclusion/brief/achieving-universal-financial-access-by-2020;
http://blog.mondato.com/latin-america-2/;
http://www.digitalcurrencycouncil.com/;
http://economictimes.indiatimes.com/articleshow/51787159.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst;

http://www.helix-institute.com/blog/burgeoning-%E2%80%98typhoons%E2%80%99-digital-financial-services;
www.rediff.com.
UFA2020 Overview, 2017. Universal Financial Access by 2020. World Bank Report.

Notes

1. http://www.worldbank.org/en/topic/financialinclusion/overview#1.
2. UN Capital Development Fund.
3. Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom.
4. The Financial Inclusion Center.
5. https://www.digitalcurrencycouncil.com.
6. Bank for International Settlement.
7. Agent Network Accelerator (ANA) Surveys.

www.elsevierdirect.com

CHAPTER 15

Digital Financial Inclusion in South East Asia

Francis Koh, Kok Fai Phoon, Cao Duy Ha

Contents

15.1 Introduction 387

15.2 Definition and Review of Digital Financial Inclusion 388

15.2.1 Financial Inclusion 388

15.2.2 Digital Financial Inclusion 390

15.3 Digital Financial Inclusion in South East Asia 393

15.3.1 Current Status of Digital Financial Inclusion in South East Asia 393

15.3.2 Digital Financial Inclusion Initiatives in South East Asia Countries 395

Singapore *396*

Malaysia *397*

Thailand *397*

Indonesia *398*

Philippines *398*

Cambodia *399*

Myanmar *399*

15.4 Analysis and Discussion 401

References 402

15.1 Introduction

Financial inclusion is a globally important objective, with increased initiatives by national central banks, international agencies including the IMF, the World Bank, ADB, and non-

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00015-2
Copyright © 2018 Elsevier Inc. All rights reserved.

governmental organizations including the Bill & Melinda Gates Foundation, Consultative Group to Assist the Poor (CGAP), the Alliance for Financial Inclusion (AFI) to promote the well-being of the global poor and disadvantaged. Fortunately or co-incidentally, we are in the midst of the greatest information and communications revolution in human history which will catalyze these initiatives.

According to Owens (2013), interest has grown in using new mobile technology to provide financial services to the underbanked and unbanked since 2004. Even among the poorest 20 percent of households, nearly 7 out of 10 have a mobile phone (see World Bank, 2016). Thus, Microsoft's Bill Gates projects that: "*By 2030, 2 billion people who don't have a bank account today will be storing money and making payment with their phones*."

This paper contributes to the literature on digital financial inclusion in surveying its current status in South East Asia. It projects the trajectory by which these diverse nations can benefit from technological revolution and the key supports that need to be put in place to enable a faster pace of financial inclusion. Providing a measure of the current status is an important starting point as national policy makers need data to develop their strategies and measure the effectiveness of their implementations (Gadanecz and Tissot, 2015).

In the paper, we first introduce and define financial inclusion and discuss digital technology that support financial inclusion efforts. Next, recent status of digital financial inclusion for the countries in South-East Asia (SEA) is reviewed using the results of the Global Findex surveys (Demirguc-Kunt et al., 2015 and Demirguc-Kunt and Klapper, 2012). We then discuss initiatives that are being put in place for these SEA nations to advance along the pathway to an inclusive digital economy. The initiatives will be discussed in relation to the various stages of evolutionary development (Radcliffe and Voorhies, 2012). Such a mapping provides a road map for each country starting from where it is at, what needs be done and the resources, processes and regulatory framework that needs to be put in place to progress up the ladder of digital finance inclusion.

We conclude with a discussion on concerns and pitfalls that may detract the populace of SEA nations from benefiting from the digital revolution.

15.2 Definition and Review of Digital Financial Inclusion

15.2.1 Financial Inclusion

There is, yet, a formal definition for the term "financial inclusion". Most usage of the term refers to two distinct aspects of financial inclusion: *"access"* to the financial products, and *"usage"*, being the ways customers use the services provided. The Center for Financial Inclusion at Accion, an action-oriented think tank, for example defines "financial inclusion" as:

> *"A state in which all people who can use them have access to a full suite of quality financial services, provided at affordable prices, in a convenient manner, and with dignity for the clients. Financial services are delivered by a range of providers, most of them private, and reach everyone who can use them, including disabled, poor, rural, and other excluded populations."*

Thus, there are, however, two dimensions of financial inclusion that are not easily quantified (see Gadanecz and Tissot, 2015). The first is the quality of services and how they fit the clients' needs. The second is the qualitative use of financial services: whether they are widely used by everyone, including the disadvantaged to bring about an improvement in their economic well-being. The differing qualitative dimensions, along with the quantifiable measures of access and usage, likely explain the broad definition of financial inclusion and the consequential use of varied measurement indicators.

Despite the definitional issue, data used to measure financial inclusion can be categorized as measures of demand and supply of financial services. On the demand side, the Global Financial Inclusion Database (Global Findex), funded by the Bill & Melinda Gate Foundation in partnership with Gallup, provides a useful data set that can be used for cross-national analysis. This data set is based on survey data collected in the 2011 and 2014 calendar years, covering more than 150,000 adults in 143 countries and representing around 97% of the world population (Demirguc-Kunt et al., 2015 and Demirguc-Kunt and Klapper, 2012). The data set comprises 44 indicators that measure how people make and receive payment, save, borrow, and manage risk. It allows us to examine the most recent status of inclusion in SEA nations. We are able to compare the status of financial inclusion for the SEA nations (except for Laos that was not among the 144 countries surveyed).

For completeness, databases on the demand side include FinScope Survey, FinAcces/Access to Financial Services Survey, Financial Inclusion Tracker Surveys (FITS), Financial Inclusion Insight Survey (FII). The FII is unique among these data sets in its strong emphasis on mobile money and digital financial services. It also includes welfare indicators based on the Grameen Progress out of Poverty Index (PPI), addressing the welfare dimension of the digital financial inclusion. We did not use this survey as it covers only eight countries, namely Kenya, Tanzania, Uganda, Nigeria, India, Pakistan, Bangladesh, and Indonesia (Nielsen, 2014).

On the supply of financial services, the most comprehensive database is the IMF Financial Access Survey (FAS). The FAS is self-reported by national government regulators, and comprises annual data for 189 nations from 2004 to 2014. Other databases include the GSMA Mobile Money Adoption Survey, the World Bank Global Payment Survey, the MIX's Geospatial Maps and FSP Maps. GSMA Mobile Money Adoption Survey is self-reported information from 114 service providers from 57 countries, of which 100 providers submitted mobile

www.elsevierdirect.com

money information, 18 submitted mobile insurance information, and 12 provided mobile credit and savings. The MIX's Geospatial Maps and FSP Maps combined data analytics and geospatial mapping to allow for an intuitive understanding of the distribution of financial inclusion. The Maps, unfortunately, are limited in the number of participating countries due to the collection cost and infrequency of reported data.

15.2.2 Digital Financial Inclusion

Digital financial inclusion has been a topic of interest for many years. As early as 1997, using a program in the Philippines supported by the USAID, rural banks, and Globe, a leading telecommunication service provider expanded financial services to the unbanked (USAID, 2013). With the use of digital technology, financial services have recently been focused on electronic money transfer and mobile technology to accelerate financial inclusion to the unbanked. This focus resulted from three converging trends:

(1) Increasing mobile subscribership, that in many developing countries have exceeded the size of their population,
(2) Success of initiatives such as M-Pesa in Kenya, and
(3) Significant financial support provided by private foundations such as the Bill & Melinda Gates Foundation and public-private sectors player including the Better Than Cash Alliance (see Owens, 2013).

Optimism over the impact of digital technology increased when Bill Gates in 2015 projected financial inclusion trend through mobile channel as one of his four mega bets for the next 15 years. He stated that:

> *"By 2030, 2 billion people who don't have a bank account today will be storing money and making payment with their phones."*

(*Bill & Melinda Gates Foundation, 2015*)

Even with such optimism over the impact of digital technology on financial inclusion, there are significant obstacles in the path in providing access to the under-served and improving their quality of life. Obstacles include providing the infrastructure, providing the appropriate services, and moving the poor up the economic ladder.

The core objective of digital financial is to provide connectivity between the poor and their peers and a range of providers. Radcliffe and Voorhies (2012) illustrate the required infrastructure components for the digital financial inclusion in Fig. 15.1 as follows.

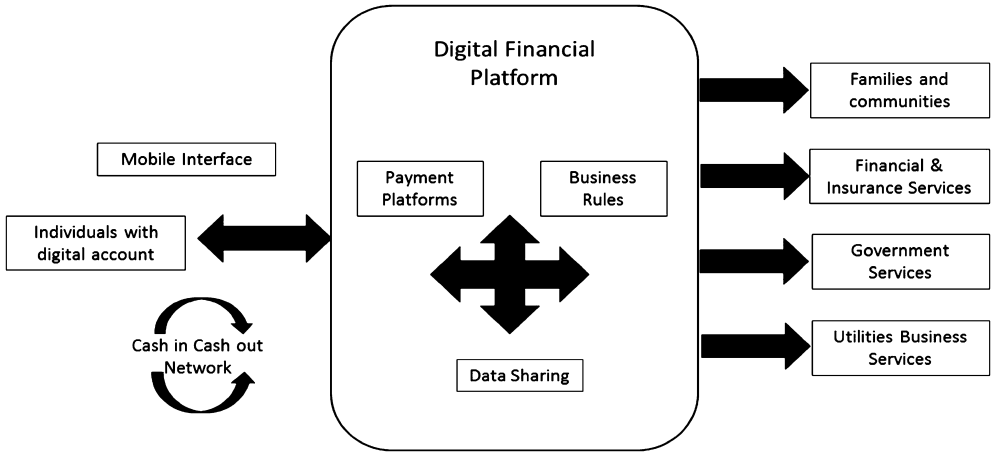


Figure 15.1: Infrastructure components of digital financial platforms.
(Source: Adapted from Radcliffe and Voorhies, 2012)

The key to accelerate digital financial services is the use of technology to provide connectivity. In Fig. 15.1, the authors illustrated a telecommunication network, enabling customers to communicate with the provider's transaction authorization system through mobiles. This network provides identification capturing points and virtual account for customers' payment transactions. Other components of this network are comprised of:

- Cash in-cash out point (CICO) to enable the poor to convert their physical cash into digital money and vice versa;
- A payment platform (or multiple connected platform) that allows the poor to transact with counterparties, regardless of their payment providers. This platform must also provide a whole range of services including saving, borrowing, and buying insurance;
- Common business rule and technical standard to provide cross-providers settlement;
- Common business rule and technical standard to provide data sharing and mining capability enabling product development and fraud prevention.

We have adapted the approach of Radcliffe and Voorhies' multi-stage evolutionary process to eventuate the full benefit of digital financial inclusion. The process is illustrated in Fig. 15.2.

It is possible that a few SEA nations, due to their relative isolation, may not have reached the first stage of the evolutionary process. To achieve a fully inclusive economy, the road map is described as:

- **Stage 1**: widen basic connectivity among the poor and rural areas. The first stage is critical in providing a communication channel for the customers and CICO agents with the

www.elsevierdirect.com

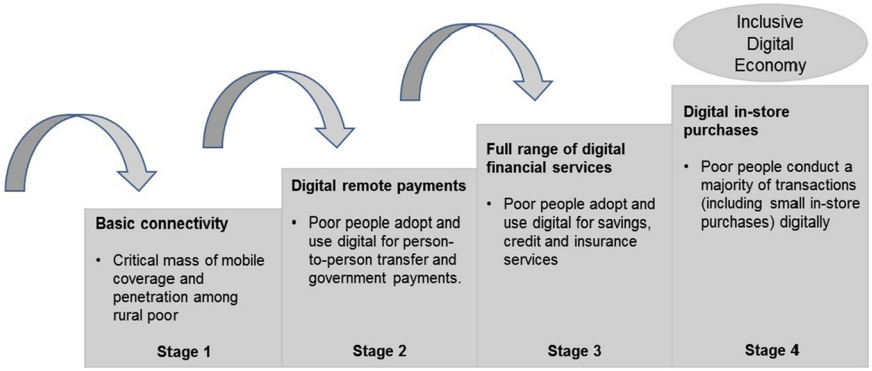


Figure 15.2: Evolutionary process to eventuate digital financial inclusion.
(Source: Adapted from Radcliffe and Voorhies, 2012)

providers' transaction authorization system. This stage is feasible globally (including developing countries) as advances in mobile technology have resulted in lower marginal cost. The main objective in this stage is to connect people to the network and the challenge is not access to technology or regulatory constraints but the income level of users.

- **Stage 2** provides the basic payment system for the unbanked through connectivity established in Stage 1. It is widely recognized that the unbanked use a range of basic payment transactions such as person-to-person transfer (P2P) and government-to-person transfers (G2P) in most countries. Users are retained within the mobile network in this stage through frequent use for payment transaction. The challenges in this stage are mainly regulatory. Separating payment and financial services intermediaries, the regulators can reduce the impact on financial intermediaries arising from the payment system. Regulators must also clarify know-your-client's (KYC) requirements and the legal status of CICO agents. Mobile network operators (MNOs) appear better placed than banks in knowing the users and acting as intermediaries with their wide database of mobile users and experience dealing with multi-agents systems.
- **Stage 3** provides sophisticated digital financial services for the unbanked. Financial intermediaries gain confidence to provide the much needed financial products such as saving, credit, and insurance to the unbanked. The main challenge at this stage is the interoperability between the current financial sectors network with the transaction system developed in the mobile networks.
- **Stage 4** is the inclusive digital economy where the currently unbanked have access to financial services and are able to carry out most of their transactions online. The arrivals of mobile payment system such as Apple Pay and Samsung Pay in the United States and Singapore and Alipay in China portent this digital economy.

We next discuss the most recent status of financial inclusion and digital inclusion for the SEA nations using the financial inclusion indicators from the Global Findex surveys for 2011 and 2014. We should note that we only discuss the SEA nations that Global Findex has data for. Lao PDR, Brunei are not included while Timor-Leste is not yet a permanent member at the time of the surveys.

15.3 Digital Financial Inclusion in South East Asia

15.3.1 Current Status of Digital Financial Inclusion in South East Asia

The South East Asian (SEA) nations' stage of economic development ranges from a developed country, viz. Singapore to nascent economies like Cambodia and Myanmar. As a result, significant differences in bank account penetration rates are expected among these nations. Fig. 15.3 below shows the account penetration rates for adults (aged 15+) and the cumulative annual growth rate in account penetration rates in the eight SEA nations in the Global Findex survey as of 2014, namely: Singapore, Malaysia, Thailand, Indonesia, Philippines, Vietnam, Myanmar, Cambodia. The account penetration rates in SEA nations can be categorized into three groups:

(1) Singapore, Malaysia, and Thailand, the more developed countries in the region, have banking account penetration of over 80%;
(2) Indonesia, Philippines, and Vietnam, with about 30 to 40% account penetration rates, and
(3) Myanmar and Cambodia with about 22% account penetration rate.

Cambodia achieved the highest growth rate of 80% per annum in account penetration rate during the period 2011 to 2014. While we do not have data for Myanmar in 2011, we expect that bank penetration rate will be of a similar order as that of Cambodia. Myanmar has been rapidly developing its banking sector growing from a low base with credit provided to the economy representing only 6% of the country GDP. Growth in account penetration is also likely to have received a significant boost with the removal of sanctions imposed by major developed countries since 2012 (KPMG, 2013). The most developed group of SEA nations saw low growth rate in the single digit and the immediate group saw growth rates of more than 10% except for the Philippines. Philippines' banking sector expanded at a slow average rate of 6% per annum during the period 2011–2013, even though the bank accounts' penetration rate in the country is still a low 31%. See Fig. 15.3.

As for banking infrastructure, the most developed group has more than 10 bank branches per 100,000 adults in 2014 but also has the highest legacy assets of more than 5 in 2011. The

www.elsevierdirect.com

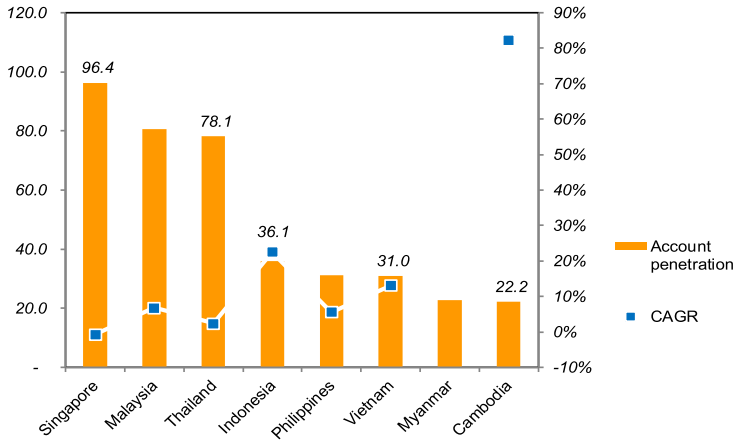


Figure 15.3: Banking account penetration as at 2014 and 2011 to 2014 CAGR of SEA nations.
(Source: Global Findex surveys 2014 and 2011)

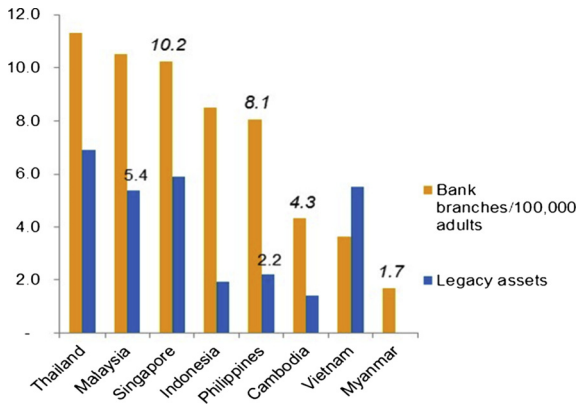


Figure 15.4: Infrastructure of banking sectors in SEA nations.
(Source: Global Findex surveys 2014 and 2011)

legacy assets is a self-calculated indicator based on the Global Findex 2011 survey's indicators. This indicator is calculated by dividing the number of ATMs per 1000 sq km to the number of bank branches per 1000 sq km. The legacy assets can be viewed as sunk-cost that banks incurred to service customers using ATM technology (with mobile being considered as the alternative to ATM technology in the financial services industry). See Fig. 15.4.

The second group comprising Indonesia and Philippines (but not Vietnam) has about 8 bank branches per 100,000 adults but low legacy asset level of 2. Cambodia and Vietnam are in the third group with around 4 bank branches per 100,000 adults. The key difference between Vietnam and Cambodia is in their investment in the banking sectors, where the banking sector

in Vietnam has invested in more than 5 ATMs per branch; that number for Cambodia is much lower at around 2. This difference likely suggests that alternative technology such as mobile banking is more widespread in its use to deliver financial services in Cambodia. Myanmar banking sectors are relatively underdeveloped among the SEAs. In 2014, there was only about 1.7 bank branches per 100,000 adults and less than 1 bank branch per 1000 sq km. There is no recorded number of ATMs for Myanmar to measure its legacy assets.

The difference in the banking-technology employed in Vietnam and Cambodia is more evident when looking at the percentage of adults with mobile accounts as of 2014. Mobile banking technology is more developed in Cambodia compared with several SEA nations. Of the 22.2% of Cambodian adults with a banking account, 60% have used the mobile to do bank transaction. Vietnam, Indonesia, and Myanmar are the nations that are slow to employ mobile technology in banking.

Our final observation is related to the customer demand. The main barriers to account ownership in SEA nations are common to populations elsewhere, viz. not having money is the reason for 59% respondents in the Global Findex 2014 survey. The second most common reason for people without a banking account in SEA nations is that a family member already has one, cited by 35% of survey participants (Demirguc-Kunt et al., 2015). Moreover, the majority of SEA nations respondents find it challenging to raise money during crisis periods where more than 30% of the adult population find it impossible to come up with emergency fund, except for those in Singapore and Myanmar. This is a high number, within the context of various social support arrangements in SEA countries such as family and friends, savings and loan from employers. The low number in Singapore can be due to its advanced economy, high per capita income and savings rate along with more developed social support policies. However, the low 9% in Myanmar among the SEA nations may be due either to "sample bias" or unique local arrangements by a totalitarian regime that is legitimized with a strong social support network. We need care in interpreting the findings for a nascent economy like Myanmar.

Overall, our review of the status of financial inclusion failed to yield conclusive evidence of the proclaimed welfare benefits from digital financial inclusion. See Fig. 15.5.

We next summarize and discuss recent initiatives by SEA governments and financial institutions to increase digital financial inclusion in their nations. We relate such initiatives to the digital financial inclusion development pathway framework of Radcliffe and Voorhies (op cit.).

15.3.2 Digital Financial Inclusion Initiatives in South East Asia Countries

This section provides a survey on some of the most prominent initiatives among SEAs countries in promoting the digital financial inclusion. The main objective here is to form a general

www.elsevierdirect.com

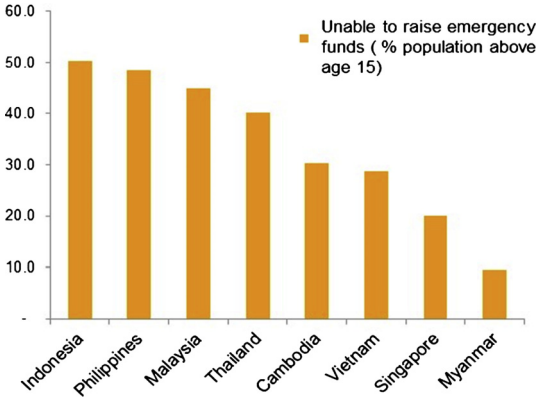


Figure 15.5: Percentage of population which cannot raise emergency funds.
(Source: Global Findex surveys 2014 and 2011)

view on the mobile banking technology utilization and on the main drivers of these movements rather than a comprehensive survey of individual participants.

Singapore

As the most developed country in the region with almost universal financial inclusion, the mobile banking technology in Singapore not surprisingly led by the banks, but also in partnership with mobile network operators (MNOs). The most advanced mobile banking service in Singapore is "Dash," created by Singapore Telecoms (Singtel) and Standard Chartered Bank. Launched in June 2014, Dash allows customers to carry out online payment, fund transfer, insurance purchase, and loan approval through mobile (see Singtel, 2014). The unique technical feature of Dash was developed by Singtel which has applied for a patent for it. The feature has enabled two phones to detect each other using GPS location data and other key indicators, instead of the more common Near Field Communication (NFC) technology. Other banks also have introduced their own mobile banking applications like DBS Bank with DBS Paylah! and United Overseas Bank (UOB) with Mobile Banking. These mobile banking applications are mainly the mobile version of online banking with the standard features of account summary, money transfers and bill payments with little additional add-on features such as eAng-Bao for DBS Paylah!.

Relatedly, the Singapore government has focused its recent budgets to include research and development in financial technology that will establish its position as a digitally inclusive economy.

www.elsevierdirect.com

Malaysia

Malaysia has emerged as a global center of financial inclusion with the establishment of Alliance for Financial Inclusion's permanent office in its capital, Kuala Lampur since October 2014. The Alliance for Financial Inclusion is a global network of policymakers from 120 financial institutions, representing 95 developing and emerging countries. The most important initiative to drive digital financial inclusion in Malaysia has been the introduction of "MyMobile" by the country's central bank, Bank Negara Malaysia (BNM). "MyMobile", officially launched on May 2013 under BNM's wholly owned subsidiary, is a project carried out in cooperation with the country's three largest banks, namely CIMB, Maybank, and Public Bank, and the three largest MNOs: Maxis, Celcom, and Digi (see Bank Negara Malaysia, 2013). The service, "MyMobile" allows banking service customers to carry out airtime top-up, money transfer, bill payment, and remittance in selected geographical areas. Customers do not need a smartphone to access the services on "MyMobile." By allowing the broadest interoperability within banks and MNOs' networks, BNM has built the transactional infrastructure towards a more inclusive digital economy.

Thailand

In contrast to Malaysia's model of interoperability and partnership between the banking and telecommunication biggest players, there are two business models for mobile banking in Thailand. MNOs driven mobile financial service includes "Advanced MPay" introduced by AIS (Thailand's largest telecommunications company) in late 2014 and TrueMoney introduced by True Corporation (one of the top three telcos), in 2005. These two initiatives mainly tapped the retail network of the parent companies to accelerate bill payment (in the case of TrueMOney) and facilitate transactions for the some 200,000 (as at end 2011 (IFC, 2011)) AIS airtime merchants.

The second business model is a partnership between MNOs and banks. This model is illustrated by the partnership between DTAC (one of top three telcos in Thailand) and K-Bank (one of three largest banks in Thailand). The partnership introduced SIM cards, which are linked to bank accounts at K-bank. Customers can use this e-wallet to do basic financial services such as airtime top-up, fund transfer, and bill payment.

Financial institutions in Thailand have only introduced mobile banking recently, with their huge investment in branches and ATMs networks. For example, Thailand's Bangkok Bank, the largest bank in Thailand with 1000 branches and 17 million customer accounts, has just recently introduced their own mobile banking and payment platform in February 2014 (Holley, 2014). Bangkok Bank platform has enabled customers to check balances, transfer funds, top up prepaid accounts, and pay bills. Thailand is in the process of providing more

www.elsevierdirect.com

access to digital financial services. However, this may be hindered by its large investment in legacy assets.

Indonesia

The "National Strategy for Financial Inclusion: fostering economic growth and accelerating Poverty Reduction" policy introduced in 2012 provided tremendous momentum in developing digital financial inclusion in Indonesia. Indonesia has seen interoperability amongst three biggest MNOs (Telkomsel, Indosat, XL Com) and the largest bank in the country by assets (PT Bank Mandiri Tbk) to deliver government subsidies of around 15.5 million poor households since November 2014 (TNP2K, 2014). Poor families received SIM cards with electronic money for the Family Welfare Deposit Program, Smart Indonesia Cards (KIP) for KIP beneficiaries, and Healthy Indonesia Cards (KIS) for KIS beneficiaries. The electronic money accounts are linked to bank accounts at PT Bank Mandiri Tbk and can be withdrawn at the Post Office branches, mobile agents, and ATMs. Overall, however, Indonesia provides adequate connectivity, but provision of digital financial services is still in its early stage.

Philippines

Philippines was an early adopter of mobile technology to deliver financial services to the unbanked. The Bangko Sentral Ng Pilipinas (BSP), the central bank in Philippines, is recognized as the first central bank in the world to open an office, the Inclusive Finance Advocacy Staff, dedicated to financial inclusion in 2007 (UNCTAD, 2014). Consequently, Philippines was ranked the first among the SEAs countries and the third in the world in terms of regulatory openness for financial inclusion according to the EIU's global microscope on the microfinance environment in 2014.

The percentage of adults with e-money account is a high 26.7%, relative to the percentage of people with bank account, at around 31% at the end 2013 (BSP, 2013). The two most prominent initiatives to support digital financial inclusion in Philippines are Smart's "Smart Money," launched in 2001, and Globe'Gcash, launched in 2004. Smart Communication, a subsidiary of PLDT, Philippines' largest MNO launched "Smart Money" in partnership with Banco de Oro, Philippine's largest bank. The service allows customers to buy airtime, send and receive money domestically and internationally via mobile, and pay for goods using cards. Globe Telecom, the second largest MNO in Philippines, launched "Gcash," an SMS-based service, that offers a similar menu of services as "Smart Money" entirely via the mobile phone. Philippines has the conditions that support the suggestion that mobile technology can deliver universal financial inclusion.

Philippines has the largest diaspora globally. Thus, it has a strong demand for remittance services and a very supportive regulatory framework for financial inclusion. These factors have

resulted in an early start in providing digital financial services. Bank account penetration rate in Philippines, however, stands at a low 31% and grew at a slow 6% during the period 2011–2014. The Philippines demonstrate the difficulties of moving up the stage from connectivity to providing financial services to support economic activity and needs.

Cambodia

As the country with the highest mobile account penetration rate among SEA nations, it is interesting to note that mobile financial inclusion in Cambodia revolves around a third party payment provider, Wing. Founded in 2009, Wing allows customers to carryout domestic money transfer, bill payments, and airtime top-up. The company works with 1800 agents and has about 1 million users (CGAP, Duflos, 2014). The company grew its revenue from $65 million in 2011 to $1.5 billion in 2013 when it offered a simple over-the-counter (OTC) transaction in 2012 to overcome its inability to process the Khmer language. However, Wing still stores customers' fund in a regulated bank. The company is helping Cambodia to achieve the first stage of digital financial inclusion, namely: the payment stage. Cambodia banks are playing catch-up in the mobile trend when ACLEDA Bank, the bank that has the largest customer base, launched its first mobile banking product in early 2013.

Myanmar

Myanmar is projected to move quickly to provide mobile financial inclusion. Myanmar has low banking account penetration, but low banking legacy asset. As of 2013, Myanmar has a relatively low mobile phone penetration rate of just about 10% of the population. The central bank of Myanmar has been developing a regulatory framework with supportive regulations to foster greater financial inclusion via mobile bank since the country started in reforming its economy in 2011 (Central Bank of Myanmar, 2013). Beside the incumbent Myanmar Posts and Telecommunication, two international MNOs, Ooredoo and Telenor, were launched in August and October 2014 respectively, with the objective to provide mobile services to 80–90% of the population within four years. Ooredoo added over 1 million subscribers in the first three weeks of operation while Telenor has added more than 2 million subscribers (Shrader and Htun, 2015). Both MNOs have committed to develop mobile financial services. While Telenor launched domestic money transfer services since mid-2015, Ooredoo's mobile money platform piloted its payment services in 2015, with development on platform started in 2012 (Mondato, 2014).

The banking sector is embracing mobile technology in partnership with the MNOs. CBbank's has introduced its mobile application to customers. Third party payment service providers have emerged including *"Myanmar Mobile Money"* and *"myKyat"* that can be used by customers of any mobile network via either smart phones or cheaper phones with minimal features. Myanmar is moving into 1 Stage phase, after years in isolation.

www.elsevierdirect.com

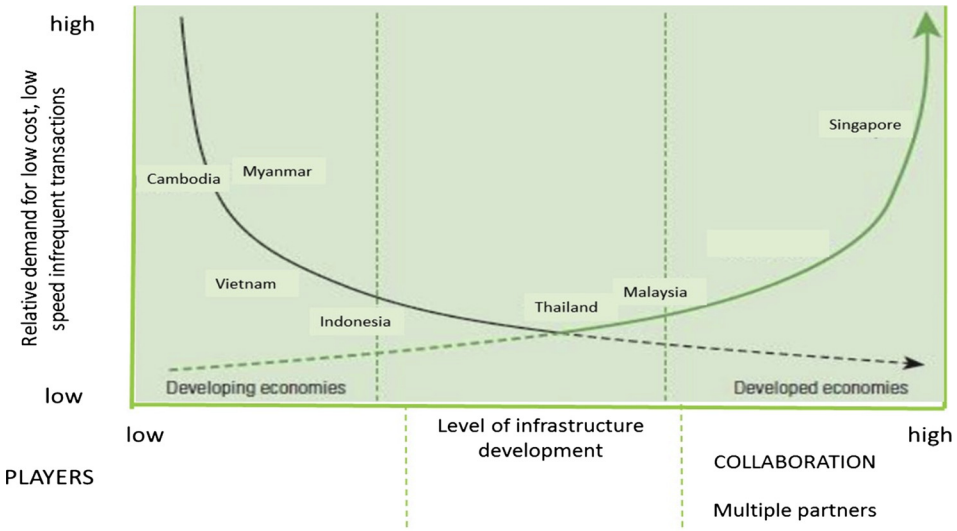


Figure 15.6: Level of infrastructure development in developing and developed SEA nations.
(Source: Adapted from World Bank, 2012, p. 67)

The main initiators of the core connectivity technology are believed to be dependent on the stage of the nation economy (World Bank, 2012). People from the nascent developing economies are likely to shift into digital financial inclusion services provided by mobile network operators (MNOs) as a result of the low level of banking infrastructure development and relatively low-speed and infrequent transactions demand. In other later stage developing countries, with a higher speed and frequency of transaction demand, along with more established banking sectors, the banking sector would lead initiatives in digital financial inclusion. In developed countries, with their developed ecosystems of banking, telecommunication, and retail sectors, would experience more varied initiatives supported by increased collaboration within the different industry players.

An illustration of the factors in developing digital financial infrastructure is shown in Fig. 15.6 above.

Beside customers penetration rate, infrastructure, and technological choices, *regulatory openness for digital financial inclusion* is another important supportive factor. The Economist Intelligence Unit has assessed regulatory environments that enabled digital financial inclusion across 55 countries using 12 indicators (EIU, 2014). These indicators include:

(1) government support;
(2) regulatory and supervisory capacity;
(3) prudential regulation;

(4) regulation and supervision of credit portfolios;
(5) regulation and supervision of credit-taking activities;
(6) regulation of insurance policy targeting low-income population;
(7) regulation and supervision of branches and agents;
(8) requirements for non-regulated lenders;
(9) regulation of electronic payments;
(10) credit-reporting systems;
(11) market-conduct rules; and
(12) grievance redress and operation of dispute-resolution mechanisms.

The standing of the various South-East Asian countries ranked by their relative regulatory openness and support are: Philippines, Cambodia, Indonesia, Thailand, and Vietnam respectively (Singapore, Malaysia, and Myanmar were not included in the survey).

Analysis of these factors and the publicized initiatives in the various countries leads us to conclude that digital financial inclusion in Cambodia will likely be driven by MNOs. Cambodia is also the SEA nation country that will leapfrog to a full service digital model (Stage 3 as discussed in Section 15.2.2). Given its limited banking infrastructure, low banking penetration rate, and strong support for microfinance institutions, we also expect that Myanmar can develop a full financial services model using the mobile technology (Duflos, 2013). Most of the other SEA nations are more likely to develop mobile banking services for the unbanked through partnerships between the banking and MNOs sectors.

15.4 Analysis and Discussion

It is widely recognized that the unbanked face three key challenges due to their reliance on cash: storage risk, transportation cost, and psychological barriers to "saving" (Radcliffe and Voorhies, 2012). The key arguments supporting digital financial inclusion on the ground of welfare benefits are access to store-of-value accounts, connection to peers and institutions, and access to enhanced financial services. While the first two benefits can arguably be supported based on usage and access, there is no clear evidence of welfare benefits from access to enhanced financial services.

However, real benefits from digital financial inclusion may be available beyond payment, savings, and micro-credit. There is a large number of the adult population in several SEA nations with significant difficulties in raising emergency funds. Digital financial inclusion can potentially provide suitable products to assist when other social support arrangements are not available.

www.elsevierdirect.com

Furthermore, an intangible social benefit may well come about from the availability of "access to cash" in itself. Once the unbanked have better financial access they may be better motivated about their future and strive harder to improve their lot.

A related issue is the role of digital money. Once the MNOs or any institutions with the network capabilities can issue money in the form of short-term debt, they can technically perform the role of banks. Nineteenth century America was an era in which the banks could issue money on its own with the backing of real and financial asset. Not until 1914 did the Federal Reserve System emerge in the United States to become a model for other countries' banking system, in which currency issuance power rests in the central government (Gorton, 2012). Going forward, digital banking may lead to a new financial system in which low risk-taking activities such as payment processes, deposits, and short-term credit run separately from the more risk-taking activities of large commercial banks. Block chain technology and universal ledger accounts can make this decentralized system feasible.

However, in the meanwhile, the World Bank (2016) remains concerned that many are still left out because they do not have access to digital technologies. Many nations still lack the infrastructure, experience poor business climate along with weak and ineffective regulations and poor governance that need to be overcome, for digital financial inclusion to be universal.

References

Bank Negara Malaysia, 2013. Bank Negara Malaysia. (2013, March 8) Retrieved May 11, 2015, from http://www.bnm.gov.my/index.php?ch=ps_mps&pg=ps_mps_type.

Bill & Melinda Gates Foundation, 2015. 2015 Gates Annual Letter: Our Big Bets for the Future. Bill & Melinda Gates Foundation, Seattle.

BSP, 2013. Report on the State of Financial Inclusion in the Philippines. BSP, Manila.

Central Bank of Myanmar, 2013. Current situation and policies in Myanmar on financial inclusion. Batam Island, Indonesia (2013, June 11).

Demirguc-Kunt, A., Klapper, L., 2012. Measuring Financial Inclusion: The Global Findex Database. The World Bank, Washington, DC.

Demirguc-Kunt, A., Klapper, L., Singer, D., Oudheusden, P.V., 2015. The Global Findex Database 2014: Measuring Financial Inclusion Around the World. World Bank Group, Washington, DC.

Duflos, E., 2013. CGAP. (2013, December 23) Retrieved May 11, 2015, from http://www.cgap.org/blog/financial-inclusion-myanmar-10-things-you-should-know.

Duflos, E., 2014. CGAP. (2014, July 24) Retrieved May 12, 2015, from http://www.cgap.org/blog/financial-inclusion-cambodia-trending-digital.

EIU, 2014. Global Microscope 2014: the enabling environment for financial inclusion. The Economist.

Gadanecz, B., Tissot, B., 2015. Key Messages of the Sasana Workshop on Financial Inclusion Indicators—Promoting Financial Inclusion Through Better Data. IFC Bulletin, Washington, DC.

Gorton, G.B., 2012. Misunderstanding Financial Crisis: Why We Don't See They Coming. Oxford University Pres, New York.

Holley, E., 2014. Banking Technology. (2014, February 10) Retrieved May 12, 2015, from http://www.bankingtech.com/201771/bangkok-bank-invests-in-mobile-banking-and-payments/.

IFC, 2011. IFC Mobile Money Study 2011: Thailand. IFC, Washington.
KPMG, 2013. The Banking and Financial Services Sector in Myanmar. Yangon.
Mondato, 2014. Mondato. (2014, August 27) Retrieved May 12, 2015, from http://mondato.com/blog/myanmar/.
Nielsen, K.B., 2014. CCGAP. Retrieved 4 9, 2015, from http://www.cgap.org/blog/10-useful-data-sources-measuring-financial-inclusion.
Owens, J., 2013. Offering digital financial services to promote financial inclusion: lesson we 've learned. Innovation, 279–290.
Radcliffe, D., Voorhies, R., 2012. Digital Pathway to Financial Inclusion. Bill & Melinda Gates Foundation.
Shrader, L., Htun, P., 2015. CGAP. (2015, January 22) Retrieved May 12, 2015, from http://www.cgap.org/blog/setting-stage-mobile-money-myanmar.
Singtel, 2014. Singtel. (2014, June 3) Retrieved May 11, 2015, from http://info.singtel.com/node/13438.
TNP2K, 2014. TNP2K: the national team for the acceleration of poverty reduction. (2014, November 4) Retrieved May 11, 2015, from www.tnp2k.go.id/en/artikel/government-launches-family-welfare-deposit-kip82038203-and-kis-programmes-in-stages/.
UNCTAD, 2014. Policies and regulation for financial inclusion: Philippine experience. In: Expert Meeting on: the Impact of Access to Financial Services, Including by Highlighting the Impact on Remittances on Development: Economic Empowerment of Woman and Youth. UNCTAD, pp. 1–7.
USAID, 2013. Innovations in Expanding Access to Microfinance: Microenterprise Access to Banking Services Program Phase 4 Final Report. USAID, Washington, DC.
World Bank, 2012. Maximizing Mobile: Report on Information and Communication. World Bank, Washington, DC.
World Bank, 2016. World Development Report 2016: Digital Dividends. World Bank, Washington, DC. License: Creative Commons Attribution CC BY 3.0 IGO.

www.elsevierdirect.com

CHAPTER 16

From the Ground Up: The Financial Inclusion Frontier

Griffin Hotchkiss, David LEE Kuo Chuen

Contents

16.1 Introduction 405

16.2 Past: 1987–2011 407

16.2.1 Burma Before Myanmar: 1988–2011 408

16.2.2 Finance Without Fintech: Banking Under Dictatorship 409

16.2.3 Outside the Grasp of Government: Microfinance 1990–2011 413

16.3 Present: 2011–2016 414

16.3.1 A Second Chance: Banking in Present-Day Myanmar 415

16.3.2 0 to 60 in 3.5 Years: The Connectivity Revolution 416

16.3.3 The Unbanked in Myanmar 417

16.3.4 Mobile Money: Wave Money and the Key Competencies 418

16.4 Future: Beyond 2016 420

16.4.1 Fostering Innovation in Myanmar 420

16.4.2 Final Thoughts on Innovative Digital Leapfrogging 422

Appendix: Myanmar and ASEAN 424

References 428

Notes 428

16.1 Introduction

The concept of financial inclusion has become an essential component in mainstream economic thought on development. Financial inclusion is a global initiative, not bound to any

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00016-4
Copyright © 2018 Elsevier Inc. All rights reserved.

country or people. But this chapter will make a case that right now in Myanmar there is a rare and unique opportunity for financial inclusion efforts.

Emerging from decades of isolation and military rule, Myanmar is in some sense a time capsule that has just been opened. Foundational systems of infrastructure, technology, and government simply have not changed since the country closed itself off in the 1960s. Political turmoil and economic hardship have been a constant characteristic of Burmese society since then. But over the past five years, an amazing shift has begun to take place. Starting with a few releases of political prisoners in 2011 and culminating in the first peaceful democratic elections in half a century in 2015, Myanmar has adopted a sudden and dramatic embrace of the outside world.

As the powers-that-be have unclenched their fist to embrace the invisible hand and to rejoin regional and global markets of trade, the world at large has likewise turned to focus on the amazing possibilities of this final frontier market in Asia. With nowhere to go but up, Myanmar has attracted considerable attention if not direct investment from foreign countries and multinational corporations. Estimates now put Myanmar's economic growth around 8.4%; more than any other country in all of Asia.[1]

In the development 'gold rush' atmosphere of modern day Myanmar, there has been a lot of thought given to the concept of 'digital leapfrogging.' The idea is compelling: Myanmar, as a late bloomer, gets to not only learn from the steps and missteps of similar countries that have before attempted a similar liberalization, but also gets to benefit from the significant technological gains that have occurred since those countries were beginning to liberalize. More importantly, hard infrastructure entails huge expenditure that is beyond a country with only USD8b foreign reserves. Connectivity inclusion by other means in a huge and sparsely populated agriculture may call for a different approach altogether without resorting to building roads, bridges, and utilities – the traditional way. Leapfrogging is possible only because it enabled by technology such as Wi-Fi, whitespace, drones, LiFi and other scalable technologies at a fraction of the cost of the old approaches building hard infrastructure.

Digital leapfrogging is a bit of a jargon term, because it can refer to different kinds of innovations. A straightforward example has happened already in the telecom sector: Ooredoo, one of the first private telecom firms granted a license in 2013, famously decided to adopt a '3G/4G only' strategy in infrastructure development, skipping all legacy technologies in its network rollout. Leapfrogging might, however, come in less obvious forms; for example many shop owners in the city have chosen to expand their business by opening a Facebook page for selling rather than opening a new stall. These kinds of smaller 'leapfrog' events are perhaps more interesting and exciting than the former example, but both are deeply intertwined with the singularly transformative power of the Internet and scalable technology.

In the context of banking and finance, the broad and optimistic promise of digital leapfrogging and financial inclusion will undoubtedly be intertwined with the Internet as well. These possibilities will be the focus of this chapter. But to clearly imagine what is possible in the future, we must examine the reality of Myanmar today – and before that it is necessary to take a quick look at the past, and just how much has been, until surprisingly recently, impossible.

The chapter is divided into three sections roughly corresponding to Past, Present, and Future financial inclusion in Burma/Myanmar. The first section presents a dark time in the country's history, from the years 1987 to 2011, when the country's nascent democracy movement was brutally crushed and nearly extinguished. The second examines the dramatic changes that have happened in the past five years which seem to suggest that Myanmar is moving on an optimistic trajectory, particularly in the context of telecommunications and the Internet. Finally, the last section is a more speculative look at what opportunities lie ahead, with some broad hopes and recommendations for regulators, foreign companies, and entrepreneurs.

Insofar as the sections are chronological, the later sections might draw upon some of the context that is presented in earlier sections, but wherever possible each section should be intelligible on its own.

16.2 Past: 1987–2011

A note for the reader: While the focus of this chapter is decidedly an economic one, it is very important to view the economy and financial systems within the context of the complicated political situation, both historically and now. The history of any country deserves more depth than can be expressed in just a few pages. Burma/Myanmar is no exception, and indeed likely deserves more careful attention than many other examples. This section will undoubtedly leave readers interested in Burma/Myanmar's rich, complex, and sometimes tragic modern history with many unanswered questions. The authors encourage those readers to consult the bibliography for further reading. What is presented here is considered the "crash course" in Myanmar's development as it relates to banking and financial inclusion.

A second note on names and spellings: Confusion over the proper and acceptable names for Burma/Myanmar is unavoidable. In very short summary, the name 'Burma' and the name 'Myanmar' both have the same meaning in the Burmese language; both names have been used interchangeably throughout history, with Burma being the more colloquial name and Myanmar a more formal designation. The confusion and controversy comes from the official renaming of the country and many cities in 1989. As we will see shortly, there was good reason for many to resist legitimizing the authority of those who initiated the name change, so

the continued use of the names 'Burma' and 'Rangoon' sometimes (but not always) carries a political statement. Western countries, particularly the U.K. and U.S., continue to use the old names, as do many (historically oppositionist) groups within the country and in exile. The authors intend to make no political insinuations; the year of 1997 is chosen as a date for sufficient recognition of 'Myanmar' as a legitimate name, as that is when the country was accepted into the Association of Southeast Asian Nations (ASEAN). The name used will always be in accordance with that event, i.e. any reference to the country as it existed before 1997 will use 'Burma' and any reference to the country after 1997 will use 'Myanmar'. Similar treatment to 'Yangon' and 'Rangoon' is given.

16.2.1 Burma Before Myanmar: 1988–2011

In September 1987, the architect of the "Burmese way to Socialism" General Ne Win decided that the existing notes of Burmese currency were unacceptable in the existing denominations of twenty-five, thirty-five, and seventy-five *kyats*. By his order, new banknotes of forty-five and ninety *kyats* were printed and declared the only legal tender. Ne Win's motivations will remain always a mystery. The new denominations were, according to Ne Win's astrologer, 'auspicious'; 45 and 90 are both divisible by nine, and their numerals add to nine.[2] Burmese who were using the kyat to keep their savings suddenly had wads of worthless paper in their wallets, cash registers, and homes.

The announcement caused riots at several universities, where students who had kept their savings for tuition were suddenly and unexpectedly broke. Unrest continued to grow in the following year, culminating in the 8888 uprising, a national student-led movement that eventually became the National League for Democracy, modern Myanmar's ruling political party. On August 8, 1988, millions of protesters nationwide were out in the streets flying the flag of the All Burma Students Union (now used by the NLD). 10,000 protesters demonstrated outside the Sule Pagoda in Rangoon, where demonstrators burned and buried effigies of Ne Win in coffins decorated with demonetized bank notes.[3] It was during this time that Nobel Laureate Aung San Suu Kyi first appeared in the political arena, delivering a speech to half a million protesters at the Shwedagon Pagoda in Rangoon, and becoming an icon for Democracy to both the people of Burma and to the outside world.

The protesters were met with brutality and bloodshed. The military abolished the 1974 constitution and formed the Orwellian *State Law and Order Restoration Council* (*SLORC*); martial law was declared. It is estimated that within the first week of securing power, 1000 students, monks, and schoolchildren were killed, and another 500 were killed whilst protesting outside the United States embassy.[4] The national Democracy movement was brutally crushed over the subsequent months. By the end of the year, some sources estimate 10,000 individuals were killed or went missing.[5]

www.elsevierdirect.com

SLORC's brutal crackdown on the 8888 Uprising is not the only or even the most lasting legacy in this dark period of Burma's history. Soon after, SLORC began implementing several fundamental changes to Burmese society, starting with the repeal of the 1965 *Law of Establishment of the Socialist Economic System*. SLORC's new objectives were then clearly outlined (daily) on the front page of *The New Light of Myanmar*:

1. *Development of agriculture as the base and all-round development of other sectors of the economy;*
2. *Proper evolution of the market-oriented economic system;*
3. *Development of the economy inviting participation of technical know-how and investments from sources inside the country and abroad;*
4. *The initiative to shape the national economy must be kept in the hands of the state and the national people*.[6]

Over the next decade, SLORC set in motion a plan that sought to build, from nothing, a modern free-market economy. As expected, "the reforms set in place by SLORC did not bring about the creation in Burma of the fundamental institutions necessary for a functioning market economy."[7]

Superficially, the most obvious changes were in name only, when *The Republic of the Union of Burma* became *The Republic of the Union of Myanmar*; and the city which had been called *Rangoon* for more than a century, became *Yangon*.

16.2.2 Finance Without Fintech: Banking Under Dictatorship

In Yangon, today, ATMs and several banks are apparently running brisk business. Savings/cheque account that comes with a debit card and an impressive interest rate of 8% or more are easily available. A couple of years ago, every transaction was in cash and a far cry from the fractional reserve system that the outside world was familiar with. It is astounding given how recently the formal banking system came to exist at all, and how close it came to total collapse just a decade ago.

The banks in Myanmar were rocked by a catastrophic financial crisis in early 2003, which culminated in a near total shutdown of financial services. Perhaps the most surprising aspect of the banking industry's recovery since that time is how little the core regulations have adapted and evolved. Of course, there are a few major improvements and liberalizations which have added a degree of stability to the financial sector, but we can still learn a lot by examining the banking sector since its (re)genesis in 1990.

www.elsevierdirect.com

In July 1990, SLORC passed *the Financial Institutions of Myanmar Law* (*FIML*), which both established the *Central Bank of Myanmar* (*CBM*) and permitted the formation of private banks. Between the years of 1992 and 1997, twenty banks were established and began operating.

While in principle good for Burma's economic prospects, the nascent private banking sector suffered from a systemic problem that has characterized Burma's laws since independence: That which is written is not necessarily instantiated in the actions of institutions or the real world. In other words, the laws looked good on paper, but reality did not reflect the law:

> *With respect to the role of the CBML in fostering macroeconomic stability in Burma, it is worthy of note that the CBM was given great formal powers. Articles 75 and 76 gave the CBM most of the requisite 'toolbox' of monetary instruments necessary for the successful application of monetary policy, including the ability to set the 'discount rate' on government securities, the powers to conduct open market operations in government securities and foreign exchange (buying and selling these to influence financial asset prices), determining the exchange rate of the currency, and being the government's principal adviser on monetary policy – while 'assisting' the same with respect to the state budget. In practice however, most of the formal monetary instruments and powers held by the CBM were rendered ineffective by Burma's underdeveloped financial system (which made irrelevant much of the toolbox above), and by the CBM's overriding role as the 'financing arm' of the state. The latter was especially critical, and more or less entirely negated the ability of the CBM in controlling inflation.*
>
> ***Turnell (2009). Fiery Dragons: Banks, Moneylenders and Microfinance in Burma***

The CBM's most glaring failure as an institution was its total inability to control and manage the country's monetary system. One can see this failure quite obviously in the 'black market' exchange rate throughout the last few decades:

Year	Official exchange rate (Kyat/USD)	Unofficial exchange rate (Kyat/USD)
1988	6.4	30
1991	6.0	60
1994	5.1	120
1997	6.4	240
2000	6.5	500
2003	6.5	1100

Source: Turnell (2009)

In passing the *Central Bank of Myanmar Law*, Burma adapted the template of the Basel Capital Accord, and set forth new banking regulations that for the most part were perfectly reasonable and prudent. In a few peculiar cases, however, regulations were severely limiting. Among the most controversial of these was a requirement that established the rates of interest that all private banks offer on deposits and charge on loans. No bank was allowed to pay interest on deposits at a rate less than 3 percent of the Central bank rate, while maximum interest collected on loans could not exceed 6 percent of the Central bank rate. This requirement is still in place today.

Nevertheless, the group of twenty private banks that opened in the 90s enjoyed amazing growth by the metrics normally used to assess banking performance. Adjusting for inflation, deposits and loans to private entities increased by 2100 and 1600 percent, respectively.[8] But under the surface, the newly formed private banking sector was not the bright healthy market-oriented system it pretended to be.

Although growing at phenomenal rates, even by 2002 the private banks were remarkably primitive, and despite seemingly impressive loan numbers, the truth was that access to financial services for a normal, 'unconnected' individuals or business remained rare and difficult. Most banks, in an effort to circumvent the laws capping interest rates, would build into their loans substantial 'establishment fees' or else just request outright bribes to secure a loan. The fees and bribes may have been 'under the table' in that they did not leave much of a paper trail, but most were accepted with the full knowledge of bank management at all levels. All banks also adopted a policy of loan collateralization. A borrower, in order to receive a bank loan, was required to provide a fixed asset worth about 200 percent the value of the loan – something far beyond the capability of all but the rich and well-connected.

The effects of such a lending environment resulted in bank loans that were short-term, high-risk, and generally imprudent. It also incentivized and enabled the widespread use of *A-kyoe-saung lou-ngan*, or 'informal finance enterprises' in English, which were "at best a function of highly speculative investments in real estate, construction and commodity trading, at worst [...] little more than gambling syndicates and Ponzi schemes."[9]

The final factor that contributed to a perfect storm in Burma's new market-oriented banking economy was the almost certain association that many of the major private banks had in money laundering activities. Burma was and is one of the world's largest producers of opium, and perhaps unsurprisingly did not have any meaningful laws or regulations that monitored mitigated, or prevented laundering activities. In June 2001, the Financial Action Task Force on Money Laundering (FATF), declared Burma to be one of sixteen jurisdictions it deemed to be 'non-cooperative'.[10] Facing pressures from FATF, the US Treasury, and others, the government created the *Law to Control Money and Property Obtained by Illegal Means* in

mid-2002. The law immediately caused a minor panic among some of the 'sensitive' depositors, enough to prompt the government to make an official announcement that banks should 'not feel threatened by the new law.'[11]

The apogee of the new 'market-oriented' financial institutions finally reached a negative inflection point in early 2003 after the sudden collapse of the informal finance enterprises. Their inevitable demise triggered a spillover to the largest and most prominent private bank, the Asia Wealth Bank, which was linked to the crash apparently by rumor alone. What followed is a classic example of a bank run. Depositors started withdrawing funds, which caused a further loss in confidence as well as several uncoordinated *ad hoc* measures by the banks to control their accounts. The panic and flight to cash continued, and with the blessing of the CBM – which should have instead been providing liquidity support – a system-wide ban on withdrawals over 500,000 kyats per customer per week was imposed. Unsurprisingly, this further eroded trust, and after just a few days 500,000 became 100,000 and then 50,000. Curiously, at the end of February, the CBM ordered all banks to halt transfer services, presumably to prevent customers from circumventing withdrawal limits.

The crisis worsened as the CBM decided to endorse private bank efforts to immediately recall loans. There is little concrete data on the damage that this caused, but reports and anecdotal evidence suggest that this did great harm. Businesses and homeowners with outstanding loans sold assets, downgraded lifestyles, and shuttered businesses. The result was a catastrophic devaluation of commodities, assets, and job loss.

> *In the final analysis, much of the blame for Burma's banking crisis in 2003 must be laid at the door of the CBM and, to the extent that it did not enjoy operational autonomy, Burma's governing institutions more broadly. The CBM did more than simply neglect its responsibilities. Throughout the crisis, it not only failed to respond to the growing crisis in the way that we have come to expect central banks can and should, but it actively encouraged reactions most likely to bring about systemic instability.*
>
> ***Turnell (2009). Fiery Dragons: Banks, Moneylenders and Microfinance in Burma***

Burma's financial system largely returned to cash and barter. Paradoxically, this caused the kyat to *strengthen* because demand for the currency was high as a medium of exchange (not a store of value, which was indisputably crisp, unblemished $100 bills). Deposits, loans, and transfers resumed after a time, but aside from the real damage done to businesses and Burmese society at large, the financial crisis cut a deep scar in the trust of the people. The banking system has continued to limp on, but the legacy of the crisis still casts a shadow on banking in modern Myanmar, where people are much more likely to conduct business in cash (transactions in kyat, savings in USD) than to use a formal banking account.

www.elsevierdirect.com

16.2.3 Outside the Grasp of Government: Microfinance 1990–2011

As explained in the previous section, access to credit was sorely lacking for a 'normal' citizen in Myanmar, despite encouraging metrics before the 2003 financial crisis, because the regulatory and legal framework of the banking system was flawed and unstable. For the very poor farmers of Burma/Myanmar, this institutional problem ran even deeper.

In the sectors that needed credit the most, such as agriculture and productive enterprises, the new private banks were in fact *forbidden to make loans*. The cause for this prohibition was ostensibly to give the state-reformed Myanmar Agricultural Development Bank unencumbered access to the whole agricultural lending market, but even in the best scenarios, MADB's agricultural loans were woefully undersized, covering only 9% of the estimated cost of production.[12] Financial services were effectively divorced from agriculture from either direct or indirect obstacles imposed by the banking system.

But already by the mid-90s, the concept of microfinance was becoming increasingly recognized as a powerful tool for alleviating poverty. Recognizing this, the United Nations Development Programme (UNDP), in collaboration with the United Nations Office for Project Services (UNOPS), launched the first initiatives at microfinance in certain regions of Burma, organized under the UNDP's 'Human Development Initiative.' This project, established in 1993, sought to implement basic development programs at the 'grass roots' level, and to avoid working through government authorities in Burma to the extent possible at that time.[13]

UNDP's microfinance operations were limited to three distinct regions chosen because they were the location of farmers, artisans, and traders proven to be the most effective beneficiaries of microfinance. The microfinance schemes covered only about 3.5% of the population of Burma, but were designed for 'national replicability' in the hope that a new rural finance system would be based on their model. The plan was to operate the microfinance schemes directly before transitioning to 'local' control; after some time, the UNDP selected three international NGOs to act as operators for the schemes, again under the hope that the NGOs might increase the degree of local control within operations and effectively become local organizations once a sufficient number of local staff were competent. This situation never materialized. In 2006, all three schemes were given to PACT Myanmar (Private Agencies Collaborating Together), which had been operating one of the schemes in the Dry Zone west of Mandalay.

Operating as a UNDP led 'project' (and later an independent NGO 'project') gave the microfinance schemes a degree of necessary freedom and shielding from the flawed framework that the 'real' financial institutions were operating within. The microfinance schemes were not subject to any of the troublesome regulations for banks, and indeed were free to be organized according to some of the important and effective models of microfinance that have been successful elsewhere. In fact, until the official microfinance law in 2011, microfinance was an

www.elsevierdirect.com

institutional 'no man's land,' where no law established roles, restrictions, or other such guidelines.

The first of the important freedoms that the schemes had was freedom to establish interest rates. Recall that the Central Bank of Myanmar Law (1990) imposed an interest rate cap of no more than 18 percent on all loans from private banks, which incentivized banks to focus loans on 'quick, easy money' such as speculative real-estate investment. By contrast, the microfinance schemes typically issued loans with average rates of around 38% interest. While this may seem quite high, it was still half of what might be charged by an 'informal' money lender for a similar loan. And, due to inflation being around 40% at the time, the loans were still potentially too low for sustainability.

The second important advantage microfinance had over bank loans was a lack of collateralization. Since the targeted borrowers almost universally had no significant assets, it made little sense to require something worth 200% the loan value as was the 'rule of thumb' practiced by banks. Instead, UNDP's microfinance used the proven effectiveness of group loan disbursements and the 'social collateral' effect that such group schemes relied on to enforce repayment. Additionally, the schemes employed the practice of 'progressive lending' whereby an individual's access to credit is dependent on the repayment performance of others in the group. These two strategies in tandem were extremely effective in enforcing and keeping incentives for loan repayment, and perhaps even had added positive externalities of broader social development for group members and the stimulation of 'mutual trust' and other social values.

Over the decade, the UNDP microfinance scheme issued collectively around 700,000 loans reaching nearly 180,000 individual borrowers, mostly women, with an average loan size of around 25,000 kyats ($20–40 by black market rate calculations). The scheme was able to maintain over 98% repayment across all operating regions.

The UNDP's official assessment of its own program declared it a success in 2005, stating that the schemes were 'making a significant contribution in promoting the income and savings of the poor.' It added that they had proved, in Myanmar, that the 'poor are bankable.'

16.3 Present: 2011–2016

On November 8, 2015, the red flags featuring the fighting peacock were again covering the streets of Yangon. This time, they were the symbol of the National League for Democracy, the opposition party that was formed from the ashes of the destroyed democracy movement nearly three decades earlier. The crowd that gathered outside the NLD office was not protesting, however, it was celebrating. That day, in one of the most astounding events to occur this

www.elsevierdirect.com

decade, the successful completion of the first credible elections since Ne Win's era. The NLD won a super-majority, and although the smooth transfer of power loomed ahead, the atmosphere was one of indescribable optimism. That day, the people had voted, and they felt good.

It remains a subject of disagreement as to why the quasi-civilian government, an incarnate of the SPDC, begun a series of surprising reforms in 2011. One possible explanation is that the unrest of the monk-led Saffron Revolution in 2007 had finally shaken the confidence of the ruling Junta, who deeply respected Buddhism as the national religion. Another quite different explanation is that the military had planned the transition to liberalized economy all along, and that it was finally coming about. A third is that opening up to western powers was a calculated risk to offset Beijing's ever-increasing influence on all industries in the isolated country. The results, however, have been indisputable: Myanmar's reforms have set off a cascade of changes that are affecting all aspects of society, and the economy booms.

There are still many deeply systemic problems in Myanmar that remain, and a long road ahead awaits both the newly elected government and all of Myanmar's people. Ethnic conflicts in many areas of Myanmar have raged on and off for the duration of independence, and there seem to be no indications that the tensions will ease any time soon. Separately from that, sectarian violence against the country's minority Muslim population, with particularly nasty results for a group of stateless individuals near the border with Bangladesh. Finally, there remain questions about how committed the military is to Democratic reform, as they still hold considerable power over all aspects of government.

16.3.1 A Second Chance: Banking in Present-Day Myanmar

It was not until 2013 that a new banking law was approved, which superseded the CMBL of 1990. This new set of reforms established an interbank market for foreign exchange, and allowed the CBM to be autonomous under the Ministry of Finance and Revenue. The new law also allotted new tools to manage interest rates and inflation.

The 14 privately owned banks that continue to operate now have permission to engage in international banking services, which has done wonders for their vitality. Permission to engage in foreign currency exchange (which formerly was only permitted for the CBM) has also given the financial institutions of Myanmar a much-needed burst of energy.

Faced with real competition, banks are now working hard to attract new depositors and borrowers, and to repair the deeply damaged public trust that has lingered from the previous decade.

"It is difficult to try to catch up by speed; we will catch up by innovation," says Serge Pun, chairman of SPA group, which controls Yoma bank, widely regarded as one of the more progressive banking institutions in Myanmar today.

www.elsevierdirect.com

It is, however, still difficult for banks to operate – and for similar reasons as the previous era: The troublesome limitations on loan terms and interest rates are still in place. Lending rates are capped at 13%, and deposits are required to pay 8%. Furthermore, banks are only allowed to lend 70–80% of deposits. Finally, the 'rule of thumb' of loan collateralization has more or less been established as the law.[14] However, a new Financial Institutions in Myanmar Law was drafted with help from the World Bank in 2013, and if passed, it would bring the banking sector up to par with international standards.[15]

16.3.2 0 to 60 in 3.5 Years: The Connectivity Revolution

There was a short time around 2013 when one could 'carbon date' a recently settled expatriate by asking them how much they paid for their SIM card. Depending on how long the person had been using the service, their answer would range from $1.30 (the current market price) to as much as $5000 (double a SIM card's original cost in 2009). That seemingly insane price was a reality under dominating state control: until 2013, *Myanmar Posts and Telecom* (*MPT*) was the state-owned monopoly telecom and thusly was able to exert an unthinkable amount of market control on their service. Because the elite were thought to be the only customers who needed or desired mobile telephony, the price for a data-enabled SIM was set to $2000 and linked to a citizen's ID. As is the case whenever there exists a mismatch between supply and demand, a black market will emerge. SIMs were sold for as high as $5000 USD before MPT reduced the official price to $150 and sold the new cheaper SIMs on a township-based lottery system. One of the authors purchased a SIM in March 2013 for about $130 from an enterprising mobile shop; it included a photo and full registration info of the original lottery winner "in case I need a replacement."

It's difficult to understate just how dramatic the last 3.5 years have been for telecommunications in Myanmar. In 2012 it was estimated that telephone penetration was somewhere between 2% and 7%, which put Myanmar slightly *below* North Korea on international rankings. In 2013, the government opened up a tender process for the first ever foreign-owned telecom companies to offer connectivity. In the end, two companies won tenders and begun an unprecedented deployment into what some considered to be the last major 'green field' market in the world. With unprecedented speed and audacious goals, Telenor (Norway), Ooredoo (Quatar), and MPT (in a joint venture with Japan's KDDI-Sumito) began to build a new country-wide system of infrastructure from basically nothing. Over the period of 2013–2015, the communications and transport sectors have attracted about 4.5 billion USD in direct investment.[16,17] In just 3.5 short years, even the more conservative estimates put telecom penetration at around 60% (the latest official number is 77.7%), making Myanmar's mobile service expansion one of the fastest in the world.

The most visible result of this proclaimed 'connectivity revolution' is in the hands of the people, literally: Smartphones. Myanmar is smartphone country; it's very difficult to pin down exact numbers, but something on the order of 60% of mobile phone subscribers use smartphones, and more than half of all subscribers use data at least once per month.[18] Even without the statistics, walk around any city in Myanmar and you'll see people of all ages and social status poking away at a smartphone of some kind. In Myanmar, it is astounding that many who live without running water or reliable electricity will still have access to Facebook. The vast majority of people in Myanmar who interact with the Internet for the first time will do so through a smartphone, and will almost certainly use Facebook for most of their time online.

"If you're not on Facebook, you're not Burmese," said Pyay Way, an art gallery owner who makes extensive use of the website to promote and publish his artist's work for both local and international buyers. It's true; Facebook is the Internet's 'killer app' in Myanmar, and it will come pre-installed on any phone you purchase from a mobile store. Because many new users don't know how to interact with the social network, many shops even sell phones with pre-made accounts, complete with a list of pre-made 'friends.'[19]

Challenges for last-mile access remain, however. While the new telecoms have delivered an unprecedented expansion of mobile network coverage in just three short years, there are still plenty of rural and remote areas in Myanmar that have little or no access to the Internet. For Myanmar to become the next financial inclusion frontier, the remaining gaps in coverage must be filled. Written into the telecom law is a provision for a Universal Access Fund (UAF) to expand coverage to those in areas which might be less attractive for mobile operator investment in infrastructure – but so far nothing has materialized. Making effective use of a UAF and expanding coverage all the way up to 100% is perhaps the greatest challenge for Myanmar in ushering a new era of innovation and innovative financial inclusion.

16.3.3 The Unbanked in Myanmar

As expected given the tumultuous history that the banking sector in Myanmar has seen, very few people in the country have access to or desire financial services. But who are these people, anyways? What sorts of financial services do they need, and how can technology be leveraged to provide them?

Not a lot was known about the 52 million people in Myanmar until the first nationwide census in over 20 years was conducted in 2014. In fact, until that date, it was thought that the population of Myanmar was 60 million!

When released, the census provided an invaluable snapshot of the country's people. Here are some fundamentals:

www.elsevierdirect.com

- Only 30% of Myanmar's 51.5 million people live in urban areas.
- Myanmar's median age is 27, comparable with Vietnam.
- 70% of the population still uses firewood as a main source of energy for cooking.
- 32% of households use electricity as their main source of lighting. Somewhere around 20% use batteries and cheap solar panels, and about the same number use candles.
- About 50% of all the working population in Myanmar are farmers.

These statistics may not paint a vivid picture for the reader of what life might look like in Myanmar for an average person. It is to some degree impossible to paint such a picture; every village faces its own unique situation with regards to resources, access to infrastructure, and simple geography. But the main takeaway is this: Myanmar is underdeveloped in most aspects of infrastructure, save one: telecommunications.

The first author recently had the opportunity to visit a small remote village for a friend's wedding. The village was a typical 200-home community of farmers in the dry zone near the city of Mandalay. Most houses were wooden or bamboo thatch, and nearly every home kept livestock of some kind. Electrical infrastructure was entirely absent; although villagers said that they hoped to be connected to the national grid within a year or so. For the lighting and musical entertainment of the wedding, $100 USD had been pooled to pay for a gasoline generator that powered lights and speakers. And yet, nearly all attendees brought their smartphones, and requested permission to take selfies with the foreign visitors. Without electricity or even running water, most of the villagers were quite comfortable with Facebook!

Myanmar's rural population faces all the challenges of development that every other rural population in Asia has faced throughout all time, but Myanmar may be the only country that can begin to tackle these challenges with the full power of Internet access, everywhere.

16.3.4 Mobile Money: Wave Money and the Key Competencies

It is on the foundations of this brand new, country-wide telecom network that new financial inclusion initiatives will be built, and the first of these efforts are already launching in the form of mobile money services.

The largest of these might be Wave Money, a joint venture between Norwegian telecom Telenor and Yoma bank. After months of marketing and pre-rollout preparation, Wave was granted a mobile money license on October 3rd.[20]

Compared to the competitors, Wave money seems unique in possessing the key competencies of mobile money service as identified by Lal and Sachdev,[21] which are as follows:

1. *Effective working relationship with regulators*.
   As one of the telecoms that won the first tender for a foreign operator in Myanmar, Telenor has advised the government and been given almost free reign with regards to their rollout in the last three years.
2. *Trust in service*.
   While it is likely that most people have ambivalent or negative opinions of banking institutions, the opposite is true for the telecoms. Having brought Internet service to most of the country where there had previously been none, the average person in Myanmar likely has a high opinion of Telenor and its affiliates.
3. *Safekeeping of customer funds*.
   Because Wave money has access to the systems and facilities of Yoma bank, customer funds are as safe as any Yoma bank account.
4. *Facilitating Cash-in/Cash-out*.
   This is one aspect that the partnership between Yoma Bank and Telenor stands out in. By leveraging the relationships with existing vendors of Telenor SIM cards as well as the banking services of Yoma bank branches, Wave money is in a unique position to have an effective network of cash-in/cash-out nodes throughout the country.
5. *Liquidity management*.
   Actual real-world performance remains to be seen, but the partnership with Yoma bank should bode well for Wave money agents and their ability to keep sufficient cash and e-float to meet the demands of their customers.
6. *Fraud mitigation*.
   Again, real-world performance cannot be commented on, but as large companies with a variety of existing anti-fraud systems in place and tremendously well-funded support systems, the outlook for Wave looks better than most companies.
7. *Effective agent networks, customer support, and ecosystem alignment*.
   Again, by drawing upon the relationships of both Yoma bank and Telenor, Wave money seems uniquely positioned for success on these competencies.
8. *Infrastructure for mobile money*.
   This is likely the greatest strength of the partnership between one of the country's largest banks and its second-largest telco: the system is uniquely aligned to the information infrastructure that Telenor has built in the last three years.

There very well may be a more successful mobile money initiative that can build these competencies without the direct access to the resources at Telenor/Yoma bank's disposal; but regardless of the company, these competencies are crucial for the success of mobile money in expanding access to financial services to Myanmar's population.

The reader may note that many of the competencies listed would be extremely difficult to attain for a mobile money service that did not have the backing of a large company or financial

www.elsevierdirect.com

institution. This is the key challenge for Myanmar's regulators and innovative companies and investors: Fostering an environment for small and medium-sized innovations that can effectively leverage the Internet as the primary tool for financial inclusion, and act in concert with the larger players like Wave.

16.4 Future: Beyond 2016

16.4.1 Fostering Innovation in Myanmar

To foster financial inclusion in Myanmar, an inclusive environment needs first to be fostered for the innovators themselves. The individuals or companies that dare to attempt new and novel approaches to financial inclusion will be the ones that define the space for the next era. To encourage this kind of experimentation it would be wise for the government and investors alike to seek policies and practices that can provide a degree of freedom for innovators to explore and test their ideas without the fear of being shut down or forced out by larger incumbent players.

In the early days of microfinance, the UNDP could make a meaningful impact primarily because their financial services were unconstrained by the prevailing laws. It is this kind of regulatory insulation that could stimulate new and innovative approaches to financial inclusion. This is not to say that sound, reasonable regulation should be avoided or flaunted. The suggestion is merely that in certain cases it can be beneficial to allow a company or technology to be tested in an insulated environment such as a Sandbox Regulatory Laboratory.

Myanmar is already quite supportive of such environments with its recent embrace of Special Economic Zones. Lowing trade tariffs, reducing frictions of registrations, and designating certain activities as 'free' within specific geographic constraints have been proven drivers of economic growth – the SEZs that exist in Myanmar today are aimed at fostering growth within the sectors of transport, trade, and manufacturing.

For financial inclusion, the concept of a shielded space for greater dividends could exist in a multitude of forms, but here are two ideas that might be interesting to try:

Village on the blockchain. Much like an SEZ, a designated 'blockchain village' would be an established township or village where experimental financial technology and financial services could operate without hindrance from regulations normally imposed on exchange, remittance, and other regulated activities. If implemented in the correct way, this might allow start-ups and other companies to work with the village community in testing their prototypes and refining them. The key consideration in such a scheme would be to ensure that companies were indeed working *with* the local population, instead of just testing their products and services *on* them.

There is some precedent for this kind of a system with the Myanmar government's apparent willingness to greenlight a few pilot projects for *Community-based Tourism* (*CBT*). In the CBT model, tour companies must work with villages and local guides to establish tour routes and activities that are still technically illegal under the national law. The model works particularly well in popular trekking destinations, where not one but several villages share revenue and responsibility as the tourists move along a pre-established route. The essential core of the CBT is its governance model: to avoid disputes and favoritism, each village in the area of deployment may opt-in by electing a representative to a governing board, which makes long-term financial and operational decisions on behalf of the community.

A 'village blockchain' pilot might employ the basic outline of the CBT model, by selecting a handful of towns along an established road, river, or village track. The democratically elected board would act as a sort of committee that exercises some degree of control over the technologies, companies, and research to be allowed within the zone. By placing control over the project with the local community, newcomers would then be incentivized to keep good relations with the members of that community, and to design products and solutions that prioritized, above all, local needs.

Independent Trust for Innovation. This is perhaps a more moderate suggestion, as it has an established and well-studied precedent in the form of FSD Kenya, an independent trust established in 2005 with the goal of improving financial inclusion efforts. FSD Kenya is at least partially responsible for the widespread success of M-PESA, although FSD itself suggests that it is not often credited for the role it played.[22] The main function and ability of FSD Kenya was as an *independent and neutral third party* working within the financial sector. This neutrality allowed FSD to make a significant impact on the sector by working with multiple (and sometimes competing) firms, with government, and with other stakeholders in the financial ecosystem.

The establishment of such an independent trust in Myanmar could potentially be quite helpful for banks, regulators, and entrepreneurs alike, as it would allow for collaboration and knowledge sharing in an environment that is becoming increasingly closed and competitive. It would also provide a single organization to take 'responsibility' for maintaining and keeping good public perceptions of often misunderstood technologies such as cryptocurrencies, offering legal and regulatory advice to smaller more resource-constrained firms like early stage start-ups.

With the sort of 'protection' that an independent trust could offer would come some degree of freedom to experiment and operate on the fringes of what might be, by the books, permitted. The fact is that the legal foundation for regulation of any kind is shaky at best in Myanmar, and when it comes to groundbreaking and unprecedented technologies, there is simply no

hope that laws will have been drafted to handle whatever frictions might arise between technology and government institution.

This, too, was articulated in FSD's ten-year self-assessment: "*Vodafone's pragmatic approach to regulation had always been not to seek permission, to ask CBK to say yes, but rather to invite CBK 'not to say no'*.[23] In other words, in the case of M-PESA and related fintech, it was better to ask for forgiveness than permission. This is the sort of approach that can only be taken by a company with a robust support system and deep expertise in business, legal and even political arbitration. Such a strategy would be simply impossible for a start-up or innovative SME without the support of something like an independent trust.

These two examples are of course highly speculative, but they share a few common elements that should be kept in consideration by anyone involved in investment or advisory in Myanmar:

- *It's important to allow experimentation*. It has been shown in many markets that when it comes to innovation and technology, a 'test and learn' approach is best. For financial inclusion efforts, this is paramount. Both from a regulatory perspective and an entrepreneurial one, the truly successful firms will engage with their customers, learn their needs, and develop products/services/laws accordingly, in that order.
- *Start-ups and SMEs are the key*. While in some aspects large and well-supported companies are the only ones that can deliver comprehensive services like mobile money, it is still crucial that smaller players be given a chance to innovate and explore new territory. There is little downside in allowing this to happen from both a regulatory perspective and a competitive one from larger firms. Regulation and new investment should favor the little guy!
- *People first*. This is perhaps the most important: Innovation and new products or services need to be developed with the target customer as the highest priority. Everybody deserves good design, but the poor can least afford bad design. All actors in the financial inclusion space should seek to prioritize community and engagement when developing their solutions.

16.4.2 Final Thoughts on Innovative Digital Leapfrogging

When talking about technology, it's very easy to pitch something as "The next Facebook/uber/airbnb." When a technologist or entrepreneur does this, the quality of that very successful, disruptive start-up that is referenced does not have much to do with the actual substance of said start-up's business. It almost always refers to the 'disruptive' or 'innovative' quality *itself*. To understand the context of a start-up like uber would require as much exploration into unions and labor laws in the United States as it would mobile apps and the sharing

economy. But nobody needs to understand those things to grasp uber's success. Rather, the point a technologist or entrepreneur is getting at when citing a company like uber or Facebook is the genuine *surprise* we feel when we contemplate the extent to which that innovation re-made the status quo.

It becomes almost inconceivable that before Internet banking, utility bills once had to be settled by standing in line at the township office, paying in cash at a little window, and waiting for someone to hand-copy your payment receipt into a large bound ledger.

Yet this is what everyone in Yangon must do later in the month. A copy of a printed meter bill for the whole block will be delivered to homes and apartments (in the first author's case, tucked under a small bit of wire tied to a cage in the stairwell). Later in the week, everyone will, between the hours of 9 and 4, make their way to the township electric power office, and, as described, wait in line to have a cash payment taken and recorded. If this is done before the 21st of the month, they will not have to pay a penalty fee or risk having an officer dispatched later in the week to physically cut the power line to their residence.

It seems easy to imagine this antiquated drudgery wiped away by Internet banking as it exists today. By comparison, an automatic bill-pay managed in a web browser on our home computer seems *revolutionary*. Indeed, to those that used the analog method the comparison evokes the exact emotion hinted at: Recognition that "this is innovation."

But there is a small misstep in thinking about this as a true innovation: when first adopted and implemented, Internet banking *was* revolutionary. Today, however, Internet banking is the status quo; it's only revolutionary *by comparison*. Bringing a full system of Internet banking to Myanmar would be revolutionary because the current system is antiquated. It would not be an example of *innovation* so much as an example of mere *deployment*. The same could be said for mobile money: Wave money is, at its core, just M-PESA transplanted from Kenya to Myanmar.

The false innovation misstep must be avoided when thinking about the future of financial inclusion in Myanmar.

The possibility that "true innovation" – the kind that causes the CEO of Barklays to proclaim "The universal banking model is dead"[24] – could arise and evolve in an urban fringe township of Yangon, or even a small village deep in the mountain range on the Indian border. A true innovation, in our electricity example, would rather be something like a blockchain-based power meter, that settled a meter bill instantly and continuously with a cryptocurrency such as Ether, Bitcoin, or Zcash.

Innovations from 'the fourth industrial revolution' have the potential to produce great value for a developing country such as Myanmar, where the primary activity is agriculture. New

www.elsevierdirect.com

innovations such as blockchain technology greatly reduce the cost of traditional banking infrastructure, while at the same time expanding access to anyone with a mobile phone and an internet connection. In some cases, a mobile phone and an internet connection may be the only technology that a farmer has!

Imagine, for a moment, the amazing potential of successful innovation in rural Myanmar: A farmer might receive regular crop and weather intelligence on his/her mobile phone, be able to apply for instant loans or micro-insurance depending on regional intelligence, and send/receive payments to distributors or family members instantly. Perhaps in the near future crucial goods may be delivered to more remote regions by drone, instead of taking days on poorly constructed roads. Livestock producers may be able to track and share assets by branding with a QR code and trading ownership with a fungible cryptocurrency backed by water buffalo!

Part of the fun of this kind of speculation is that it is boundless. We can't predict exactly what will happen if Myanmar can capture the power of true digital leapfrogging for development, but we can certainly say that if it does, it has the potential to improve the lives of millions (or even billions) if such innovations can be scaled regionally. Myanmar has not a lot to lose and much to gain by allowing a little bit of innovation experimentation, and hopefully there are willing entrepreneurs and inventors ready to rise to the challenge.

A nascent but promising technology, combined with some favorable confluence of political, economic, and sociological factors, a small unlikely group of exceptional people, and a dash of blessing, could yield something better than "the next M-PESA or Alipay." With the change in the political landscape, combined with the emerging scalable technology of the fourth industrial revolution, Myanmar is certainly ripe for a transformation that the world has been waiting for.

Appendix: Myanmar and ASEAN

To understand the fintech opportunities in Myanmar, we have produced and collated seven figures to show its linkages and positioning within ASEAN. ASEAN is pro-active in promoting both trade and payments among ten countries. Fig. 16.1 shows the geographical position of Myanmar within ASEAN. Fig. 16.2 demonstrates the growth potential of Myanmar within a community that has a combined GDP of USD2.4 t. Figs. 16.3–16.5 outline the initiatives within the ASEAN. Fig. 16.6 shows the potential of Fintech and inclusion within Myanmar as compared to the other eight countries. The last figure, Fig. 16.7 shows the projected growth of Myanmar for 2017 at 8.3%, the highest among the ten countries!



Figure 16.1: ASEAN 10.

Country	Total land area	Total population	Gross domestic product at current prices	Gross domestic product per capita at current prices	
	km^2	thousand	US$ million	US$	US$ PPP
	2013	**2013**	**2013**	**2013**	**2013**
Indonesia	1,860,360	248,818.1	860,849.5	3,459.8	9,467.1
Thailand	513,120	68,251.0	387,573.8	5,678.7	14,131.6
Malaysia	330,290	29,948.0	312,071.6	10,420.5	23,089.0
Singapore	716	5,399.2	297,941.3	55,182.5	78,761.9
Philippines	300,000	99,384.5	269,024.0	2,706.9	6,403.8
Viet Nam	330,951	89,708.9	171,219.3	1,908.6	5,314.7
Myanmar	676,577	61,568.0	54,661.2	887.8	3,464.4
Brunei Darussalam	5,769	406.2	16,117.5	39,678.7	73,775.0
Cambodia	181,035	14,962.6	15,511.1	1,036.7	3,081.8
Lao PDR	236,800	6,644.0	10,283.2	1,547.7	4,531.6
ASEAN	**4,435,618**	***625,090.5***	***2,395,252.5***	***3,831.8***	***9,389.8***

Note that Myanmar population may be less than reported here.

Source: ASEAN and various agencies

Figure 16.2: Myanmar GDP/capital was the smallest in ASEAN in 2013.

www.elsevierdirect.com

- The ASEAN Economic Community is the goal of regional economic integration by 2015. Its characteristics include:
  - a single market and production base
  - a highly competitive economic region
  - a region of fair economic development
  - a region fully integrated into the global economy.
- The areas of co-operation include human resources development; recognition of professional qualifications; closer consultation on macroeconomic and financial policies; trade financing measures; enhanced infrastructure and communications connectivity; development of electronic transactions through e-ASEAN; integrating industries across the region to promote regional sourcing; and enhancing private sector involvement.

Source: ASEAN and various agencies

Figure 16.3: Myanmar is a party to AEC 2015.

- Finance and monetary integration, namely
  - capital market development
  - capital account liberalisation
  - financial services liberalisation
  - ASEAN currency co-operation
- Capital market development entails promoting institutional capacity, including the legal and regulatory framework, as well as the facilitation of greater cross-border collaboration, linkages and harmonisation between capital markets in the region.
- Orderly capital account liberalisation will be promoted with adequate safeguards against volatility and systemic risks.
- Currency co-operation would involve exploration of possible currency arrangements, including an ASEAN currency payment system for trade in local goods to reduce the demand for US dollars and help promote stability of regional currencies, such as by settling intra-ASEAN trade using regional currencies

Source: ASEAN and various agencies

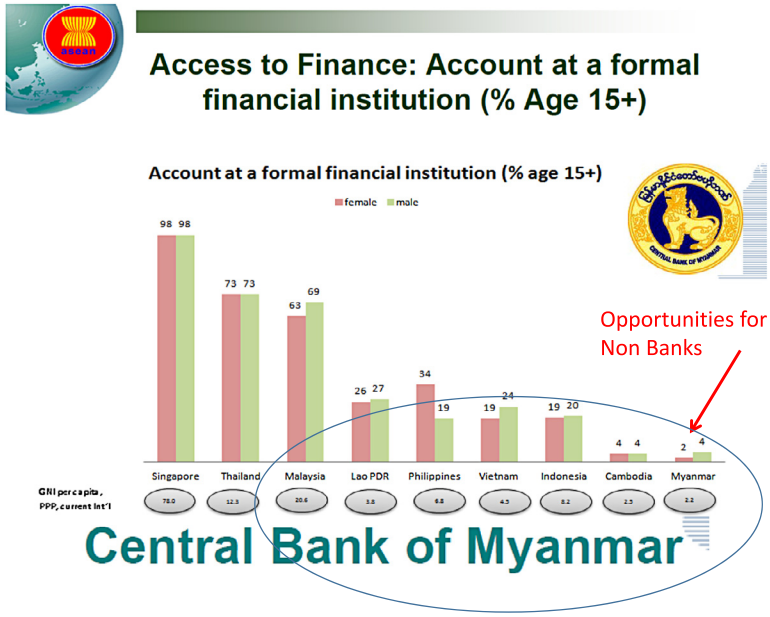
Figure 16.4: Opportunities in FinTech in ASEAN and Myanmar!

- As the flow of goods, services, investment, capital and skilled labour between countries are liberalised with the ASEAN Economic Integration in 2015, the need arises for ASEAN banking institutions to accommodate and expand its services to a greater intra-ASEAN market.
- Non-Banking Institutions my be provided with banking services

Source: ASEAN and various agencies

Figure 16.5: 2020 ASEAN banking integration framework (ABIF) is positive for Myanmar.

www.elsevierdirect.com



Source: ASEAN and Central Bank of Myanmar, 2015

Figure 16.6: Myanmar has the lowest access to finance.

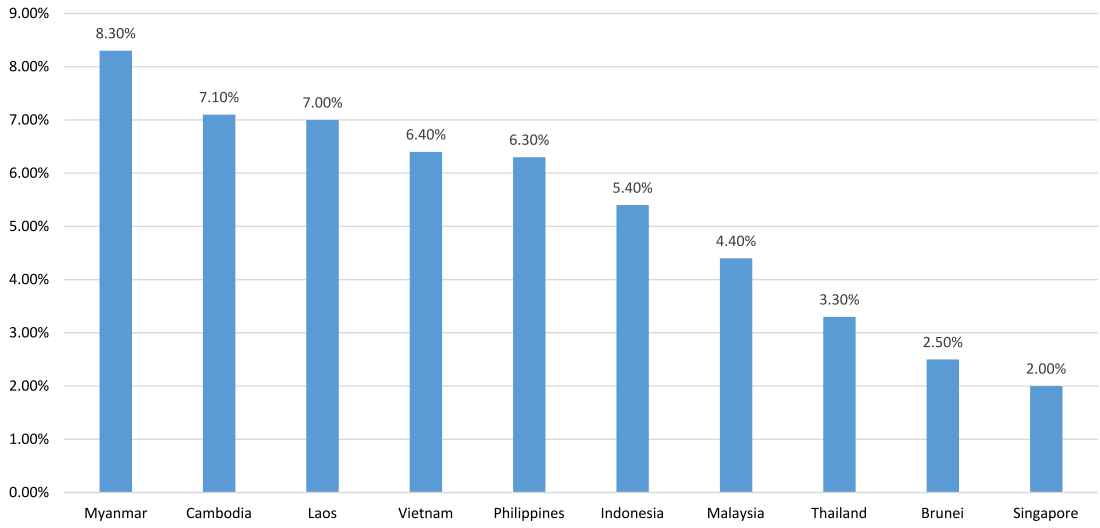


Figure 16.7: Projected 2017 GDP growth by ADB.

www.elsevierdirect.com

References

Anon, 2016. Wave Money Receives Mobile Financial Service License From Central Bank. The Irrawaddy. Available at: http://www.irrawaddy.com/business/wave-money-receives-mobile-financial-service-license-from-central-bank.html. [Accessed November 6, 2016].

Arnold, M., 2014. Barclays' Antony Jenkins calls end of universal banking. Financial Times. Available at: https://www.ft.com/content/ef588b42-860a-11e4-b248-00144feabdc0. [Accessed October 23, 2016].

Bank, A.D., 2016. Asian Development Outlook 2016 Update: Meeting the Low-Carbon Growth Challenge. Asian Development Bank.

Gibson, A., 2016. FSD Kenya: Ten Years of a Market Systems Approach in the Kenyan Finance Market. FSD Kenya.

Mod, C., 2016. The Facebook-Loving Farmers of Myanmar. The Atlantic. Available at: http://www.theatlantic.com/technology/archive/2016/01/the-facebook-loving-farmers-of-myanmar/424812/. [Accessed October 31, 2016].

Oxford Business Group, 2014. The Report: Myanmar 2014. Oxford Business Group.

Oxford Business Group, 2016. The Report: Myanmar 2016. Oxford Business Group. A. Jeffreys (Ed.).

Packer, G., 2008. Drowning. The New Yorker. Available at: http://www.newyorker.com/magazine/2008/08/25/drowning. [Accessed October 8, 2016].

Rajiv Lal, I.S., 2015. Mobile Money Services – Design and Development for Financial Inclusion. Harvard Business School.

Trautwein, C., 2016. MPT leads subs race with 18 million users. Available at: http://www.mmtimes.com/index.php/business/18980-mpt-leads-subs-race-with-18-million-users.html. [Accessed October 31, 2016].

Tucker, S., 2001. Burma: Curse of Independence. Pluto Press.

Turnell, S., 2009. Fiery Dragons: Banks, Moneylenders and Microfinance in Burma. NIAS Press.

Watcher, B., 1989. Burma in 1988: there came a whirlwind. Asian Survey 29 (2), 174–180.

Wintle, J., 2007. Perfect Hostage: A Life of Aung San Suu Kyi, Burma's Prisoner of Conscience. Skyhorse Publishing Inc.

Notes

1. (Bank, 2016).
2. (Packer, 2008).
3. (Tucker, 2001).
4. (Watcher, 1989).
5. (Wintle, 2007).
6. (Turnell, 2009).
7. (Turnell, 2009).
8. (Turnell, 2009).
9. (Turnell, 2009).
10. (Turnell, 2009).
11. (Turnell, 2009).

12. (Turnell, 2009).
13. (Turnell, 2009).
14. Some market participants are unclear about whether collateralization is a legal requirement or just an industry standard.
15. (Oxford Business Group, 2016).
16. (Bank, 2016; Oxford Business Group, 2014).
17. Curiously, telecoms are regulated under the same ministry as transportation, so the investment statistics are inseparable.
18. (Trautwein, 2016).
19. (Mod, 2016).
20. (Anon, 2016).
21. (Rajiv Lal, 2015).
22. (Gibson, 2016).
23. (Gibson, 2016).
24. (Arnold, 2014).

www.elsevierdirect.com

CHAPTER 17

Indonesian Microfinance Institutions (MFI) Move to Technology – TBOP's Prodigy Experience

Adrian Yeow, David LEE Kuo Chuen, Roland Tan, Michelle Chia

Contents

17.1 Introduction 431

17.2 TBOP and Its Prodigy Experience 433

17.2.1 Background of TBOP 433

17.2.2 TBOP's Prodigy Experience 434

17.3 Applying FinTech Development in MFI Market 448

References 449

17.1 Introduction

Microfinance institutions (MFIs) emerged to serve the unbanked populations with formal financial services that traditional financial institutions had failed to reach. From its humble beginnings as microcredit organizations in Brazil and Bangladesh, MFI has grown into a US$60 to US$100 billion industry with 200 million clients (World Bank, 2015). The goal and motivation behind microfinance is to transform rigid economic structures and develop financial inclusion by providing financial resources such as micro-loans and micro-savings, to destitute or rural poor households so they could move themselves out of poverty (Morduch, 1999). Although a recent industry report predicts a slower 10–15 percent growth in the global microfinance markets, the Asia Pacific region will still see around 30 percent growth (Herger et al., 2015).

Indonesia has one of the largest unbanked populations in the world (about 64 percent unbanked) (World Bank, 2014), with more than 81 percent of its population earning less than

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00017-6
Copyright © 2018 Elsevier Inc. All rights reserved.

US$4.50 a day (World Bank Estimates). As such, it has had a long history of microcredit programs dating back more than 100 years (KPMG Indonesia, 2015). Some industry experts estimate that there are more than 36 million microfinance borrowers through Indonesia's diverse institutions, programs, services setup by both government and nongovernmental groups. The Indonesian microfinance market is split between two segments: one segment is covered by regulated microfinance providers such as commercial banks such as Bank Rakyat Indonesia (BRI) and rural banks or Bank Perkreditan Rakyat (BPR) focused on districts and sub-district towns; the other segment is covered by NGOs, cooperatives, and village-based institutions referred to as Badan Kredit Desa (BKD) and Lembaga Dana Kredit Pedesaan (LDKP) focused on the lower end of the market with some reach to remote rural areas. Altogether there are over 1,643 BPRs and 188,181 cooperatives in Indonesia. However, there are many unlicensed non-bank MFIs and their numbers vary from 40,000 to 600,000. Overall, commercial banks dominate the market with five times more branches and contribute 98 percent of all loans (KPMG Indonesia, 2015).

Like many microfinance markets, the promises of microfinance have not been fully fulfilled in Indonesia given the following challenges. The first challenge is that microfinance services are very costly. A recent report in 2016 by the World Bank Group found that the median unit cost is US$14 for each US$100 of loans outstanding (Cull et al., 2016). This is also reflected in its "high" interest rates that it charges borrowers (global average is around 35 percent) (Kneiding and Rosenberg, 2008). This high cost is related to two underlying reasons. First, it is linked to the cost of operational processes involved in providing microfinance services, i.e., search costs to reach poor, unbanked, remote populations as well as intense and costly monitoring of clients by loan officers. Second, it is related to the fact that loan amounts are often small and the revenues are a direct function of these loans (Kneiding and Rosenberg, 2008).

The second challenge is the number of controversies surrounding MFIs in recent years. For example, some research has begun to question if MFIs have led to greater exploitation of the poor (Sandberg, 2012) while others have begun to scrutinize the sustainability and impact of MFIs on social and economic improvements (Mader and Winkler, 2013; Hamada, 2010). As such, donors and regulatory agencies have begun to seek for more accountability and to exercise more intensive oversight into MFI operations. Furthermore, organizations that fund these MFIs by way of loans or outright gifts are increasingly asking for analytics, which allow for tracking of the social impact brought about by MFIs' work. In 2012, the Indonesian government enacted various regulatory changes to reduce the perception that MFIs are risky investments and to improve the MFIs' efficiency and integration into the financial systems. Specifically, Indonesia's New Microfinance Law that recently went into effect from 8 January 2015 increased the government's regulatory oversight of all MFIs. Some aspects of this law include financial reporting and information obligations and other licensing requirements. Another set of regulations relates to Branchless banking rules or "Laku Pandai"

that enables current commercial banks to enter into the microfinance segment through agent networks – the traditional system used by existing BKD and LDKP (KPMG Indonesia, 2015).

Put together, MFIs in Indonesia are faced with two sets of pressures. One set involves cost and revenue pressures and MFIs have only two recourses: to either ask their clients and donors to absorb them or to build in efficiency into the operational processes in order to drive costs down. The other set involves increased regulatory and government scrutiny of MFIs' operations and potential competitive threats from existing commercial banks. In a way, both sets of pressures are driving the MFIs towards one clear path, i.e., to focus more on efficiency and profitability. The strategy to improve efficiency is definitely superior as it provides the platform to scale the number of clients and thereby progress towards a more sustainable mode of operations. At the same time, it involves developing better operational standards and control mechanisms across the different aspects of MFIs' operations. The question is how could Indonesian MFIs achieve these objectives? We discuss below a case study of how MFIs could build a system that would enable them to successfully embark on this strategic pathway.

17.2 TBOP and Its Prodigy Experience

17.2.1 Background of TBOP

TBOP Pte. Ltd. ("TBOP") is a Singapore based company formed in 2012. Two of the founders were pioneers in the broadband Internet industry, having been involved in the setup and management of various telecommunication companies in Singapore and Indonesia in the late 1990s and early 2000. Building on the core security business of one of its shareholder, a Singaporean cybersecurity firm that designs, implements, and maintains online identification and security infrastructure, and is Asia's first publicly accredited certification authority, TBOP was formed to focus on deploying software solutions to the world's lowest socio-economic level. The company believes that the use of relevant technology, especially via mobile devices, can bring considerable and measurable social impact to those at the base of the pyramid. The three main areas that TBOP focuses on, and which are generally recognized to be important to poverty alleviation in rural areas, are Financial Services, Health Services, and Education. One of the strategic domains was the development of robust and secure mobile applications for MFIs. The main principle behind TBOP's application development is to focus on solutions that enable MFIs to implement best practices, improve operational efficiency, and increase operational cost effectiveness while instituting responsible lending practices and to provide clear audit trails with a view to control fraud.

www.elsevierdirect.com

17.2.2 TBOP's Prodigy Experience

Inception: The project started when TBOP was contacted by a Singapore based consultant for a large MFI in Indonesia who wanted a system that could represent best practices in their internal audit as they were preparing for due diligence by new investors. TBOP's team spent three months with the MFI studying their existing business processes, field operations, information systems, as well as understanding the different microfinance products they offered. TBOP's team also met up with key personnel from International Finance Corporation and other industry stakeholders working in the financial inclusion industry to get additional inputs into potential operational improvements and requirements for a MFI system. This study resulted in the decision to develop the system from scratch, which was named Prodigy, as it was not possible to find a suitable product in the market that would meet the specific requirements of the MFI. TBOP began the development of Prodigy in the first quarter of 2015.

Boots on the ground – challenges from the field operations: As part of their principle of building systems that would enable MFIs to reach their full operational potential, TBOP's first step was to put "boots on the ground," in other words, they invested a significant amount of time and resources to send their personnel to the MFI central IT offices, branch offices and to also accompany the field officers who were conducting their weekly field visits in the villages. Based on their interactions with the various industry leaders and from their time spent with the different Indonesian MFI field offices, TBOP's team surfaced several critical challenges to the development of effective management information systems. The first set of challenges is rooted in the operational work of MFIs' field officers while the second set of challenges is found in the process flows linking the central office to the field offices.

To fully understand the operational work of the MFIs' field officers, one needs to appreciate the nuances of their work environment and cultural expectations. Whereas clients of commercial banks usually go to their bank offices to settle any bank transactions, MFIs who service the unbanked in rural areas with poor infrastructure usually send their field officers to the clients' villages instead. The frequency of the meetings between field officers and the clients differs and it depends on the model of lending as well as needs of clients and institutions. Some MFIs have meetings on a regular basis, e.g., every two weeks, while others may only meet a few times a year (Brouwer and Dijkema, 2002). Currently in Indonesia, MFIs practice two different models of lending: individual-based contracts and group lending. The largest Indonesian MFI, BRI, employs the individual-based contracts and requires pledges of collateral. However, the smaller MFIs have employed the group lending model or the Grameen model (Wikipedia, 2016). Regardless of the model employed, the success of the MFI operations depends mainly on its field offices and field officers.



Figure 17.1: Typical MFI field officer meeting with clients (© 2016 Roland Tan).

MFI field officers serve the "last mile" of any MFI's operations and they are the de facto "face" of the MFI to the clients. As such, a field officer's work is about managing the face-to-face processes beginning with the recruitment and evaluation of clients, to the gathering of credit information (family, business expenses), to credit analysis, to disbursement of loan, and supervision of loan repayment. In the case of missed payments, they are also involved in enforcing collection policies. At the same time, field officers oversee the upselling of other loan and related products, e.g., insurance when the current loan matures. Apart from these diverse routine tasks, a field officer is also responsible for coordinating and monitoring the different groups (in the case of group lending) or individuals (in the case of individual contracts) for each meeting. The arrangement of regular client meetings helps to build the social cohesion and social capital between the MFI field officers and their clients as well as a source of information on clients for MFIs. For example, some MFIs use the meetings to give out awards, discuss regulations and late repayments, or to conduct training (Brouwer and Dijkema, 2002). See Fig. 17.1 for one of such meetings.

Undergirding this range of activities, field officers need to understand and apply complex rules such as policies relating to size of new loans, eligibility for new products, saving capacity of group loads, collection procedures that adjust to as a function of number of missed repayments. For example, field officers need to be aware that different loans are associated with different savings plan, and with each saving plan, which is comprised of a combination of mandatory and voluntary saving products; and with each mandatory saving product, there is specific weekly saving amount calculated based on the loan size. Also in connection with higher compliance requirements, field officers need to conduct reviews with the clients on specific timeframes, i.e., first week, seventh week, and the 45th week. These reviews are important as the client's eligibility for the next loan is determined by how they perform in each

www.elsevierdirect.com

of the reviews (TBOP Field Interview Notes). As most field officers do not bring their policy manuals out during their visits to the clients, they are expected to commit all these complex rules to memory. At the same time, field officers are often asked to make discretionary decisions as many of their clients are not well educated or well experienced with financial matters. So even though administrative activities are guided by standard policies, almost all clients need some form of customized treatments (Brouwer and Dijkema, 2002). In some cases, field officers may want to help out their clients when they missed certain repayments or require larger loans than what they are entitled to as they are the ones who know their clients best (Canales, 2014).

In addition to the field officers' difficult working conditions, few MFIs have sophisticated management information systems to assist the field officers' work. Most MFI field officers rely on manual paper-based systems to capture all the transactions. Thus, all disbursement of funds and collection of repayments are manually captured on paper notebooks.

This leads to the second major challenge, which is the manual process flows linking the central office to the field office and officers. First, the manual process flows tend to reduce the timeliness and accuracy of relevant data and information stored at the MFI central office. Since most of the data and processes beginning from its field officers to its field offices are based on paper systems, all monitoring and tracking of loan performance and savings data have to be manually done by the field office staff. However, given that the field officers only visit each village on a specified time interval (e.g., two months), the data from each client will be lagged by that time period. Also, data on the social impact of the programs, e.g., improvement in working opportunities and jobs or housing and neighborhood improvements are often not systematically captured. A study shows that less than 30 percent of field officers collect these data and most report that they only do it in an informal manner (Brouwer and Dijkema, 2002). Couple these field problems with the laborious process of entering all the paper-based transactions into standalone computer systems or paper ledgers and then transporting the information back from thousands of field offices to the central office via paper cartons for paper files or low-bandwidth data leased line, it is no wonder that there is a lack of timely and accurate information on key indicators of the MFI operations. Thus, MFIs may find it difficult to execute timely interventions on delinquent borrowers or deal with threats of fraudulent activities among field officers. More importantly, MFIs may find it difficult to roll out improvements and more varied products given the lack of up to date client information. See Fig. 17.2 for a typical field office in Indonesia.

Second, the manual processes linking the field officers and field office also impact the ability for MFIs to recruit and scale their operations. For example, potential new clients are asked to fill in paper forms as part of the recruitment and evaluation process. These paper forms are



Figure 17.2: Typical field office in Indonesia (© 2016 Roland Tan).

collated and sent back to the field officers' office for data entry into standalone computer systems or simply filed into paper folders. The field office manager will then review the data on the computers or the files to verify that the data entered are complete and valid. However, if there are missing, invalid, or erroneous data, the field officer has to return back to the villages to ask the potential clients to fill or update the information on the paper forms. This to-and-fro process can easily drag for more than a month and thus make the recruitment process a lengthy and inefficient one.

Finally, the paper-based system also creates significant data vulnerabilities. Indonesian MFIs have reported many cases where field offices experience natural or man-made disasters that led to the destruction of all the client paper records. In one short vignette, an MFI CEO recalled that one of their branch offices was destroyed when a volcano erupted near the village. Given the catastrophic loss of data, the entire operation for that village had come to a standstill. However, this operational standstill was not tenable as MFI's relationship with its clients in the village is built on trust and word of mouth and if that trust is lost due to incompetence, then it will quickly be spread to the rest of the other villages in the region (Brouwer and Dijkema, 2002). In this case, the CEO of the MFI had to fly into the village and attempt to restore the operations as well as to go to the different leaders to do damage control. Because all the data were recorded only on paper, the CEO had to accompany the field officers to ask

www.elsevierdirect.com

each and every client to produce their client loan cards and painstakingly record them down to rebuild their operational database (TBOP Field Interview Notes).

Enable, don't disrupt – TBOP's Design Approach: Given their in-depth understanding of Indonesian MFIs' operational challenges, TBOP's approach in designing the Prodigy system – the MFI management information system – was "enable, don't disrupt."

This crux of this principle was to provide the least amount of functional disruption for the field officers. Recognizing that the field officer's work is key to any MFI's operations, TBOP's team designed the Prodigy system from the field officer's perspective. As such, the Prodigy system was built to seamlessly integrate with existing processes while taking into consideration the social and cultural nuances of the field officer's work. This can be seen in the design of their Field Officer Mobile Module. In this module, TBOP replicated all the existing paper-based forms as features in a mobile device. For example, at the start of day, field officers are typically given a sheet of paper that contains a to-do list with the number of collections and evaluations they have to do in each particular village. This is now replicated as an operational dashboard with the tasks-for-the-day summary. It shows that total repayment collection total, total savings, total savings withdrawal, and total disbursement as well as the cash on hand. In the past, the field officers would have to acknowledge on paper all these work tasks and sign the form to draw the cash for their work and to manually calculate sums of monies to be collected and disbursed and the cash they should have at the end of the day. With the new system, they only have to acknowledge on the mobile device and the system, and the system would work out automatically how much cash they should have by the end of the day. See Fig. 17.3.

Whilst these features are important to the proper filling of forms and data, TBOP's team recognizes that there will be situations where field officers may have to make ad hoc changes to the amounts that they collect or to input data on specific customization and contingencies as discussed earlier. The need for some latitude and discretion on the part of the field officers is also incorporated in the Field Officer Mobile Module in that they are able to update any of the repayment amounts or savings or whether the repayment was assisted or missing. These functionalities therefore assist the field officers in dealing with last minute changes that they may meet in their regular meetings with clients. On the other hand, the Field Officer Mobile Module also includes an audit trail that captures any of these variations that are applied to the clients. This ensures that while field officers are able to handle contingencies in the field, the field office managers can ensure that proper checks and audit are applied to these changes. See Fig. 17.4.

Likewise, all paper transactions between the field officer and the clients have also been replicated and replaced by the Field Officer Mobile Module installed on the mobile devices. For example, field officers used to have to issue a paper receipt after collecting the repayments from the clients. In the Field Office Mobile Module, field officers are able to enter the amount

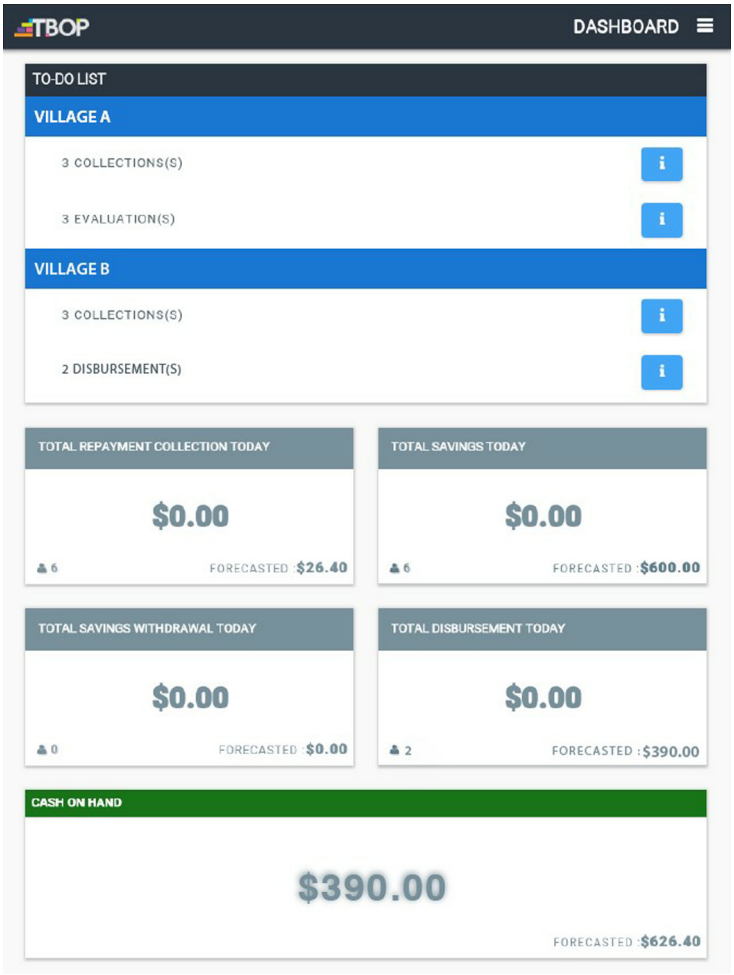


Figure 17.3: Prodigy dashboard with daily to-do list and summary of collections and disbursements for the day (© 2016 TBOP).

collected and then have an option to either to send a SMS to the client's hand phone or print a receipt for the client. If the client so wishes, the field officer can also do both – send an SMS and print a receipt for the client.

More importantly, unlike the paper-based system, the field officer is able to now access all the past records and transactions of a client by using the search function and client profile. This would enable the field officer to track, monitor, and conduct timely interventions or to provide better service to the clients depending on the past transaction profile. Also, included in the Prodigy system is the new client creation feature. Using the intuitive interface and assisted

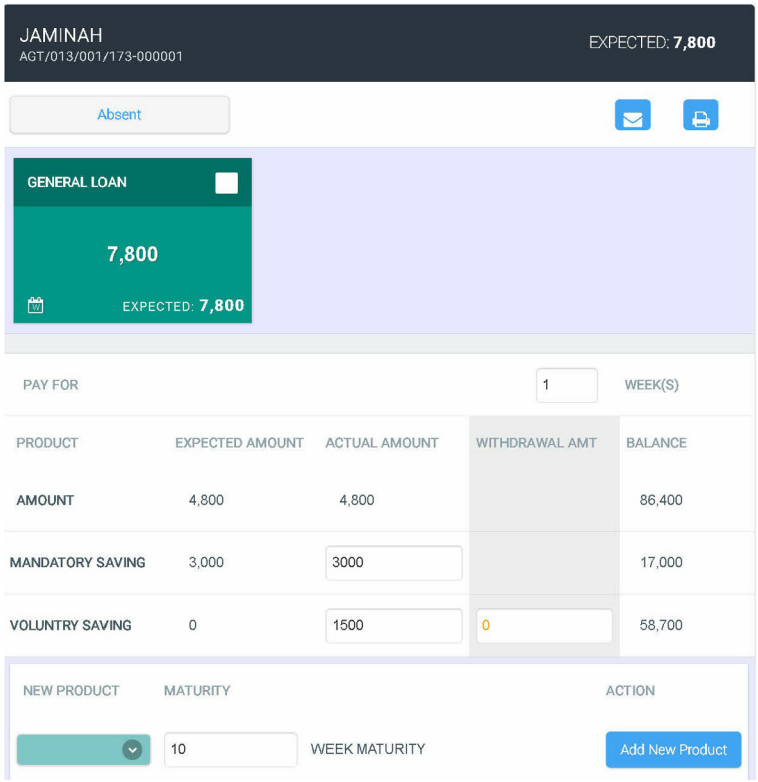


Figure 17.4: Field Officer Mobile Module (Prodigy^{m}) – Screen with details of the day's transaction(s) of an individual client. If the Actual Amount collected differs from the Expected Amount for a particular product, Field Officer will update the amount collected in the respective textbox. Once the SMS is sent or receipt is printed, Field Officer will not be able to amend the amount entered in the Actual Amount field (© 2016 TBOP).

by dropdown options, field officers can easily capture the critical personal information of a potential client, and with the mobile device's camera function field officers can easily capture the photos of client as part of the documentation. This feature thus aims to plug some of the issues in new client creation, e.g., data input errors, invalid or missing data, and thus reduce the time required for new client approval. See Fig. 17.5. Finally, the field officer's work of capturing data on the social impact of the programs is also part of the Field Officer Mobile Module. Specifically, the Prodigy system incorporates a Housing Index scoring feature where field officers enter in criteria for the housing index, e.g., housing type, housing size, etc., and the module will calculate the housing index for the client.

By blending the existing work processes and form designs in the Field Officer Mobile Module, TBOP's system retains the familiarity of the existing work while providing critical



Figure 17.5: Field Officer Mobile Module (Prodigy^{m}) – Highly interactive form filling screen for creation of new client record with integrated photo capturing function (© 2016 TBOP).

www.elsevierdirect.com

changes in capturing and updating vital client transaction data. This seamless integration is key to overcoming potential user resistance towards the mobile system and remove any sense that field officers are being forced to use a new and unfamiliar technology (Davis et al., 1989). In fact, the field officers who have been exposed to the Prodigy's Field Officer Mobile Module expressed delight and immediate interest in using it in their work. As one MFI field officer shared with the TBOP's team:

> *"We enjoy the tablet because it helps us in (our) work. It brings us one step up. No just going out on motorbike with paper and forms. With the tablet, we are more modern and smart."*
>
> ***Translated from Bahasa Indonesia, TBOP Field Interview Notes***

In addition to the design of the Field Officer Mobile Module, Prodigy's team recognized that the field officers required a solution that could work in rural areas with little or no infrastructure such as mobile or broadband data networks. As such, the Prodigy team consciously designed the solution to work on HTML so that they could be deployed on any mobile device installed with a web browser. The printing of receipts is enabled by low-cost portable Bluetooth printers connected to the mobile device. This ensures that MFIs that do not have large IT budgets can still be able to deploy the solution on cheap off-the-shelf mobile phones or tablets. Next, the Field Officer Mobile Module is also designed to operate in either "online" or "offline" modes depending on the availability of Internet and/or mobile connectivity. In most cases, where field officers are operating without any access to Internet connectivity, the Field Officer Mobile Module is able store all transaction records first so that these records are uploaded to the main management module when the field officers return to their field offices. The data synchronization can be done either via physical networks or via wireless means such as Bluetooth or Wireless LAN. This near real-time system architecture thus harnesses the power of mobile technologies for MFIs while taking into account the physical and budgetary constraints that MFI field offices face in their work. In this way, TBOP's Prodigy system truly reflects a localized platform that is there: "enable, but don't disrupt."

Building a bottom-up scalable platform: In addition to the Field Officer Mobile Module, given the challenges arising from the manual process flows linking the central office to the field offices, TBOP recognized the need for an integrated management module that not only deals with these issues but could also achieve the application of responsible lending practices and fraud controls. As we have briefly discussed above, the Prodigy's Field Officer Mobile Module captures all the transactions and changes that are made by the field officers. By embedding all the mobile module forms with the rules relating to loans and/or savings, the Prodigy system helps ensure that field officers adhere to the various MFI policies that apply to different clients. Moreover, each field officer has a unique username that they use to login to use the

system. All transactions and changes made in the Field Officer Mobile Module will be tagged with the field officer's username and time-stamped. Through all these system measures, the Prodigy system's Field Officer Mobile Module helps to promote accountability, transparency of data, and a set of proper audit trails to control fraud and increase operational clarity.

At the same time, the Prodigy system incorporates a Management and Back Office module that is installed in each field office. In the past, most field offices had a management information system that is linked to their central office banking and MIS servers. However, because the existing field office management information systems are not integrated to the field officer's work, there is significant inefficiency, as the manual data entry by the field office managers becomes a major bottleneck in the entire workflow. Furthermore, as discussed above, because most data is stored on paper files, the risk of loss of data, inaccuracies, and lack of timeliness remains very high and the operations are susceptible to catastrophic data loss.

Prodigy's Management and Back Office module was designed bottom-up by the team to deal with these critical data gaps in the MFI field office operations. First, the Management and Back Office module is fully integrated with the Field Officer Mobile Module. The ability to easily synchronize and update client data and transactions helps to deal with the bottleneck caused by the current data entry issues. More importantly, field office managers are now able to easily access client management information so as to review their performance, approve any changes to their loans and savings, and verify the social impact on their clients. This was especially helpful in shortening the duration between enrollment and approval of new clients since field office managers can easily review all potential client applications via the Management and Back Office module. See Fig. 17.6. Furthermore, with a more efficient database system, the field office managers can conduct a more stringent check on each application that includes: verifying if the client is already a borrower in another MFI, whether they have outstanding loans, character of client, etc. In the past with paper records, this process would have been very time consuming or in some cases overlooked as the competition for new clients among the different MFIs is quite intense. Altogether, the integration and computerization of client data in the Prodigy system has improved the efficiency and quality of work of the field offices.

Second, the Management and Back Office module also improves work processes with regard to the management of field officers. See Fig. 17.7. In the past, given the paper-based forms, field office managers might require significant amount of effort to collate and review each field officers' work and to ensure that they were performing in accordance to set targets. Yet the reality is that many of the field officers may only work part-time with one MFI and hold other jobs (Brouwer and Dijkema, 2002). As a result, there is a risk of high turnover, low work morale, and poorly trained field officers. With the integrated database and reporting features (both standard and customized reports are available), the field office manager has better

www.elsevierdirect.com

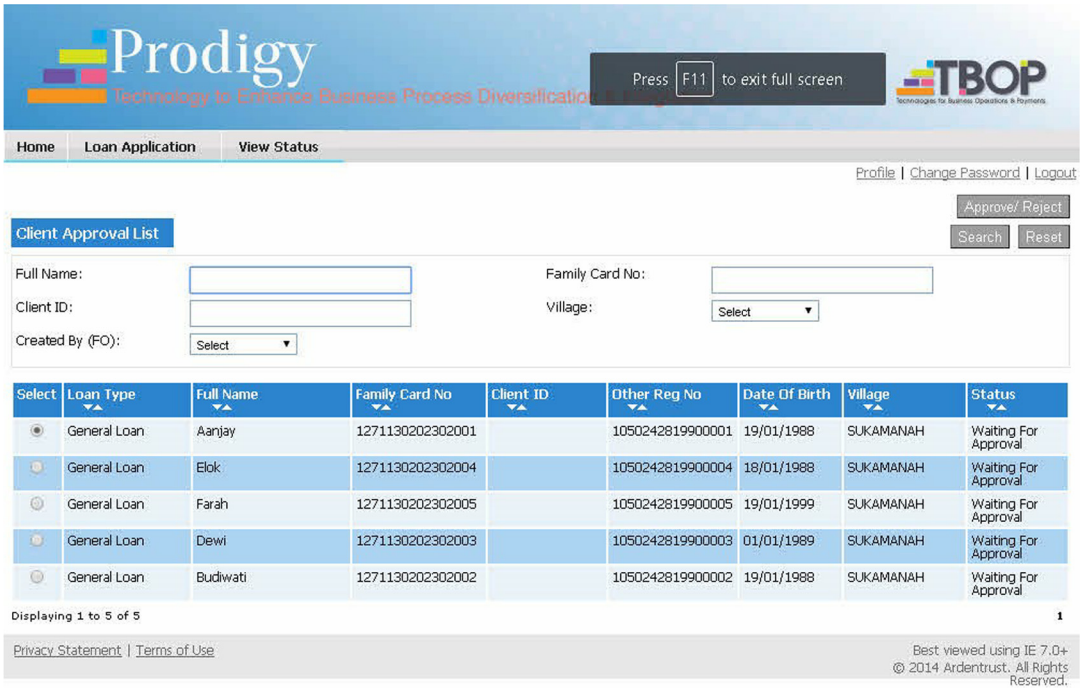


Figure 17.6: Management and Back Office (*Prodigy*$^{+}$) – Loan Approval & Management Function (© 2016 TBOP).

insights into each field officer's work performance; for, e.g., the field office manager can now track the performance history of the clients assigned to each field officer as well as the trend data for new client enrollment or new loans and savings take up rates. This set of information thus allows field office managers to effectively manage the field officers and put in place informed interventions. For example, the field office manager could single out field officers who are not performing well for counseling and training. On the flipside, field office manager could highlight the top performing field officers for monetary awards so as to spur the other field officers to perform better.

Not only does this improve the tracking and monitoring of work performance, the Management and Back Office module ensures that any potential fraudulent activities could be flagged up for interventions. The problem of fraud is also controlled by a strict set of secure and auditable processes for issuance and submission of collected cash between the field officers and the field office personnel. For example, all cash monies transactions require the authentication of users via individual PIN. At the same time, given that user security on the field officer's mobile device is vital, the management module also allows field office managers to update any changes to field officers' assignments, centralized provisioning, and configuration

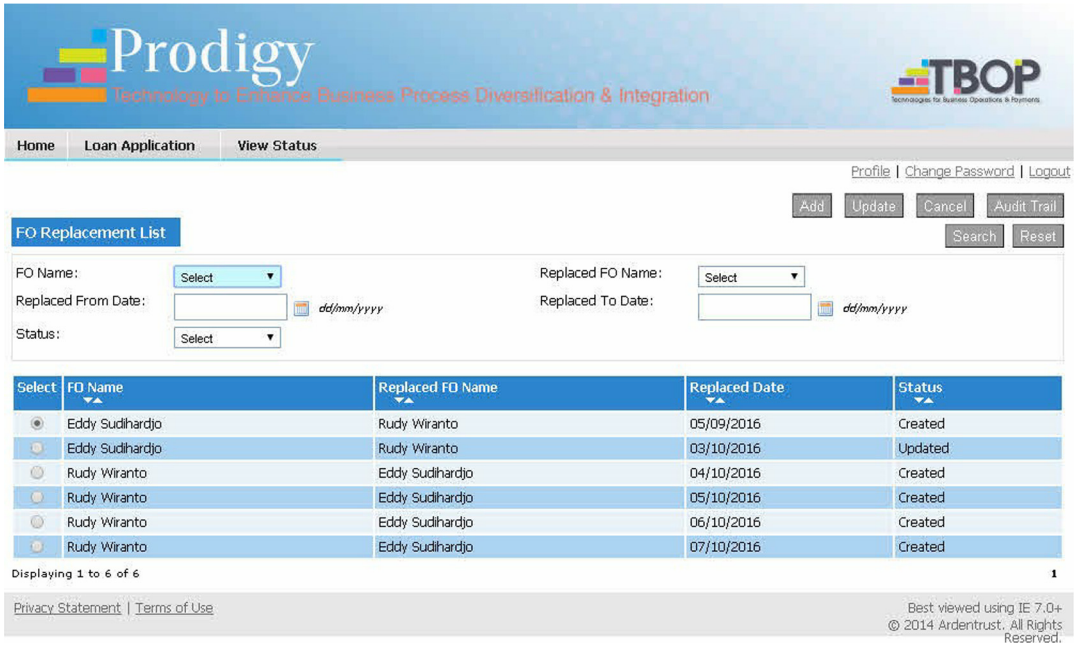


Figure 17.7: Management and Back Office (*Prodigy*$^{+}$) Assignment of Customers to Dedicated Field Officer; and management of Field Officer's customer base (© 2016 TBOP).

of mobile devices, and in the rare case of theft of devices, the management module can even remotely revoke user access to the device.

Beyond managing the field office and field officer operations, the Management and Back Office module serves as an important platform for the entire MFI organization. First, each field office Management and Back Office module can be integrated with the MFI central office's existing banking and MIS systems. In the past, MFI field office staff had to log into their local banking system terminal and print out daily tasks and jobs. The daily transactions were then entered in manually at the end of day on the same banking system terminal. With the integration between the Management and Back Office module and the existing banking and MIS systems, all transaction and job data can be easily stored and transferred between field offices and the central office and then to the field officer's mobile device seamlessly. Given that many MFI field offices are not equipped with broadband data links (via leased lines or Internet), TBOP's Prodigy system was designed to work with low data bandwidth environment. The MFI's central office banking server is linked to the Prodigy Management server, which would manage the daily scheduled data extraction and transfer between the MFI central banking system and all its field offices' Prodigy Management and Back Office systems.

www.elsevierdirect.com

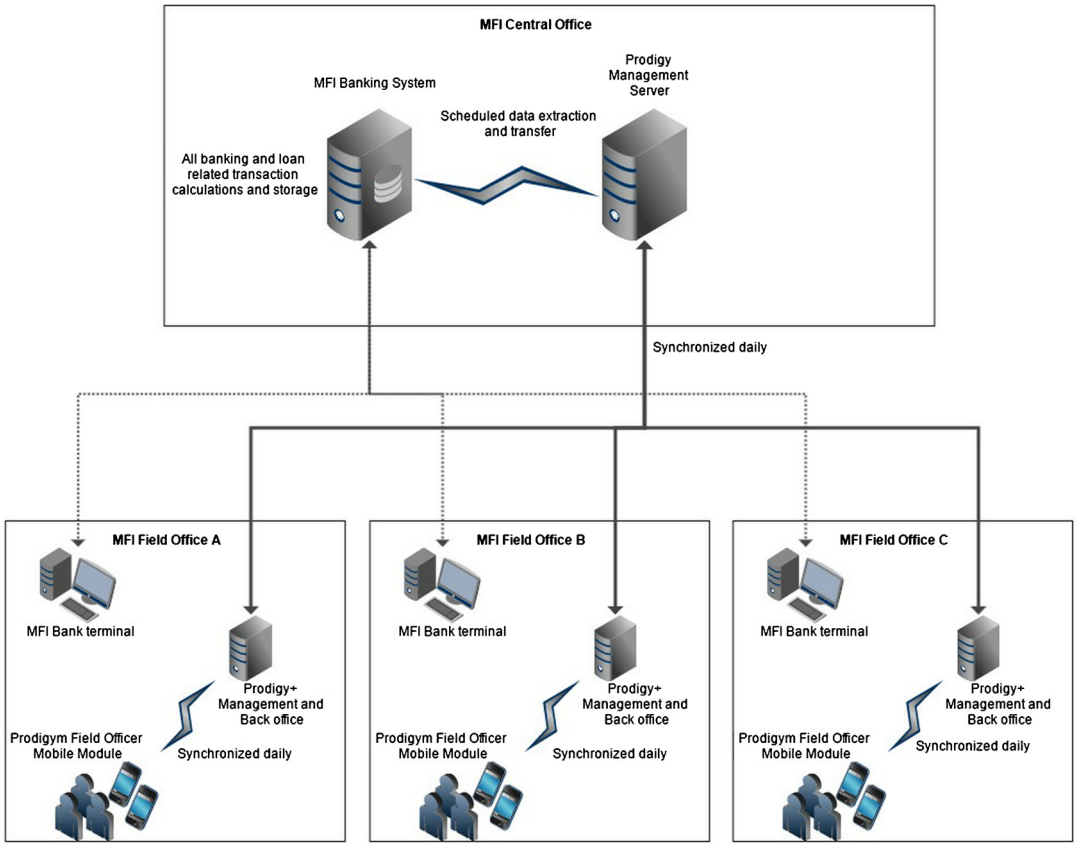


Figure 17.8: Basic system architecture of the Prodigy system (© 2016 TBOP).

The Prodigy Management server and the field office Management and Back Office module thus act as a data transfer and management module while the MFI's banking system continues to manage all banking and loan related transaction calculations and storage. See Fig. 17.8 for the basic system architecture of the Prodigy system. This modular design reflects the bottom-up approach as it allows MFIs to continue to leverage on their banking system investments while being able to improve the operational efficiencies across its entire field office networks. Furthermore, with the scheduled data transfer feature built into the Prodigy Management server, field office data are now automatically updated into the central office banking systems on a daily basis. In this way the Prodigy system helps enable best practices of robust business continuity, data security, and risk management into the MFI data network while providing near real-time data updates for MFI central office staff.

In addition, given TBOP team's rich experience in building and managing broadband infrastructure, they have introduced other features into the Management and Back Office setup to

minimize the risk of system downtime and failures – a problem that plagues many MFI field office operations. First, the Prodigy field office Management and Back Office server is physically linked to an external hard drive for daily onsite backups. The Management and Back Office module is easily linked to an automated data backup module that will back up the data onto the external hard drive. This setup serves as an onsite backup solution if the Management and Back Office server fails. Second, to avoid any interruption in the data transfer between the field office and central office systems, the Prodigy system can be connected to mobile wireless modems that serve as a data backup in case the field office's data links are disrupted or disconnected.

Finally, the Prodigy's Management and Back Office system can also work for remote field offices that are not currently connected to any data network. In such cases, MFI remote field offices can choose to work on a standalone mode. When required, the MFI remote field office staff can connect the Management and Back Office server (installed on a laptop) to any Internet links, e.g., an Internet café or mobile wireless hotspots, and activate a data synchronization with the MFI central office banking system. This particular configuration is important as some MFI field offices operate in remote parts of Indonesia where telecommunication infrastructure is still not developed. Without a system like Prodigy, these field offices currently depend on manual transportation networks to ship cartons of paperwork back to the central offices – often located on the main capital city of Jakarta. As such, they introduce significant amount of cost and delay to the consolidation of data of MFIs' operations – an issue that will impact the sustainability of MFIs given the increased financial reporting and information obligations required by donors and the Indonesian governments.

In sum, the TBOP's experience in building the Prodigy system for the Indonesia MFI market dispels a common IT system development myth, that is: "if you build it, they will come." Although there are many studies and industry white papers that have discussed why and how MFIs need to improve their operational management information systems and thereby improve the efficiency and overall sustainability of its business (Morduch, 1999; Jawadi et al., 2011), the take-up among MFIs for more advanced and technically robust solutions has not been as high, and in some cases, the IT systems that were adopted were later abandoned due to high cost and problems of maintenance (Parikh, 2006). TBOP's experience in building the Prodigy system for Indonesian MFIs reveals three effective principles that other MFIs could consider: a) adopt the MFI's perspective by investing in a "boots on the ground" approach, b) translate the ground-level requirements and understanding into a user-focused design that "enable, (but) don't disrupt" their processes, and c) build a bottom-up scalable platform that could be leveraged across the network of MFI offices. In this way, MFI and technology companies would be able to collaborate and build systems that enable the MFIs to effectively embark on the path towards greater efficiency and sustainability in light of current economic and regulatory pressures.

www.elsevierdirect.com

17.3 Applying FinTech Development in MFI Market

The importance of FinTech in the MFI market lies in its ability to power inclusive growth in emerging economies. Studies show that FinTech could potentially reduce operating costs and enable MFIs to increase their reach among the unbanked and underbanked (Lee, 2015). Indonesia, for example, has set the objective of reaching 75 percent of adults as being financially included by 2019 (Duflos, 2016). For the country this translates to unlocking productivity and investment, reduce poverty, empower women (as MFIs generally lend to women), strengthen institutions by reducing corruption, and thereby narrow the gap between the difference financial strata of the population.

The biggest obstacle to financial inclusion is the difficulty of the unbanked to gain access to basic banking facilities, i.e., receive money, send money, pay bills, and manage cash flows effectively. The mobile device, with its every increasing penetration to all segments in a community, is the answer to this. FinTech in the form of applications and delivered via smart phones will be the basis of digital finance moving forward (Mori and Zimmer, 2015). The building blocks of FinTech in the MFI industry will be a widespread digital infrastructure, a sustainable financial services industry supporting the unbanked as they move towards financial inclusion, and a robust and secure, well-disseminated personal identification system that financial-services providers can easily verify.

In other words, the MFI FinTech ecosystem is made up of the individual client, the microfinance and banking institutions, merchants, and other non-banking institutions like the telecom companies. A system like TBOP's Prodigy could serve as the digital platform that will provide an end-to-end solution in this ecosystem. Potentially borrowers could access all mainstream banking and microfinance services on their mobile devices, the financial institutions would service and support all their customers with a robust, secure, and efficient electronic system with the ability to mine the data for analytics, the merchants have their relevant Prodigy module on the point-of-sales terminals (which could be mobile devices), payments can be made cashless through integration with digital money providers, and the telecom companies can provide and ensure connectivity through their infrastructure. Governments will be quick to embrace and encourage this drive to a digital economy as it will bring obvious benefits of increased social stability through financial inclusion and the reduction of poverty and hunger, raise gender equality, improve education and healthcare, and experience growth in tax revenue from businesses.

An estimated two billion adults lack access to a transaction account and are excluded from the formal financial system (World Bank, 2014). In response, the World Bank Group with private and public sector partners have set an ambitious target to achieve Universal Financial Access (UFA) by 2020. The UFA goal is that by 2020 adults globally have access to a transaction

account or electronic instrument to store money, send and receive payments. Financial access is the first step toward broader financial inclusion, where individuals and firms can safely use of a range of appropriate financial services, including savings, payments, credit and insurance. Systems like TBOP's Prodigy represent a step towards the achievement of this goal.

References

Brouwer, A.W., Dijkema, D., 2002. Microfinance dilemma: the case of Bandung, Indonesia. In: Economics Science Shop. Groningen University, Groningen.

Canales, R., 2014. Weaving straw into gold: managing organizational tensions between standardization and flexibility in microfinance. Organization Science 25, 1–28.

Cull, R.J., Demirguc-Kunt, A., Morduch, J.J., 2016. The microfinance business model: enduring subsidy and modest profit. Policy Research working paper [online]. Available: http://documents.worldbank.org/curated/en/404501470669620154/The-microfinance-business-model-enduring-subsidy-and-modest-profit [accessed 20/10/2016].

Davis, F.D., Bagozzi, R.P., Warshaw, P.R., 1989. User acceptance of computer technology: a comparison of two theoretical models. Management Science 35, 982–1003.

Duflos, E., 2016. Emerging opportunities for digital finance in Indonesia. Available from: http://www.cgap.org/blog/emerging-opportunities-digital-finance-indonesia [Accessed 25/10/2016 2016].

Hamada, M., 2010. Commercialization of microfinance in Indonesia: the shortage of funds and the linkage program. The Developing Economies 48, 156–176.

Herger, N., Hug, C., Janett, U., 2015. Microfinance market outlook.

Jawadi, F., Jawadi, N., Ziane, Y., 2011. Can information and communication technologies improve the performance of microfinance programs? Further evidence from developing and emerging financial markets. In: Ashta, A. (Ed.), Advanced Technologies for Microfinance: Solutions and Challenges. IGI Group.

Kneiding, C., Rosenberg, R., 2008. Variations in microcredit interest rates.

KPMG Indonesia, T., 2015. New Indonesian 'Branchless Banking' and Microfinance Laws – A Catalyst for Microfinance Growth? KPMG.

Lee, D., 2015. Future growth, financial inclusion, and Asia.

Mader, P., Winkler, A., 2013. Rise and fall of microfinance in India: the Andhra Pradesh crisis in perspective. Strategic Change 22, 47–66.

Morduch, J.J., 1999. The microfinance promise. Journal of Economic Literature 37, 1569–1614.

Mori, M., Zimmer, T., 2015. Mobilizing banking for Indonesia's poor. Innovations 10, 95–124.

Parikh, T.S., 2006. Rural microfinance service delivery: gaps, inefficiencies and emerging solutions. In: 2006 International Conference on Information and Communication Technologies and Development. IEEE, pp. 223–232.

Sandberg, J., 2012. Mega-interest on microcredit: are lenders exploiting the poor? Journal of Applied Philosophy 29, 169–185.

Wikipedia, T., 2016. Solidarity lending [online]. Available: https://en.wikipedia.org/wiki/Solidarity_lending [accessed].

World Bank, T., 2014. Financial Inclusion Data/Global Findex.

World Bank, T., 2015. Does microfinance still hold promise for reaching the poor? [online]. Available: http://www.worldbank.org/en/news/feature/2015/03/30/does-microfinance-still-hold-promise-for-reaching-the-poor [accessed 20/10/2016 2016].

CHAPTER 18

FinTech: Harnessing Innovation for Financial Inclusion

Dimitrios Salampasis, Anne-Laure Mention

Contents

18.1 Introduction 451

18.2 Financial Innovation and Sustainable Development 452

18.3 The Emergence of FinTech 454

18.4 FinTech and Financial Inclusion 456

18.5 Concluding Remarks 459

References 460

18.1 Introduction

The landscape of financial inclusion has for long been considered as the soft side of financial services, having received scarce attention from a financial, regulatory, and policy point of view, despite its central role within the global economic empowerment. Part of the disadvantaged and low-income segments of global population is left without (i.e. financially excluded) or very limited access (i.e. financially underserved) to basic financial services, creating a highly critical equality deficit in different parts of the world. In this frame of reference, financial exclusion still remains a highly critical problem that hinders developing regions around the world from eradicating poverty leading to large-scale starvation and civil unrest. Moreover, financial exclusion is interwoven with social dependency making financially excluded/underserved populations strongly dependable on their social networks (MasterCard Insights, 2014). The emergence of FinTech, the new breed between financial innovation and financial technology, which has been challenging the prevailing position of incumbent financial institutions, is providing a promising vehicle of tackling this phenomenon by closing the gap between unbanked, under-banked and developed societies, opening the door to the global digital economy, bringing a long-term societal transformational change for the financially excluded/underserved, while leading to inclusive economic growth (Demirgüç-

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00018-8
Copyright © 2018 Elsevier Inc. All rights reserved.

Kunt et al., 2015) helping move towards a more just and equitable society (Bisht and Mishra, 2016).

18.2 Financial Innovation and Sustainable Development

The new millennium has brought unprecedented progress in technology and science, but this is not the case for the big contemporary social issues: global warming, poverty, inequality, and death from treatable diseases, to name a few, are not being addressed with the same urgency. In the past, governments have been relied upon to deal with these issues, but more and more budgets are stretched and bureaucracy is often an impediment to advancement. What is needed in order to tackle these pressing social issues is to harness the capital markets.

Furthermore, the financial crisis has created a new realization of our financial world, leading to the destruction of institutionalized practices and depicting an emerging motivation for change. These institutionalized practices have a direct impact on the society, the environment, and the economic development, the three pillars of sustainable development (Kates et al., 2005). This impact is interpreted under the question on "*how can we create a financial system that sustains the economy, the people and the planet itself?*" The link between the financial sector and sustainable development is financial innovation.

As a concept, financial innovation "*embraces changes in the offerings of banks, insurance companies, investment funds and other financial service firms, as well as modifications to internal structures and processes, managerial practices, new ways of interacting with customers and distribution channels*" (Mention and Torkkeli, 2012, p. 11). In other words, it encompasses the making and promotion of financial products and services, the development of new processes, as well as the interaction with customers and development of new structures for the financial institutions (Mention, 2011a, 2011b).

Financial innovation is perceived under the context of strategic approach and behavior leading to value innovation or "*conventional logic*" (Costanzo et al., 2003, p. 259). Studies on the service context by Gadrey et al. (1995), by Frame and White (2004) and by Avlonitis et al. (2001) identify types of financial service innovations which "*are associated with different development processes in terms of activities, formality and cross-functional involvement as well as performance outcomes*" (Avlonitis et al., 2001, p. 334). Moreover, the emergence of the role of the user who is willing to contribute both to the development of a service but also to the technology per se behind the implementation of collaborative services since "*users often develop and self-provide important financial services before banks or other types of financial service producers begin to offer them*" (Oliveira and von Hippel, 2011, p. 806).

www.elsevierdirect.com

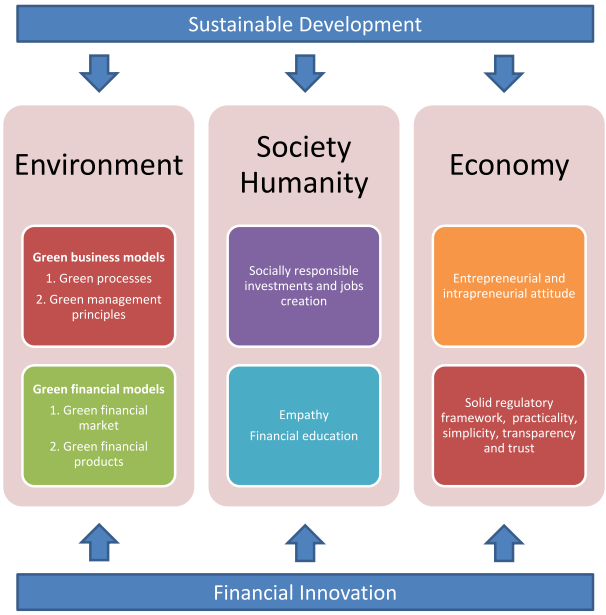


Figure 18.1: Financial innovation and sustainable development.

Financial innovation is about understanding the customer, appreciating the information from the partner, and differentiating from the competition. Financial innovation is strongly focused on the how, on the process of perceiving the specific needs of every customer, so as to offer personalized offerings, as far as the regulation and other constraints allow doing so. A stronger process innovation development leads to understandable tools, content and information.

Financial innovation shows the ability to evolve in order to be ready for the future. By evolving under an organizational and competences-oriented perspective based on customer and partner needs easies the process of creating a competitive advantage by differentiation. This requires a clear strategy and the ability to make choices. Innovation means to have the ability to decide, to admit being wrong, to have the ability of fast realization and understanding that if something is not working it is the time to stop. Innovation means to be able to make hard and difficult choices and the ability to say no. In short, innovation is first of all a matter of prioritization and choices (Fig. 18.1).

In September of 2015, the UN General Assembly consisting of 193 countries adopted the 2030 Development Agenda titled "Transforming Our World: The 2030 Agenda for Sustainable Development." Some of the world-transforming goals were: No Poverty, Quality Education, Gender Equality, Affordable Clean Energy, Decent Work and Economic Growth, Reduced Inequality, among others. Considering the magnitude, the multidimensionality and

www.elsevierdirect.com

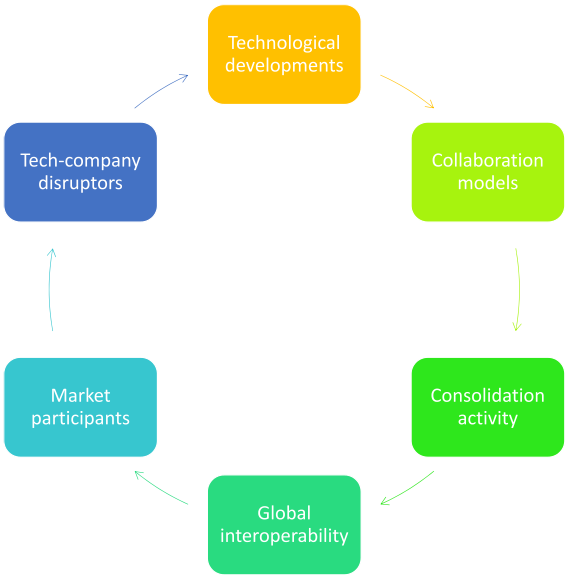


Figure 18.2: Challenges within the financial services sector (developed by the authors).

the geographic expansion of these world-transforming goals, innovation and entrepreneurship are necessary for connecting the poor to the formal financial system, hence the need for financial inclusion, which can be actively supported by FinTech, becomes crucial.

18.3 The Emergence of FinTech

The financial services sector is operating within a constantly changing world characterized by increasing complexity, interconnectivity, and velocity. These changes are taking place in both domestic and international markets. In this frame of reference, the financial services sector is faced with a number of critical challenges (Fig. 18.2).

Within these norms, a renewed momentum for a globally emerging technology-enabled financial services innovation paradigm is observed:

- challenging traditional business models, services and regulations
- modernizing the current financial architecture
- democratizing the financial innovation process
- catalyzing changes in financial habits and consumer behaviors
- developing new ways for accessing, delivering, experiencing, and co-creating financial services
- providing greater transparency and improved risk management

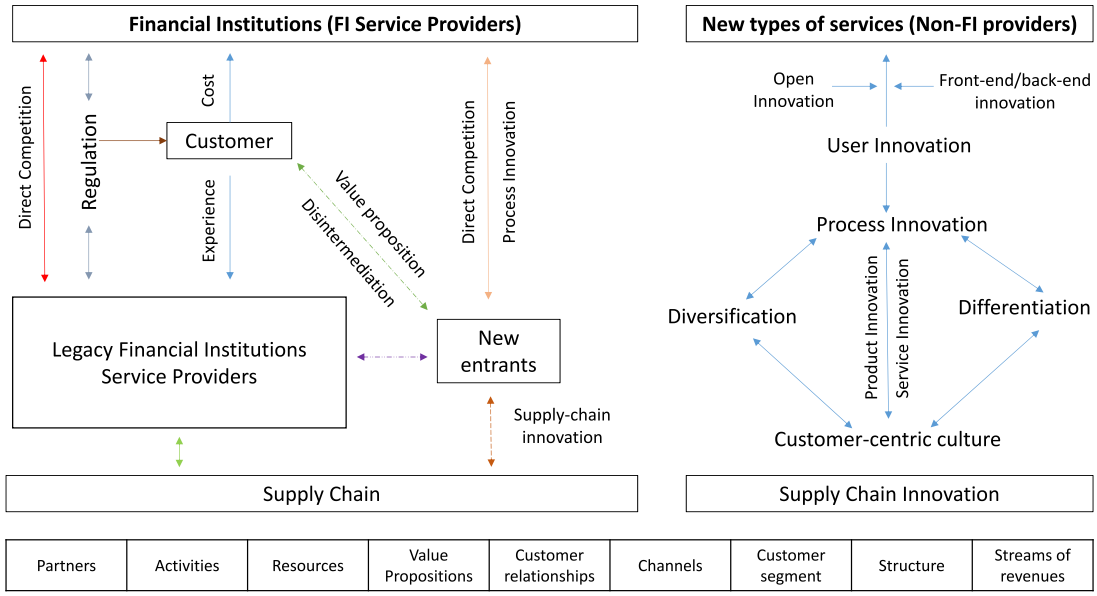


Figure 18.3: FinTech business model (developed by the authors).

Financial Technologies, aka FinTech, have been creating an unprecedented pressure to traditional financial institutions by unveiling new value propositions, through innovative and non-traditional technology-led business models. It brings an entire different logic that is causing fundamental changes in the structure and purpose of business, changes that the majority of traditional financial institutions are not ready to face (Fig. 18.3).

It is time for financial innovation to become more social and to further focus on people, economy, and environment. Financial innovation needs to make the best of limited resources and contribute to the world and social progress. It is simply a matter of incentives.

The current global challenges have shown an imperative need for collaboration among leaders of the public and private sectors so as to develop together a new global financial system based upon commonly interrelated regulatory policies, efficient technologies, trust, ethics, transparency, and collaboration for value co-creation and competitiveness.

The pillars under which financial innovation should be developed are related to the real and not virtual demands of the economy and finance, in line to the development of global, national, and local economy, in accordance to the consumer/user's financial maturity and needs, and under effective and efficient regulatory framework and supervision. Financial education, environmental awareness, and societal changes are the key for a more sustainably developed future and the financial sector by embracing financial innovation should be the pioneer to this social change.

www.elsevierdirect.com

18.4 FinTech and Financial Inclusion

"*We are seeing frictionless, super-scalable tech that will tip this iceberg and making a payment will be as easy as sending a text message*" argues Kosta Peric from the Bill & Melinda Gates Foundation.

FinTech challenges age-old orthodoxies about capitalism, nurturing the potential to facilitate widespread social and environmental change by harnessing the power of financial innovation and financial technology.

"FinTech is becoming an enabler of economic inclusion. In addressing previously excluded consumer demographics, the industry is in a position to drive innovation and economic and social change [. . .] Therefore, even modest strides in achieving economic inclusion present the single largest addressable opportunity in FinTech." (Strategy&, 2016, p. 7).

In this frame of reference, FinTech has led to the framing of a "digital financial inclusion" paradigm, which aims at developing digital transactional platforms with the ability to provide necessary financial services to the world's financially underserved societies, which are considered as a "goldmine" untapped market. The McKinsey Global Institute estimates a flow of $4.2 trillion in deposits in developing countries due to digital finance that allows a magnitude of people to have access to savings accounts beyond traditional and informal mechanism. This digital narrative has initiated a shift, within the financial services landscape, towards the generation of both economic and social positive outcomes in individual and collective terms, allowing societies to develop digital financial capabilities through to deployment of innovative technologies and financial tools (Shrier et al., 2016).

"High unbanked population, weak consumer banks and high mobile phone penetration make emerging markets ripe for FinTech disruptions [. . .] In our view, new entrants have a greater chance of success in markets with underdeveloped or fragmented banking systems accompanied with a high level of digital readiness [. . .] Smartphone penetration is higher than banking penetration in many emerging market countries and many emerging markets are digital leaders while they are banking laggards." (Citigroup, 2016, pp. 10+28).

Financial inclusion calls for democratizing financial services, catering for equal, unrestricted and universal access to, and use of, different types of distributed financial services provided, in a responsible manner, by legitimate institutions and at a reasonable price, and in a cost-effective manner. It focuses on creating self-sustained and replicable solutions, leveraging the symbiotic relationship between sustainable development, human development and economic empowerment. "Studies show that broader access to and participation in the financial system can reduce income inequality, boost job creation, accelerate consumption, increase investments in human capital, and directly help poor people manage risk and absorb financial shocks" (Klapper and Singer, 2014, p. ii).

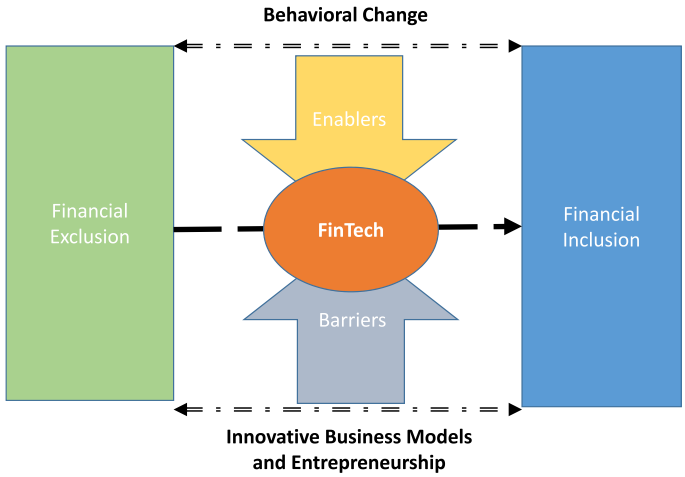


Figure 18.4: FinTech and financial inclusion (developed by the authors).

According to the 2014 World Bank Global Findex Database, the number of people globally having an account grew by 700 million between 2011 and 2014. Furthermore, 62% percent of the world's adult population have an account compared to 51% in 2011. Three years ago, 2.5 billion adults were unbanked. Today, 2 billion adults remain without an account, representing a 20% decrease. The main reasons for these improvements are related to technological advances, particularly growth of mobile devices and digital financial services.

In this context, the World Bank Group (WBG), together with fourteen private and public sector partners, has put forward the Universal Financial Access (UFA) by 2020. According to the World Bank, by 2020, 1 billion unbanked adults, globally, will have access to a transaction account or electronic instrument to store money, send and receive payments. Financial access is the first step toward broader financial inclusion, where individuals and firms can safely use a range of appropriate financial services, including savings, payments, credit, and insurance.

The role of FinTech, hereby, is to promote transparency, safety, and accountability through a secure, behavioral, cashless, cultural mind-shift in terms of building a financially inclusive world, strengthening the economic and sustainable development. The mobilization of innovative technological, but at the same time humanly-centered, designed applications (primarily mobile) aspires to gradually improve the quality of and access to financial services for the underserved around the globe. Particularly, mobile money and applications of blockchain technology and digital currency in the remittance industry have a very promising potential in terms of providing access to financial services to under- or un-banked populations

www.elsevierdirect.com

Table 18.1: Examples of high-impact innovative financial inclusion channels and platforms that can advance financial inclusion.

Company/ Application/ Platform	Geographic Location	Business Model/Services
Safaricom/M-Pesa	Kenya	Mobile money services (mobile money transfer)
MoneyGram Anglophone Africa	Nigeria	Mobile money services/Trusted money transfer provider
Vemmo	India	Mobile Payment Services/Digital Wallet Service "Share Payments"
bKash	Bangladesh	Mobile money services (money transfers and payments)
Telenor/Easypaisa	Pakistan	Mobile money services (money transfers and payments)
Transfer Banamex	Mexico	Mobile money services (Mobile payments)
Mibanco	Peru	Lending/Microfinance
Musoni (FarmDrive)	Kenya	Lending/Microfinance (Loans to farmers with no formal credit history via mobile phones)
MobiKwik	India	Mobile money services "More than a wallet" and "Simple, Fast, Hassle-Free payments"
CreditMantri	India	Lending/Microfinance (Credit Analysis and Credit Score Online)
L-Pesa	Tanzania	Lending/Microfinance (Microloan for mobile banking customers)
Tala (f.k.a.) Mkopo Rahisi	Kenya	Lending/Microfinance (Instant Mobile Loans Finance App)
First Access	Tanzania	Lending/Microfinance (Automated credit scoring)
Bima Mobile	Africa, Asia, Latin America and the Caribbean	Insurance (Mobile microinsurance) "Creating a world where everyone can access the products and services needed to protect their family' future"
MeraDoctor	India	Insurance "Message a top doctor and solve your health query without leaving home"
TongJuBao	Shanghai	Insurance "Protect each other"/"Trust, Help, Protect"
WorldCover	Ghana	Insurance/Protecting farmers from natural disasters while giving investors diversified returns and direct social impact
Airtel	Uganda	Savings "Make Transactions Between Your Bank and Airtel Money"
M-Shwari	Kenya	Savings/Revolutionary new banking product for M-PESA customers that allows to save and borrow money through phone while earning interest on money saved with M-Shwari, the customer is also entitled to affordable emergency loans
Tigo Pesa	Tanzania	Savings/ Cash-In by depositing money at any Tigo Pesa Agent and Cash-out by withdrawing money at any Tigo Pesa Agent

(Biggs, 2016). Furthermore, this galaxy of applications provides viable solutions to this deficit by harnessing entrepreneurship, innovation, and capital and funneling these resources into strategies for financial inclusion. In this way, capital is used to support underserved populations and finance businesses, enabling innovative and lower-cost business models (Fig. 18.4).

However, financial inclusion cannot be disseminated and scaled up globally, in a responsible and sustainable manner, due to a number of barriers: a) constantly developed technological breakthroughs, along with necessary mobile and online access, IT infrastructures, interoperability, and support mechanisms worldwide; b) financial education and financial literacy in terms of understanding and appreciating the value proposition of these financial applications, easing their adoption; c) various ad hoc regulatory limitations and constraints; and d) cultural considerations and content applicable to different settings worldwide.

The above-mentioned examples (Table 18.1) depict that FinTech is active, to a different extent, across the financial services value chain, providing technology-based solutions and services to financially excluded individuals around the globe, enabling entrepreneurial and innovative business models leading to social value and long-lasting impact.

18.5 Concluding Remarks

The global community is in the process of accepting and adopting innovative financial inclusion models. To that respect, financial inclusion needs to be perceived in a holistic manner and not only from a top-down viewpoint. This requires universal and systematic collaboration in order to develop and build the right financial tools, models, and regulatory policies so as to change the existing financial behavior and enable a dynamic ecosystem for innovative financial inclusion. Especially, from a regulatory point of view, appropriate KYC ("know your customer") transparent and concrete rules, which safeguard financial integrity, are important to be institutionalized (Gelb, 2016). In this frame of reference, financial inclusion shall allow financial health to thrive and develop within a secure and stable framework (Friedline, 2016). FinTech is bound to play an integrative part into the development of radical value propositions and innovative financial services, and products customized for underbanked and unbanked societies (Richardson, 2016). What is important is to understand the end-user and be able to offer directly applicable solutions, carefully designed in order to embrace but also mobilize and further develop the background, education, and technological literacy of the respected customers (Buckley and Webster, 2016). To that respect, financial inclusion shall become the key prerequisite for social and economic development, leading to an unrestricted and universal access to basic financial services.

www.elsevierdirect.com

References

Avlonitis, G.J., Papastathopoulou, P.G., Gounaris, S.P., 2001. An empirically-based typology of product innovativeness for new financial services: success and failure scenarios. Journal of Product Innovation Management 18 (5), 324–342.

Biggs, D.C., 2016. How non-banks are boosting financial inclusion and remittance. In: Tasca, P., Aste, T., Pelizzon, L., Perony, N. (Eds.), Banking Beyond Banks and Money. Springer International Publishing, pp. 181–196.

Bisht, S.S., Mishra, V., 2016. ICT-driven financial inclusion initiatives for urban poor in a developing economy: implications for public policy. Behaviour and Information Technology 35 (10), 817–832.

Buckley, Ross P., Webster, Sarah, 2016. Fintech in developing countries: charting new customer journeys (June 1, 2016). Journal of Financial Transformation 44. Forthcoming; UNSW Law Research Paper No. 2016-73. Available at SSRN: https://ssrn.com/abstract=2850091 [Last accessed: November, 9th, 2016].

Citigroup, 2016. Digital disruption: how FinTech is forcing banking to a tipping point. Citi GPS: global perspectives and solutions. March 2016. Available online at: https://ir.citi.com/D%2F5GCKN6uoSvhbvCmUDS05SYsRaDvAykPjb5subGr7f1JMe8w2oX1bqpFm6RdjSRSpGzSaXhyXY%3D [Last accessed: November, 7th, 2016].

Costanzo, L.A., Keasey, K., Short, H., 2003. A strategic approach to the study of innovation in the financial services industry: the case of telephone banking. Journal of Marketing Management 19 (3/4), 259–281.

Demirgüç-Kunt, A., Klapper, L.F., Singer, D., Van Oudheusden, P., 2015. The Global Findex Database 2014: Measuring Financial Inclusion Around the World. World Bank Policy Research Working Paper (7255).

Frame, W.S., White, L.J., 2004. Empirical studies of financial innovation: lots of talk, little action? Journal of Economic Literature 42 (1), 116–144.

Friedline, T., 2016. Building Bridges, Removing Barriers: The Unacceptable State of Households' Financial Health and How Financial Inclusion Can Help. University of Kansas, Center on Assets, Education, and Inclusion, Lawrence, KS.

Gadrey, J., Gallouj, F., Weinstein, O., 1995. New modes of innovation: how services benefit industry. International Journal of Service Industry Management 6 (3), 4–16.

Gelb, A., 2016. Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to "Know Your Customer". CGD Policy Paper 74, Center for Global Development, Washington DC. Available online at: http://www.cgdev.org/publication/balancing-financial-integrity-financial-inclusion-risk-based-approach [Last accessed: November, 9th, 2016].

Kates, R.W., Parris, T.M., Leiserowitz, A.A., 2005. What is sustainable development? (cover story). Environment 47 (3), 8–21.

Klapper, L., Singer, D., 2014. The Opportunities of Digitizing Payments: How Digitization of Payments, Transfers and Remittances Contributes to the G20 Goals of Broad-Based Economic Growth, Financial Inclusion and Women's Economic Empowerment. A report by the World Bank Development Research Group, the Better Than Cash Alliance and the Bill & Melinda Gates Foundation to the G20 Global Partnership for Financial Inclusion. Prepared for the G20 Australian Presidency August 28th, 2014. Available online at: https://docs.gatesfoundation.org/documents/G20%20Report_Final.pdf [Last accessed: November, 7th, 2016].

MasterCard Insights, 2014. The Road to Inclusion: A Look at the Financially Excluded and Underserved. Knowledge Leadership Report. Available online at: http://www.mastercardadvisors.com/_assets/pdf/MasterCard-Road-to-Inclusion-Report.pdf [Last accessed: November, 7th, 2016].

Mention, A.-L., 2011a. Intellectual capital reporting: an exploratory study on the practices in the banking industry. Journal of Management Control 22 (3), 279–309.

Mention, A.-L., 2011b. Innovation for Financial Services. Innovation Management. Available online at: http://www.innovationmanagement.se/2011/09/13/innovation-for-financial-services [Last accessed: June, 15th, 2016].

Mention, A.-L., Torkkeli, M., 2012. Drivers, processes and consequences of financial innovation: a research agenda. International Journal of Entrepreneurship and Innovation Management 16 (1/2), 5–29.

Oliveira, P., von Hippel, E., 2011. Users as service innovators: the case of banking services. Research Policy 40 (6), 806–818.

Richardson, C.J., 2016. Smartphones, FinTech, and education-helping the unbanked reach financial inclusion. In: Chishti, S., Barberis, J. (Eds.), The FinTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries. John Wiley & Sons, Ltd., Chichester.

Shrier, D., Canale, G., Pentland, A., 2016. Mobile Money and Payments: Technology Trends. MIT. Available online at: http://cdn.resources.getsmarter.ac/wp-content/uploads/2016/08/mit_mobile_and_money_payments_report.pdf [Last accessed: November, 8th, 2016].

Strategy&, 2016. The un(der)banked is FinTech's largest opportunity. DeNovo Q2. FinTech ReCap and Funding ReView. Available online at: http://www.strategyand.pwc.com/media/file/DeNovo-Quarterly-Q2-2016.pdf [Last accessed: November, 6th, 2016].

CHAPTER 19

Inclusive Growth as Democratizing Productivity[1]

Yuwa Hedrick-Wong[#]

Contents

19.1 The Basic Ideas 463

19.2 Inter-Dependency Between Productivity and Inclusion/Exclusion 465

19.3 Inclusive Growth as Democratizing Productivity 468

Notes 470

19.1 The Basic Ideas

The challenge of income inequality is widely recognized as the burning issue of our times, and its political consequences are dramatically highlighted recently by Brexit and the victory of Donald Trump in the US election. Depending on how this challenge is understood, however, the solutions could vary dramatically. At one end of the spectrum, the market economy is perceived as having failed to spread equitably the fruits of economic growth, hence more aggressive government interventions, including income redistribution, are needed. At the opposite end, inept governments, counter-productive and anti-market public policies are to be blamed, and it follows that unshackling market forces will lead to improving income equality.

We see these extremes as dogmatic and unhelpful.

The reality is that the challenge of income inequality is actually a lot more complicated and nuanced, and is embedded in a much deeper puzzle of economic growth. There has been indeed a massive increase in disparity between the rich and the poor, both between countries and within countries. For instance, the ratio of the richest to the poorest country in per capita GDP was about 10 in 1870 (the richest country then was the UK). By 2010, the ratio has risen to over 100 (the richest country being the US).[2] But this is only part of the story.

[#] An abridged version of this paper was published in the US News and World Report, July 6, 2016.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00019-X
Copyright © 2018 Elsevier Inc. All rights reserved.

There has also been a dramatic decline in global poverty in the last 50 years (poverty defined as living on less than US$3 a day at constant 2005 US$). In 1960, about 50% of the world's population was assessed to be living in poverty. By 2011, it has been reduced to only 5%. Admittedly, a significant portion of this reduction happened in China. In the 30-year period of 1980 to 2010, China cut the number of people living in poverty by around 600 million, and it did this indirectly; by building everything from roads to factories to schools to hospitals, and by globalizing its once autarkic economy.[3] But China is certainly not alone; dramatic decline in poverty has also been seen in East and Southeast Asia in the last half a century, and more recently in India and Bangladesh. Indeed, the middle class in the faster growing emerging markets has been the biggest beneficiary of globalization in recent decades.

So there is a puzzle of a simultaneous increase in disparity and a decline in poverty. Why so many people in the world are steadily getting ahead while others are being left further and further behind? Why market forces seem to be working well in some places but not so well elsewhere? And why different localities in the same country could experience dramatically diverse trajectories in economic growth and poverty reduction in spite of having the same macroeconomic policies, institutions, and regulatory regimes at the national level?

This puzzle of economic growth has compelled a deep reevaluation of many conventional theories and approaches, and in so doing, a rethinking of the fundamental constructs of economic growth itself. Expert advice over the last half a century on accelerating economic growth has run the gamut from macro policy prescriptions like the IMF's structural adjustment programs and the so-called Washington consensus, to industrial policy for nurturing infant industries, to more grassroots oriented microfinance and direct assistance to the poor, and to emphasis on investment in education and health, etc. The poor results of this half-a-century efforts have been aptly described by William Easterly as "the elusive quest for growth".[4] However, through a new paradigm of understanding how knowledge and know-how drive productivity, Ricardo Hausmann's more recent pathbreaking work on economic complexity offers a promising alternative to the standard models and policy prescriptions, which in turn provides a new foundation for evolving innovative approaches for tackling inclusive growth.[5]

The research on economic complexity highlights a key feature in today's economic process; the need for economic agents, be they individuals, firms, and even countries, to collaborate in order to be productive. Such collaboration typically takes the form of being connected to a range of vital networks that are powerful enablers for raising productivity. The fact is that modern economic production requires a very large set of complementary inputs. At the most basic level, we need to be connected to networks that supply us with clean water and power, and affordable transportation networks that move us efficiently and affordably, before we can even participate meaningfully in the economy. Then there are the critical networks for accessing information, and for obtaining important services like health, education, banking, and

finance. Many such service networks are also interdependent: if there is no road, then it is very difficult if not impossible to connect to electricity supply, which then means all sorts of appliances, including computers, would not work. There are also the more intangible but no less critical social and professional networks for accessing skills and know-how that reside in people's heads. How well an economic agent is connected to these vital networks determines fundamentally how productive it can be.

The more complex the production, the more is the need for combining know-how that resides in different people, and know-how is qualitatively different from knowledge. Knowledge is codified information that can be readily downloaded and shared in the forms of instruction manuals, text books, software and so on. Know-how, on the other hand, resides mostly in our heads and manifests in our ability to do things. The ability to ski is a kind of know-how, even though most skiers do not have any understanding of the physics of skiing, let alone how the body functions making turns on the ski slope. And the only way we can learn how to ski is to practice it, not by downloading and memorizing a comprehensive analysis of the physics of skiing. So know-how mostly resides in people and cannot be downloaded and easily shared. While both knowledge and know-how are needed in modern economic production, the more sophisticated the production, the more critical is the need to combine diverse and complementary know-how. Since there is a clear limit on how much know-how can be embodied in a single individual regardless of how well-educated and learned she is, combining know-how means connecting people and finding ways for them to collaborate effectively. From an individual perspective, the ability to plug into service networks like finance, education, and information; and people-oriented social, professional, and cultural networks become a critical precondition for increasing productivity.

From this perspective, the poor are poor precisely because they are stuck in low productivity activities. In poor countries workers, micro entrepreneurs, businesses, and even entire industries are often shackled to low productivity operations due to the absence of many of the critical conditions that would have enabled workers to learn new skills and get better jobs; micro entrepreneurs to thrive, small businesses to expand, and bigger firms to finance acquisition of productive assets and to access new and promising markets and customers and so on.

From this perspective, raising the productivity of the poor is the real key to poverty reduction and sustainable growth; and it requires inclusion.

19.2 Inter-Dependency Between Productivity and Inclusion/Exclusion

Conventional approaches to economic development and poverty reduction tend to focus on providing what people, firms, and industries in poor countries need immediately. Typically, poor farmers are provided with tools, seeds, and livestock, microfinance agencies offer loans

to poor households and small businesses; subsidized project loans are provided for industries deemed important for development, and structural reforms are introduced to ease conditions for doing business, and so on. The track record of these approaches is mixed at best, and very often they fail to address the crux of the problem: low productivity.

The most important dimension of productivity is the ability to produce more output with less input, often characterized as efficiency, which is distinct from the more commonly known labor and capital productivity which comes with an increase in these two production inputs. It is in turn critically dependent on generating better ideas of how to do things, and innovative ideas for new ways of doing things that can replace the old, and how such better and innovative ideas can be diffused rapidly to more market participants.[6] Recent and thought-provoking research points to its overwhelming importance in explaining why some countries are rich and others are poor. For example, the GDP per worker in China and India is estimated to be respectively 86.4% and 90.4% lower than the GDP per worker in the US. It turns out that most of the difference (82.9%) in GDP per worker between the US and China is due to China's much lower performance in this critical aspect of productivity compared with the US. And in India it is 67.0%. A similar pattern can be observed across the entire spectrum of developing countries. In one cross-country analysis covering both rich and poor countries, the correlation between GDP per worker and productivity that is based on efficiency and innovative ideas is an almost perfect fit of 0.96.[7]

And we believe that exclusion from any of the vital enabling networks reduces our productivity. Conversely, gaining access to these networks improves our productivity.

Imagine the best brain surgeon in the world being put to work in a village clinic in Sub-Sahara Africa, without a high tech operating room, the ICU with all the advanced medical devices, and teams of professional staff, and alone unsupported by diagnostic laboratory services and associated specialists. Under such circumstances, the very best that this brain surgeon can do is to function at the level of a general practitioner, dispensing basic medicine to patients, but very likely not even that. In other words, her productivity is dramatically reduced if she is confined to working on her own, disconnected from all the vital networks that she needs to function effectively as a brain surgeon.

In contrast, let's look at the example of fresh fruit production to see how productivity jumps from being connected. To be able to grow fruits and sell them to make a living, good knowledge in agriculture is obviously essential. And know-how embedded in the workers in the fruit farm is also important. Knowing when to look out for telltale signs of a plight that may wipe out the crop, based on years of experience, could mean the difference between saving or losing the entire harvest. But if the fruits are sold only locally, the entire operation is relatively simple, and the productivity of the fruit farm, even when profitable, is likely to be relatively modest.

www.elsevierdirect.com

Now think of stepping up the game to export fresh fruits to overseas markets, from rural Kenya to Dubai, for instance. It requires literally a quantum leap in the need of combining a much wider range of know-how. Apart from running the fruit farm successfully, exporting fresh fruits requires cold-storage facilities with reliable power supply, and all the specific know-how embodied in such operations. Then there is the need for efficient freight logistics support and management to get the fruits to Dubai while they are still fresh. Once landed in Dubai, an efficient distribution system has to be in place to get the fresh fruits to the hands of the customers in the shortest time possible. Because we are moving fresh fruits across national borders, we also need efficient customs, backed up by all the necessary know-how in compliance with international sanitary and safety standards and so on. And if the farm aims to export to Europe for even higher prices, then know-how for securing the certification of good agricultural practices (Eurep-GAP) will also be needed. To pay for the costs upfront before payments from customers arrive, the ability to access to trade financing is in turn critical. Should the farm operator be able to access all these vital networks of complementary inputs and know-how, the fresh fruits from her farm can be sold internationally at much higher prices. Another way of putting it is that the very same farm that produces the very same fruits now becomes much more productive because it is now connected to these vital networks of know-how. There is a huge jump in economic complexity from producing fruits to exporting fruits, with a corresponding jump in productivity.

These thought experiments are supported by empirical research. For instance, household surveys from 35 countries show that returns to working experience vary hugely across countries, with poor countries having much flatter age-earning profile.[8] This suggests that in spite of gaining more experience and getting better at what they do, experienced workers in poor countries are less able to move onto more productive jobs with better pay. In other words, the huge potential of raising productivity from deploying the more experienced and skilled workers in positions where they can be more productive is left untapped in poor countries. Obviously, many factors are at work, but there is little doubt that labor market rigidity, poor transportation, and lack of social and economic inclusion are very much at the crux of the problem.

A parallel situation can be found at the level of the firm. In the US, firms get much bigger as they age; firms that are more than 35 years old have eight times the employment than firms in the same sector that are less than five years old. Older firms are those that have survived the test of competition and have evolved to become more productive and efficient; in other words, they are much more productive. And as they expand their employment, they are also creating opportunities for more workers to function at higher level of productivity. In contrast, firms that are over 35 years old in Mexico have only twice the employment of firms that are less than five years old. And in India, there is virtually no difference in employment between

www.elsevierdirect.com

the older and younger firms.[9] Again, evidence points to the lack of social and economic inclusion as the smoking gun. This is also corroborated by research evidence showing the lack of access to financial services in general and credit in particular being a major cause of loss in productivity.[10] Whether it is due to poor infrastructure, labor market rigidity, monopolistic practices, restricted access to finance, collusion of vested interests, or stifling regulations (most likely some combinations of them), innovative micro entrepreneurs and successful firms alike in many poor countries are prevented from growing in size, which reduced their potential growth of productive employment, leading to lower productivity overall in the economy.

19.3 Inclusive Growth as Democratizing Productivity

Through the lens of economic complexity, we can now reinterpret poverty as people being trapped in low productivity activities due to a lack of access to any number of the vital networks that are powerful enablers for raising productivity. We can also address the puzzle of why there has been a simultaneous increase in income disparity and reduction in poverty. The dramatic reduction in poverty that the world has seen in the last half a century came about because hundreds of millions of people who used to live in poverty got connected to many of the vital networks that enabled them to raise their productivity. China is a prime example where rapid improvement in infrastructure, the movement of tens of millions of migrant workers from rural areas to cities, and massive influx of know-how that arrived with foreign direct investment created endless opportunities for poor peasants to get connected to such networks which then dramatically increased their productivity. At the same time, however, many countries, and segments of population within countries, continue to fail to access many of these vital networks for a variety of reasons so they are stuck in low productivity traps. As a result, the distance between the richest and the poorest has continued to grow in spite of massive reduction in poverty.

From this perspective, inclusive growth is all about overcoming barriers of exclusion. Some exclusion is due to the nature of the network itself. For instance, there is a high fixed cost per customer in providing banking and financial services with conventional banking business model, and low income people typically cannot generate sufficient business volumes to justify the fixed cost involved. So they are excluded. On the other hand, many social and institutional networks for connecting people and combining know-how have evolved historically, predating the modern economy, and ancient prejudices embedded in these networks could seriously constrain segments of the population from full participation. Gender bias that is rooted in traditions and cultural practices is one such form of exclusion. And there are many others.

www.elsevierdirect.com

In this context, we can conceptualize inclusive growth as a process of democratizing productivity. Just as citizens in a democracy have a set of participatory rights in choosing their leaders and setting parameters for public policies, inclusive growth means extending basic rights for all to access and participate in the vital networks of services and know-how that are the indispensable enablers of increasing productivity in today's modern economic production. And in order to democratize productivity, we may need to work with governments under certain conditions, and yet to amplify market forces in some other contexts. In fact, governments and markets need to function as complements in order for inclusive growth to succeed. Government regulations are needed to create standards, protect property rights and enforce the rule of law so that markets can operate efficiently. And governments play a major role in the production and protection of what is referred to as public goods: health, education, safety of consumers, and the environment. The bottom line is that markets and governments are complements in inclusive growth, not opposing substitutes.

And the focus on democratizing productivity also means that we need to be flexible and pragmatic, and when necessary deploying different development models adapted to specific circumstances in order to raise productivity for all. In other words, what works well in China may not be appropriate in Africa; and, indeed, what has worked well in China may become counterproductive in the future. Ultimately, seeing Inclusive growth as democratizing productivity allows us to focus on driving growth through higher productivity across the widest possible spectrum of economic agents in a society; with improving income equality as a welcomed result, not as some sacrosanct priority to be realized even at the expense of economic growth.

A final caveat: democratizing productivity is not the same as enforcing an artificially equal distribution of all the necessary inputs and connectivity to every economic agent, even though it may appear more "democratic" on the surface. Just as voters do not have perfectly equal influence on the outcome in the democratic process, democratizing productivity does not mean guaranteeing an outcome of equal productivity for everyone. Instead, democratizing productivity means dismantling barriers of exclusion to create equal opportunities of access and connectivity, even though it is inevitable that some economic agents who are more energetic and enterprising will be able to accumulate more resources and get connected faster and better and becoming more productive than the rest. However, under conditions of inclusive growth (absence of barriers of exclusion), when some parts of the society are enjoying faster growth in productivity than others, a win–win situation results. The more productive segments of the society would generate new opportunities for more productive activities that would benefit even those who are slower moving and less successful, pulling the entire society along. In this regard, democratizing productivity is also the most productive way of improving income equality.

www.elsevierdirect.com

Notes

1. I am grateful to Ricardo Hausmann for reviewing and commenting on an earlier draft of this paper.
2. Angus Maddison, 2001. *The World Economy: A Millennial Perspective*. OECD. IMF WEO data base.
3. Estimates by the World Bank, also see B. Milanovic, 2012. "Global Income Inequality by Numbers: In History and Now – An Overview". World Bank Policy Research Working Paper Series 6259.
4. W.R. Easterly, 2002. *The Elusive Quest for Growth: Economists' Adventures and Misadventures in the Tropics*. The MIT Press.
5. See for example Hausmann, R., C.A. Hidalgo, and S. Bustos, 2013. *The Atlas of Economic Complexity: Mapping Paths to Prosperity*. The MIT Press, Cambridge Mass. And London, UK. For a more physics oriented narrative, see C.A. Hidalgo, 2015. *Why Information Grows: The Evolution of Order from Atoms to Economies*. New York: Basic Books.
6. Technically this dimension of productivity is referred to as "total factor productivity," which is distinct from productivity derived from having more labor or capital. Total factor productivity hinges on how useful information is being shared, and through widespread sharing, reproduces itself in ever more useful new forms. See also Cesar Hidalgo, *ibid.*
7. See evidence assembled by C.I. Jones, "The facts of economic growth". Stanford GSB and National Bureau of Economic Research, working paper draft version 0.4. April 6, 2015.
8. Lagakos, D., Molls, B., Porzio, T., Qian, N. and Schollnian, T, "Experience matters: Human capital and development accounting". *National Bureau of Economic Research Working Paper 18602*, December 2012.
9. Hsieh, C.T. and Klenow, P.J., "The life-cycle of plants in India and Mexico". *Quarterly Journal of Economics*. 129 (3), 1035–1084.
10. Midrigan, V. and Xu, D.Y., "Finance and misallocation: Evidence from plant level data". *American Journal of Economic Review*. February 2014: 104 (2), 422–458. Also see Moll, B. "Productivity loss from financial frictions". American Journal of Economic Review. September 2014: 104 (10), 3186–3221.

www.elsevierdirect.com

CHAPTER 20

Autonomous Finance

Andras Kristof

Contents

20.1 Trust, Accountability and… Autonomy? 471

20.2 Autonomous Organizations 472

20.3 DGD 472

20.4 More Than a Promise 473

20.5 Can't Touch This 473

20.6 Self-imposed, Unbreakable Vow 473

20.7 How The "DAO" Became a Four-Letter Word 474

20.8 The DAO Attack 474

20.9 Are We Ready for This? 475

20.10 A Postmortem 476

20.11 Distributed Autonomous Finance Use Cases 477

20.11.1 Cashless Payments 477

20.11.2 Logistics 477

20.11.3 Corporate Management 478

20.11.4 Patterns and Conclusion 478

Notes 479

20.1 Trust, Accountability and... Autonomy?

The main benefits of using blockchain technology are well known, and have been analyzed in countless articles. Blockchains make things more trustworthy and accountable. Since records can't change and all transactions are stored as long as the chain exists, we can have very high confidence in the validity and accountability of the data that are stored on-chain.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00020-6

Copyright © 2018 Elsevier Inc. All rights reserved.

But in most of the cases we can't say the same about the rules and regulations that handle the data. We can't have the same level of confidence about the algorithms that process our data, or the (financial and other) systems that make decisions based on our data.

Wouldn't it be great if we could have the same level of confidence in our algorithms as well? That they are really doing what they claim to do, and that they are doing neither less nor more than what they are supposed to be doing.

Such systems are called "smart contracts". One of the most well-known and successful projects as of today, implementing a smart contract framework, is Ethereum. Ethereum is a universal purpose blockchain. It has its own programming language, and it can store not only the transaction and account data, but also the decision making rules and algorithms.

The same rules apply to these algorithms as well – the blockchain assures that the code of the algorithms is unchangeable and accountable. This is very good, and might give us the assurances we were looking for. Based on this, sufficiently advanced smart contracts can operate and make decisions without human interaction. But – taking one more small, but very daring step – they can also operate and make decisions where humans are not allowed to interfere.

The distinction between "does not have to interfere" and "not allowed to interfere" makes that last step a revolutionary leap.

20.2 Autonomous Organizations

2016 was the year of the first autonomous organizations. In both cases, the developers deployed the code on Ethereum, and – not surprisingly – both projects implemented a financial use case.

The first successful crowd sale conducted by an autonomous entity was developed and deployed by a Singaporean company, called Digix[1]. For the record, the crowd sale started on 30th March 2016 and was going to end on 28th April 2016. In reality, it ended only a few hours after it opened up, because it hit the maximum amount of 5.5 million dollars.

While it's important to note the dates and the amounts, the real importance lies in *what* was sold and how the money was handled.

20.3 DGD

The crowd sale sold DGD tokens. These tokens had two functionalities. One, holders of these tokens were to benefit from the transaction fees of Digix's actual asset, the gold-backed DGX tokens. Two, token holders were entitled to determine how the money was spent[2].

20.4 More Than a Promise

Note that since the tokens and the entirety of Digix's infrastructure are written in smart contracts and live on the Ethereum blockchain, the promise that the DGD token holders will benefit from the gold token transactions fees is not really a promise, but a verifiable, unavoidable fact. Digix is incapable of breaking this "promise," and DGD holders are incapable of not receiving their shares from the transactions.

20.5 Can't Touch This

But there is more. It's not Digix who received the money, but an account on the Ethereum blockchain that is controlled by a smart contract. In other words, Digix does not have control over the 5.5 million dollars*.

What Digix can do is to make a proposal to this autonomous organization about how they want to spend part of that money. And then the DGD token holders – the very same people who put in their money – can vote whether the proposal shall pass or not.

If it passes, the contract sends the funds to Digix, otherwise the proposal will be denied and no money will be sent out.

20.6 Self-imposed, Unbreakable Vow

This is indeed revolutionary in many levels. The concept of autonomous entities with clear rules and accountable decision-making is very powerful. It extends the strengths of the blockchain from simple transactions to decision-making, governance, and finance.

It promotes honesty and transparency on the organization level. There is no "creative accounting", no hostile takeover, no CEO disappearing with funds. This is a self-imposed restriction that really shows the core values of the company. It benefits the investors without prohibiting the organization from doing anything legal.

Once autonomous systems like this can be deployed easily and they are working properly and reliably, any company not utilizing them will raise eyebrows.

Unfortunately, as we shall see shortly, the system is not working flawlessly just yet.

www.elsevierdirect.com

20.7 How The "DAO" Became a Four-Letter Word

We can safely say that the Digix story – so far – is a success. It proved that it is possible to handle finances in a semi-autonomous way, and that blockchain-based systems can add accountability to traditional processes, like funding, investments, and corporate governance.

Unfortunately not all attempts ended well, and it soon became apparent that – while the idea is solid – the technology might not be ready to handle autonomous finance just yet.

The DAO was a decentralized autonomous organization and a form of investor-directed venture capital fund. Technically, it was a smart contract, written in Solidity and deployed on the Ethereum blockchain.

The code has put a lot of emphasis on autonomy – there was no way to a human to control or withdraw the funds. The funds in the contract had to obey the pre-programmed, unchangeable rules of its own functions. It was meant to be like the Memorandum and Articles of Association of a traditional company.

It was crowdfunded in May 2016, and during the funding phase, it received about USD 150 million dollars' worth of funds, thus setting the record of the largest crowdfunding project in history.

20.8 The DAO Attack

Despite multiple security reviews, the DAO was subjected to a hack that managed to drain most of the funds into a child contract.

On June 17th, 2016, Vitalik Buterin, the creator of Ethereum wrote a blog post, publicly announcing the vulnerability[3].

The same autonomy that was touted to be the strength of the project now became its weakness – there was no permitted way in the DAO smart contract to abort operations and refund the funds. While the funds were not technically lost (they were in a child contract), they could have been withdrawn by the attacker after a 28-day pre-programmed cool-down period.

The exploited bug and the attack are well explained in several places. A very clear explanation is given by reddit user "tweq"[4]:

> *The details are more complicated of course, but basically their withdraw logic looks like this:*

```
function Withdraw(amount) {
   if (yourBalance >= amount) {
       Send(amount)
```

```
        yourBalance = yourBalance - amount
    }
}
```

The problem is that the receiver doesn't have to be just a dumb account, it can be a smart contract in itself whose code is executed by the Send function, and that code can call Withdraw again (calling functions from within themselves is called "recursion"). If that happens, because the sending is done before the balance is adjusted, the executed code effectively looks like this:

```
if (yourBalance >= amount) {
    Send(amount)
    if (yourBalance >= amount) {
        Send(amount)
        if (yourBalance >= amount) {
            Send(amount)
            // and so on...
            yourBalance = yourBalance - amount // this never reached
        }
        yourBalance = yourBalance - amount
    }
    yourBalance = yourBalance - amount
}
```

So you can withdraw the balance you have again and again.

The Ethereum developer community decided to intervene, and changed ("forked") the Ethereum code itself to prevent the loss of funds and make it possible to refund the money to the original investors[5].

This was a very radical step, analogous to changing the working of the Internet itself to prevent a vulnerability in a badly written email client. Or changing the laws of a nation to enable the prosecution of a person who exploited a – previously non-criminalized – loophole in the law.

While the funds were recovered by the original investors, the incident raised a lot of questions and resulted in negative feedback. Among other things, the market cap of Ethereum crashed from USD 2Bn to less than USD 1Bn.

20.9 Are We Ready for This?

The incident obviously raised a lot of moral, legal, and technical questions. We shall not form an opinion on the moral and legal questions, as they are – thankfully – out of the scope of this document.

www.elsevierdirect.com

Admittedly, the technical questions raised by the DAO are quite serious. The two major issues raised by critics were the lack of formal verification for smart contracts, and the lack of testing / modeling tools.

The first issue, the lack of formal verification comes from the fact that the structure of Solidity, Ethereum's programming language – as some critics put it – is more suitable for simple scripting tasks than to write complex contracts that should be immutable and unchangeable.

Let us understand the above claim better. Standard application development is accustomed to go through development cycles. Release, bug fixes, release, bug fixes, etc. On the other hand, one of the great premises of smart contracts is that they are immutable – similarly to "traditional" contracts, they are not supposed to be changed. Since if they can be changed, then the original statements of the contract can be changed and overwritten.

This breaks the traditional development cycle, as smart contracts deployed on a blockchain cannot be changed, not even for bug fixing purposes.

This makes it extremely important to get the code right the first time, and Solidity does not seem to offer the tools to make that easy.

The good thing is that the failure of the DAO highlighted these issues, and several projects sprung up to provide formal verification tools and testing facilities for smart contracts written in Solidity.

So, to answer the question of the paragraph title: We are not there yet, but we are on the right path.

20.10 A Postmortem

The DAO was a great experiment, but it was too early, and was allowed to grow too big. It was too ambitious for its own good, and lacked the security measures to match the finance risks.

The DAO also highlighted the risks of autonomy. First, the right amount and type of autonomy has to be implemented, and second, the technical foundations must be rock solid. Running a project of the scale of The DAO on an experimental platform is very, very risky.

Fortunately, at the end, it did end well. Thanks to the active intervention of the Ethereum developers, the original investors were able to get back their funds.

The community made the best out if this episode, and moved the development of Ethereum and its tools to address the problems highlighted by The DAO.

www.elsevierdirect.com

20.11 Distributed Autonomous Finance Use Cases

Distributed systems, smart contracts offer a varying degree of autonomy, depending on implementation. As we have seen in the previous paragraphs, badly chosen autonomy with imperfect technology can be dangerous.

But if the correct degree of autonomy is deployed, one that matches the underlying business case, then autonomous systems could offer real benefits for various industries.

Below is a list of practical use cases that could greatly benefit from such decentralized autonomous systems.

20.11.1 Cashless Payments

One of the current challenges of telecommunications companies and banks is to get into the business of cashless payments. Telcos already missed several boats, including data communications and the rise of the messenger apps.

Their next challenge is to capture the market of cashless payments. Unfortunately, so far, every attempt by Telcos and banks was just another push to make the market more fragmented – every company comes out with their own wallets and payment systems that are not compatible with each other. No customer wants to have and use several different wallets, and no merchant wants to go through the pain of integrating with a dozen different systems.

Unfortunately, collaboration seems not to be in the cards – nobody wants to give up control and use someone else's system. By using another Telco's or bank's system, they would potentially give up their most important assets, their customer information and spending habits.

A distributed, autonomous payment processing and clearance system could mitigate these concerns. Such system could be co-owned by all industry players and controlled by none; customer information and spending patterns could be provably kept private by the autonomous system.

Transactions could be easily managed by the ledger, and all participating parties would be able to participate in the lucrative part where customers can cash in and cash out from the system.

20.11.2 Logistics

Today's logistics ecosystem is full of inefficiencies. A significant part of the industry is making money by withholding information. And even ignoring that, the logistics companies are suffering from incomplete information and severe underutilization of their assets.

www.elsevierdirect.com

Meaningful cooperation would be beneficial for all honest parties. However, it is highly unlikely for similar reasons observed in the Telco use case. The most prized intellectual properties of logistics companies are their customer base, their routes, their pricing.

Using a 3rd-party system that makes collaboration between companies possible would come with the potential risk of exposing these assets to potential competitors.

A distributed, autonomous system could be deployed to mitigate these risks and foster cooperation at the same time. Such system could be provably unbiased, protect the data of the individual companies, and enable very tight cooperation at the same time.

The system could be written in a way that even the creators of such distributed, autonomous organization would not be able to view the logistics companies' intellectual property.

20.11.3 Corporate Management

There are few areas where more transparency and accountability would be more welcome than in corporate management. There have been several attempts and projects to put company assets (shares, options) on a distributed ledger. That space is well known and the benefits are well understood.

However, with the advent of more intelligent distributed systems, much-needed autonomy could be implemented. The exact time and mode of vesting of options, the precise rules of buying and selling shares could be implemented.

Governance, critical decisions, unbiased enforcements of certain parts of contracts now within reach.

20.11.4 Patterns and Conclusion

Whenever a company is part of an industry, both the company and the industry will benefit from a meaningful collaboration. And – depending on the industry – certain parts of that collaboration can be made autonomous and ruled by strict formulas that protect the good actors of the industry and make fraud more difficult.

Implementation will be different from industry to industry, but the pattern is clear: There is definitely a space for autonomous entities to enrich collaboration and protect vital information at the same time.

Notes

1. digix.io homepage.
2. Digix whitepaper: https://dgx.io/whitepaper.pdf.
3. Vitalik Buterin announces the DAO vulnerability: https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.
4. Reddit user "tweq" explains the DAO exploit: https://www.reddit.com/r/Buttcoin/comments/4omhp1/eli5_the_dao_hack/?st=iva34a70&sh=ea2d847a.
5. Ethereum hard fork announcement: https://blog.ethereum.org/2016/07/20/hard-fork-completed/.

www.elsevierdirect.com

CHAPTER 21

Inclusion or Exclusion? Trends in Robo-advisory for Financial Investment Services

Roland Schwinn[#] **, Ernie G.S. Teo**[##]

Contents

21.1 Introduction 481

21.2 Robo-advisors 483

CASE 1: Betterment (Largest Independent Robo-advisor Platform) 484

CASE 2: MarketRiders (International Semi-automated Robo-advisor) 485

CASE 3: 8Securities (1st Robo-advisor in Asia) 486

21.3 Discussion: What Is the Future of Robo-advisors? 488

21.3.1 Scalability and Geographical Distribution 488

21.3.2 Product Mix (Availability and Acceptance) 489

21.3.3 Customer Demographic 489

21.3.4 Other Industry Trends: Social Trading Platforms 490

21.4 Conclusion: Inclusion or Exclusion? 490

References 491

Notes 492

21.1 Introduction

Before electronic trading, orders were placed manually by calling brokers on the phone. The trades were then executed on trading floors. The entire process could take days to confirm and

[#] Executive Director, Eurex (Deutsche Börse Group) and CEO, Eurex Clearing Asia Ltd. (Deutsche Börse Group).

[##] Research Scientist, IBM Research, Singapore.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00021-8
Copyright © 2018 Elsevier Inc. All rights reserved.

were expensive and cumbersome, making stock trading an exclusive affair to the privileged few. With the advancement of Internet technology, this soon changed. Brokerages were quick to adapt with electronic communications networks (ECNs) being used as early as 1967 with the birth of Instinet,[1] the first off-exchange trading platform designed to compete with the New York Stock Exchange (NYSE), this marked the beginning of automated financial markets (Kunz and Martin, 2015). The Securities and Exchange Commission defines ECNs as "electronic trading systems that automatically match buy and sell orders at specified prices" (SEC, 2013). Going electronic improved efficiency, Barclay et al. (2001) show that increased trading on ECNs improves most measures of overall market quality.

The next milestone was in February 8, 1971 when the National Association of Securities Dealers Automated Quotations (NASDAQ) began trading as the world's first electronic stock market for over 2500 securities (Terrell, 2010). "In August 2002, ECNs accounted for approximately 40 percent of volume in NASDAQ securities… Several ECNs are currently registered in the NASDAQ system (such as)… Bloomberg Tradebook and Instinet" (Hendershott, 2003).

The innovation that finally brought stock trading to the masses was retail trading platforms. In 1985, Trade∗Plus started offering one of the first retail trading platforms on America Online and Compuserve (History of Online Stock Trading, 2010). Several others such as TD Ameritrade soon followed. The NYSE census in 1952 revealed that only 6.5 million Americans owned common stock (about 4.2% of the U.S. population). By 1990, this increased to around 51 million (more than 20% of the U.S. population) (Investopedia, 2008).

Electronic trading not only created efficiency but also created inclusion, allowing for more people to own stocks. As competition heats up with the increasing number of platforms, commissions were lowered and more participated in the stock markets. "An advisory group reported that the number of online brokerages in US jumped from 12 in 1994 to more than 140 by the end of 2000" (History of Online Stock Trading, 2010). Fink et al. (2006) show that ECN has the following effects on the NASDAQ: tighter quoted, effective, and relative bid-ask spreads, greater depths, and less concentrated markets. Their results also show that an increase in ECN trading may have caused some traditional market makers to exit the market, a sign of the disruptiveness of technology.

In the mid-1990s, the first online brokers introduced intraday trading, which allowed individuals to make use of short-term market movements during the day. Being offered access to real-time market data, private individuals were enabled to trade like professionals for the first time. The so-called "Day Trader" was born.

With the intense rivalry, online platforms realize that to increase and retain business, they should offer investors an advantage through information/education. The more successful an

investor is in trading on a platform, the more likely he is to put more money in and continue using it and generating commissions. This led to the provision of tools to aid in researching and selecting investments, such as charting software, technical analysis tools, and online trading front-ends. Platforms streamed prices live and execute orders in near instances.

Online trading experienced an enormous boost during the dot.com bubble, starting in the late 1990s and coming to a more or less abrupt decline with the crash in 2001/2002. A lot of investors got burned, lost fortunes, and stayed away from actively speculating stock markets.

Later with advancing technology, the provision of high frequency market data became important as traders aimed to beat the herd. With the advent of computers, some electronic platforms also opened APIs and created scripting tools to allow the development of algorithmic trading systems. Due to the high costs of technical infrastructure needed for the large amount of computational power and sophisticated market data required low latency trading remained to be the domain of professional trading firms.

The experience of the dot.com crash made individual investors rethink their participation in actively trading financial markets. Despite investing into other more tangible asset classes like real estate (also fueled by low interest rate environments), the mutual fund industry saw impressive growth rates as investors went back to more passive investing. In particular, Exchange Traded Funds (ETFs) experienced significant growth, as they were cheaper and easier to buy and sell. According to BlackRock statistics, global ETF's assets under management (AUM) grew from about 770 billion USD at the end of 2008 to 2.96 trillion USD at the end of 2015 (BlackRock, 2016). It is estimated that global AUM has reached 3 trillion USD in 2016 and according to a PWC survey 41% of the survey participants expect AUM to grow between 7 and more than 10 trillion USD by 2021 (PWC, 2016).

21.2 Robo-advisors

The first robo-advisors were introduced after the 2008 financial crisis, these were mainly passive automated asset allocation and portfolio management platforms using ETFs which automatically rebalance when market shifts skews the portfolio. This came at a time when investors preferred a lower risk portfolio and stability but were at the same time fearful of financial shocks.

Robo-advisors are changing the way people invest, as most start-ups in the industry target investors that are currently underserved. In the following sections, we will explore robo-advisors in detail, giving an overview of the ecosystem, its evolution and discuss a few notable industry cases. In the final section, we analyze future trends in the industry and consider the role of robo-advisors in creating an inclusive investing environment.

www.elsevierdirect.com

Robo-advisors can be defined as a type of financial advisor that provides web-based portfolio management with almost zero human intervention. These online advisors typically use algorithms and formulas (SWFI, 2015). Before the availability of robo-advisors, investors who cannot afford it did not have access to personalized investment advice (Lieber, 2014). This changed after the 2008 financial crisis, the low interest rate environment post-crisis, and thin returns of active asset management at relatively high costs, which led to investors shifting from active to passive investment management such as index tracking funds and ETFs. It was in this period when ETFs saw the strong growth, mainly in the US and in Europe. This created demand for a more automated and cheaper approach to portfolio rebalancing and management, which drove innovation in the industry and led to the introduction of services like Wealthfront and Betterment. As these gained popularity, established asset managers and brokers such as Charles Schwab, Vanguard, BlackRock, Goldman Sachs, and Merrill Lynch joined the game. In 2014, U.S. robo-advisor services managed $16 billion in assets. By the end of 2015, that had jumped to $50 billion (Collins, 2016). We can categorize robo-advisors into two types:

- independent start-ups like Betterment and MarketRiders,
- robo-advisory platforms of established investment companies like Fidelity Go or Future Advisors of Blackrock.

While some of the independent start-ups liaise with larger distribution partners, the platforms of established investment firms extend the existing distribution capabilities. In a bid to differentiate themselves, many start-ups started to enter the market using algorithms like the Black–Litterman[2] asset allocation model for portfolio allocation and rebalancing to provide robo-advise, while some also added market sentiment data to their respective algorithms. Some run their own accounts and others use international partners such as Interactive Brokers to host their clients' portfolios.

Due to domestic regulations with regard to investor protection and compliance related requirements such as KYC (know your customer), most robo-advisors only offer their services restricted to a particular country or region. So far, this resulted in most robo-advisors being strongly US focused and limited to US investors. There are however some advisors that allow investments for international clients. In the next section, we examine three case studies of robo-advisors with varying regional coverage and different business models.

CASE 1: Betterment (Largest Independent Robo-advisor Platform)

Betterment was launched in 2010 by founder John Stein. When first pitched to investors, many felt that the product was too simple to use and felt like a toy (Stein, 2016). Betterment

challenged the way that people viewed financial system and set out to build a product that met the needs of investors.

With over 175,000 customers and more than $5 billion in assets under management, Betterment is (as at July 2016) the largest independent robo-advisor Internet platform (Stein, 2016). Betterment boasts one of the lowest costs in the market, charging 0.35% per year for accounts under $10,000. Like most other robo-advisors, they offer flexibility for their customers with open-ended ETFs, which carry no restrictions around issuing or redeeming shares (Gardon, 2015).

Betterment offers customized portfolios for wealth building, retirement planning and other saving goals. The customer's portfolio composition is initially based on parameters like age, retirement timeline, annual income, and investment goals. The on-boarding process is fully automated and provides the applicant transparency about the proposed portfolio allocation. Portfolios are automatically reweighted on an ongoing basis (Lotich, 2016). Another feature is the automated reinvestment of dividends and yields, which are allocated across the portfolio.

Betterment's services target long-term passive investors with a basic understanding of financial markets and portfolio allocation. In addition, the high degree of automation and low-cost engine also make Betterment suitable for those with little or less financial education, who have realized the importance of retirement savings and also understand the cost advantage compared to traditional investment plans.

The success factors of Betterment are clearly its low-cost investment service offering, which is completely automated for the investor, starting with an efficient onboarding process without long KYC questionnaires. In addition, it provides a high degree of transparency and no long-term tie-up compared to some traditional investment plans to the investors. According to CEO Jon Stein (CB Insights, 2016, July 6), their most successful marketing tools are mouth-to-mouth referrals. The majority of its customers have around 100k USD of net worth; High Net Worth investors have not picked up the services yet as desired.

Being a robo-advisor restricted to US customers only, Betterment's features are customized towards the US market such as Tax Loss Harvesting+[3] and RetireGuide,[4] both of which consider US tax implications. This customization benefits its customer base but also limits its market to the United States. The next case study looks at MarketRiders which works with international distribution partners to reach global customers.

CASE 2: MarketRiders (International Semi-automated Robo-advisor)

MarketRiders, founded in 2007 by M. Tuchman, St. Beck and R. Pfenninger works on a subscriber model and, so far, has supported investors to build up more than 15,000 portfolios

valued at more than 5 billion USD (MarketRiders, 2007). Compared to Betterment, MarketRiders targets the more active investors, by offering a platform which only recommends an optimal portfolio composition based on similar attributes like age, investment goals, portfolio lifetime, risk appetite, and available assets. The proposed portfolio composition is then to be executed by the clients themselves.

MarketRiders clearly set on reducing cost for investors by also using ETFs as investment products. The services offered can be used with any brokerage account, but they have set up a network of preferred partners, which includes Charles Schwab, Sogotrade, Ameritrade, Fidelity, and Vanguard. Some of these firms offer commission-free ETFs, which are considered when MarketRiders optimizes a customer individual allocation proposal.

Collaborating with those international distribution partners also allows MarketRiders to reach out to a global customer base, as one of the few robo-advisory firms being able to do so. Accounts are held with firms like Ameritrade as the broker, so all regulatory and compliance related matters such as KYC are already taken care of at the brokerage level and relieve MarketRiders with those complex and cost intensive issues.

MarketRiders also offers more flexibility in terms of rebalancing to their clients, as the risk parameters can be modified by the investor resulting in modified allocation proposals. Compared to other advisors, investors can then react by trading the position adjustment themselves. The platform offers additional tools to observe and analyze the portfolios, but in particular brokerage fees. Another feature is the educational offering including articles and also webinars.

The product offering of MarketRiders is wider too, also including for example gold ETFs and REIT ETFs. The fee model is subscription based, where the clients can choose between an annual or monthly fees.

The lack of automated execution with MarketRiders does not put it into the category of the fully automated robo-advisors. As the investor does the trade execution by himself, the business model of MarketRiders offers more flexibility to the more educated investor, while aggressively promoting ETFs as cost-efficient investment instruments.

CASE 3: 8Securities (1st Robo-advisor in Asia)

In Asia, the investment industry is still highly fragmented due to individual regulatory environments of each country. This is particularly with regard to private investor protection, know your customer (KYC), and compliance restrictions. Compared to western markets, the acceptance of ETFs is still lagging behind in most of the Asian countries, as banks and wealth managers still prefer to offer high-margin unit trusts or structured notes to their clients. Global

assets under management (AUM) for ETFs are currently estimated to be at 3 trillion USD in 2016 (Voros, 2016, April 12). The United States is estimated to account for 70% of that, whereas the Asia-Pacific ETF industry is estimated to reach 250 billion USD AUM in 2016 (up from 165 billion USD in 2014) (BNY Mellon, 2014, December 5).

According to Rex Wong, MD of BNY Mellon, Hong Kong and China account for about 35% of the AUM in Asia-Pacific, while Japan is accounting for about 45% (BNY Mellon, 2014, December 5). Markets like Taiwan are seeing a strong growth in ETFs as well, AUM growing by almost 40% from 2014 to 2015, from 4.4 billion USD to 6.5 billion USD (Taiwan Stock Exchange, 2016, February 05). Even though Asia is still lagging behind the global AUMs, the strongest growth rates for ETFs are expected in this region, with estimates varying between 15 and 30% p.a.

The low adoption rate of ETFs (so far) in turn affects the size and growth of the robo-advisory industry in Asia. However, there are still some leaders in this region. Hong Kong, Singapore, and Japan are the pioneer markets of this industry in the region.

8Securities is the first robo-advisor in Asia. Started in Hong Kong by founders Mathias Helleu and Mikaal Abdulla, 8Securities was launched in 2012 (with $8 million in funding) as a trading platform with multiple trading tools such as access to news and social media built into the platform (Wee, 2012, March 21). It is licensed in Hong Kong under the Securities & Futures Commission and in Japan under the Financial Services Agency. It entered the Japanese market in May 2014 and two months later launched a wealth management service which acts as a simple tool to create an automated, customized portfolio (Quigley, 2014, May 19). 8Securities' Autoportfolio service is directed at passive investors who prefer to just make a deposit and not be actively involved in managing the portfolio. Users just need to complete a quick survey and it determines the allocation, period of investment, and a risk versus reward ratio. The portfolio then manages itself.

A social trading portal was also introduced as an opt-in service. If chosen, all transactions made can be seen by other users. As explained by Mikaal Abdulla: "If I want to receive a push notification to my mobile phone when more than five investors place a buy order for Apple shares, its now possible. Our big data engine will allow customers to see virtually any piece of data they wish across individuals, stocks, geography and time horizon. Unlike social trading mobile apps or bulletin boards, we have combined the social interaction and the actual trade." (Quigley, 2014, May 19).

By September 2014, the social trading dashboard has had over 20,000 actively trading accounts and managed around US$800 million of assets, mostly in Japan. After Japan, the next market which 8Securites targeted was China, where the strategy was to be a first mover of sorts and enter the market as a trading simulation until regulatory permission is obtained to

www.elsevierdirect.com

launch as a trading platform (Bischoff, 2014, September 04). In April 2016, the platform announced that its customers can trade over 15,000 US, HK, and China H shares and index funds for $0 commission (Fox, 2016, April 27). Soon after, it also moved to lower its robo-advisory fees to attract more cost-sensitive investors (Wong, 2016, August 4).

In August 2016, 8Securities announced Asia's first robo-advisory app named "Chloe"; the app is "powered by artificial intelligence (AI) and machine learning technologies developed in-house, Chloe will learn day-by-day as its user base and database grow to optimize goal-setting and portfolio matching for customers with different financial needs" (finews.asia, 2016, August 1). In the same period, 8Securities also announced that they are seeking regulatory approval to launch in Singapore by end of 2016 (Chia, 2016, May 24).

Compared to the first two cases, 8Securities' product offerings are more varied, providing users with more tools and information to base their investment on. Being based in Asia, its geographical strategy is to move into one market at a time, expanding its reach from Hong Kong to Japan, China, and Singapore.

The three examples of robo-advisors above demonstrated significantly different business models with different target groups and distribution reach. The case studies give some insight into the current business models of robo-advisors and by no means represent the entire industry.

It is expected that future service offerings will be determined by the targeted investor groups and investor's demand based on the respective geographical distribution region. In the next section, we look into additional influencing factors that could shape future developments.

21.3 Discussion: What Is the Future of Robo-advisors?

The future trends of robo-advisors will be affected by a few factors. As with most fintechs, **scalability** is an important issue. For most robo-advisors, scalability is limited by regional regulations. **Product mix** is currently limited to most ETFs and is also an area which robo-advisors need to consider to expand their reach. **Customer base** is another concern, tech savvy millennials tend to be the target market of robo-advisors but this demographic has limited wealth. To become sustainable, robo-advisors should also consider capturing the attention of High Net Worth Individuals (HNWIs). We discuss each of these factors in detail below.

21.3.1 Scalability and Geographical Distribution

Currently most robo-advisors (such as Betterment) limit their service offering to domestic regulatory environments like the US. This goes back to investor protection regulation, compliance requirements and also taxation rules. Although the US is one of the largest global

consumer markets and has huge growth potential, limiting to a single market does not allow for economies of scale and scope in making full use of the scalability of infrastructure and partnerships.

In markets like Asia, with a high degree of fragmentation, the respective market potentials are even facing stronger restrictions, as every country has its own regulatory framework. To achieve a complete global scalability, those restrictions limiting the distributions capabilities need to be overcome.

21.3.2 Product Mix (Availability and Acceptance)

In US and Europe, the rise of cost-efficient investment products like ETFs has resulted in a broad investor's acceptance and thus deep liquidity in most ETFs. In Asia the degree of penetration of ETFs is still low and at an early stage compared to the US and Europe. Thus, a wide breakthrough of ETFs triggered by customer demand is key for the rise of robo-advisors in Asia.

For the more developed markets like Europe and US, we might see further diversification into other asset classes like ETCs (exchange traded commodities), foreign exchange products, REITS (real estate investment trusts), and maybe even cryptocurrency products beyond the classical and more conservative equity and fixed income allocation.

21.3.3 Customer Demographic

As the Betterment case shows, most of the investors of a typical robo-advisor account for a net worth of up to 100k USD, millennials make up a large proportion of these investors. According to Betterment CEO Jon Stein (CB Insights, 2016, July 6), the firm has only one customer with a portfolio of 10mil USD with the advisor. This example shows that fully automated robo-advisors still seem to struggle to attract affluent investors including HNWIs.

Although millennials have strong affinity towards mobile services and automation, they typically lack significant amounts of assets available for investments. In contrast, HNWIs (with higher amounts of assets available) tend to demand individual high quality personal advisory. The robo-advisors currently serving the smaller investors need to come up with additional attractive service offerings to tap into the wealthier pools of investors.

This might result in more hybrid robo-advisors, adding human advisory in addition to the fully automated services or in advisors targeting more exclusively on HNWIs with additional high quality advisory through human interaction.

www.elsevierdirect.com

21.3.4 Other Industry Trends: Social Trading Platforms

Social trading is an emerging trend which robo-advisories may consider to add as part of their services. As seen in our case study above, 8Securities has already implemented a social element on their platform.

The growth of online trading in the 1990s using the Internet also allowed for the easy sharing of information. Back then, individual traders would track and exchange trade gossip within their own physical networks or trading forums or discussion boards or follow some successful traders' or analysts' strategies in news columns. With the rise of social networks, this has since moved online with bulletin/discussion boards to blogs and to social media. Social trading platforms then emerged, where traders' personal accounts and actions can be recorded for reference to other traders. This provided a new way to analyze financial data by allowing traders to compare and copy trades and strategies. Social elements can provide a value added for investors (especially on non-fully automated platforms), peers' actions can prove to be a useful reference point in making decisions.

21.4 Conclusion: Inclusion or Exclusion?

The expansion of robo-advisory platforms and their acceptance by individual investors clearly contributes to financial inclusion and helps generate level playing fields. The platforms enable private investors to have access to a large portfolio of cost effective financial instruments – mainly ETFs – covering global multi-asset classes. Those products are not easily accessible by a lot of private investors everywhere, particularly in the less developed financial retail mass markets, as cost-efficient products are not being (actively) offered to the ordinary customer by many retail banks. Robo-advisors also bring customized financial advice on an automated basis to the masses. So far, customized advice was mainly available to the more affluent or high net worth investors. For the less developed retail financial investment markets in Asia, the degree of inclusion will be even higher with a growing penetration of ETF products and robo-advisors.

Also, savings in investment cost will contribute to inclusion of the unserved or less served and thus generate better returns, as well as an increase in awareness of the importance of retirement savings for private individuals fueled by the expansion of robo-advisors.

In conclusion, the technological trends in the industry could allow more people (especially younger individuals with low net worth) to enter the market but they could also exclude the less tech savvy. How the industry could develop remains to be seen, as new and innovative methodologies are incorporated into robo-advisory services and the global economy evolves.

References

Barclay, M.J., Hendershott, T., McCormick, T., 2001. Electronic Communications Networks and Market Quality. Simon School of Business Working Paper No. FR 00-19.

Bischoff, P., 2014. Social wealth management startup 8Securities builds trust in Japan, sets eyes on China. Retrieved October 28, 2016, from Tech In Asia, https://www.techinasia.com/social-wealth-management-startup-8-securities-builds-trust-japan-sets-eyes-china-startupasia-arena.

BlackRock, 2016. Growing use of ETFs. Retrieved October 31, 2016, from iShares by Blackrock, https://www.ishares.com/us/about-etfs/what-is-an-etf/growing-use-of-etfs.

BNY Mellon, 2014. Asia-Pacific ETF assets under management could reach US250 Billion by 2016 says BNY Mellon. Retrieved October 31, 2016, from https://www.bnymellon.com/us/en/newsroom/news/press-releases/asia-pacific-etf-assets-under-management-could-reach-us250-billion-by-2016-says-bny-mellon.jsp.

CB Insights, 2016. Jon Stein, CEO of betterment: "We made investing easy and delightful". Retrieved October 28, 2016, from https://www.cbinsights.com/blog/fintech-customer-acquisition-costs-robo-advisors-betterment/.

Chia, Y.M., 2016. Commission-free stock trading by year-end? The Straits Times. Retrieved from http://www.straitstimes.com/business/invest/commission-free-stock-trading-by-year-end.

Collins, M., 2016. Robo-Advisers. Retrieved October 22, 2016, from Bloomberg Quicktake, https://www.bloomberg.com/quicktake/robo-advisers.

finews.asia, 2016. Hong Kong Robo-Advisor set to Democratise global investing. Retrieved October 28, 2016, from http://www.finews.asia/finance/22726-robo-advisor-fintech-asia-8-securities.

Fink, J., Fink, K.E., Weston, J.P., 2006. Competition on the Nasdaq and the growth of electronic communication networks. Journal of Banking & Finance 30 (9), 2537–2559.

Fox, M., 2016. Hong Kong financial technology startup 8 Securities launches $0 commission trading. Retrieved October 26, 2016, from https://www.leaprate.com/2016/04/hong-kong-financial-technology-startup-8-securities-launches-0-commission-trading/.

Gardon, M., 2015. How betterment won my retirement account. Retrieved October 25, 2016, from The Simple Dollar, http://www.thesimpledollar.com/how-betterment-won-my-retirement-account/.

Hendershott, T., 2003. Electronic trading in financial markets. IT Professional Magazine 5 (4), 10.

History of Online Stock Trading, 2010. Retrieved September 12, 2016, from http://www.stock-trading-warrior.com/History-of-Online-Stock-Trading.html.

Investopedia, 2008. Stocks then and now: the 1950s and 1970s. Retrieved September 12, 2016, from http://www.investopedia.com/articles/stocks/09/stocks-1950s-1970s.asp.

Kunz, K., Martin, J., 2015. Into the breech: the increasing gap between algorithmic trading and securities regulation. Journal of Financial Services Research 47 (1), 135–152.

Lieber, R., 2014. Financial advice for people who Aren't rich. The New York Times. Retrieved from http://www.nytimes.com/2014/04/12/your-money/start-ups-offer-financial-advice-to-people-who-arent-rich.html?_r=0.

Lotich, B., 2016. A look at betterment: the easiest way to begin investing. Huffington Post. Retrieved from http://www.huffingtonpost.com/bob-lotich/a-look-at-betterment-the-_b_12529626.html.

MarketRiders, 2007. About MarketRiders. Retrieved October 31, 2016, from http://www.marketriders.com/about.

PWC, 2016. ETFs: a roadmap to growth. Retrieved from http://www.pwc.com/us/en/asset-management/investment-management/publications/assets/pwc-etfs-growth-roadmap.pdf.

Quigley, J.T., 2014. 8Securities, an online platform that makes stock trading transparent, launches in Japan. Retrieved October 28, 2016, from Tech In Asia, https://www.techinasia.com/8securities-seeking-us5m-series-launches-japan.

SEC, 2013. Electronic Communication Networks (ECNs). Retrieved September 12, 2016, from https://www.sec.gov/answers/ecn.htm.

Stein, J., 2016. The history of betterment: how we started a company that changed an industry. Retrieved October 25, 2016, from Betterment.com, https://www.betterment.com/resources/inside-betterment/our-story/the-history-of-betterment/.

SWFI, 2015. Everyone wants a Robo-Advisor, right? Retrieved October 22, 2016, from http://www.swfinstitute.org/swf-article/everyone-wants-a-robo-advisor-right-8461344//.
Taiwan Stock Exchange, 2016. ETF AUM and Trading Reach New High. Retrieved October 31, 2016, from http://www.tse.com.tw/en/about/press_room/tsec_news_detail.php?id=18258.
Terrell, E., 2010. History of the American and NASDAQ stock exchanges. In: Library of Congress–Business Reference Services.
Voros, D., 2016. Global ETF assets top $3 Trillion. Retrieved October 31, 2016, from ETF.com, http://www.etf.com/sections/features-and-news/global-etf-assets-top-3-trillion.
Wee, W., 2012. After 18 Months and $8 Million Funding, 8 Securities Finally Launches Publicly. Retrieved October 28, 2016, from Tech in Asia, https://www.techinasia.com/8-securities-launches.
Wong, I., 2016. ETF robo-adviser to launch in Hong Kong. Retrieved October 28, 2016, from International Adviser, http://www.international-adviser.com/news/1030761/etf-robo-advisor-launch-hong-kong.

Notes

1. The first packet switching networks like Telenet were only developed in the late 1960s.
2. http://www.blacklitterman.org.
3. https://www.betterment.com/resources/research/tax-loss-harvesting-white-paper/.
4. https://www.betterment.com/retirement/.

CHAPTER 22

How 3D Printing Will Change the Future of Borrowing Lending and Spending?

Abhijit Patwardhan

Contents

22.1 History of 3D Printing 494

22.2 The 3d Printing Landscape 494

22.2.1 The 3d Printing Process 495

22.2.2 Materials for 3d Printing 497

22.2.3 Enablers to Accelerate Adoption 497

22.2.4 Applications 498

22.3 The Future of Spending by Consumers, Businesses and Governments? 503

22.3.1 Consumers 503

22.3.2 Commercial or Businesses 505

22.3.3 Government 511

22.4 The Future of Borrowing and the Risks of Lending 515

Notes 518

"Give me a place to stand and a lever long enough and I will move the world"
Archimedes, a Greek mathematician (3rd century BC)

Technologies like IoT, Big data, 3d printing are levers made of silicon chips and electronic circuits[1] that will have a profound effect on people, businesses, and Governments around the world. Let's take a trip through this landscape, appreciate the history, understand its denizens, and take a look at the future through their eyes.

Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2
DOI: 10.1016/B978-0-12-812282-2.00022-X
Copyright © 2018 Elsevier Inc. All rights reserved.

Millions of personalized hearing aids are 3d-printed in the US today. The FDA recently approved a 3d-printed prescription tablet for consumer use. A British start-up 3d-printed a Swarowski studded prosthetic arm for Grace Mandeville, a YouTube star.

3D printing is changing our world in a myriad of ways. Sometimes it is disruptive and disturbing and at other times gradual.

Wohlers, a leading research agency on 3d printing estimates that the industry will *quadruple* to $12bn in just 2 years.

22.1 History of 3D Printing

Additive Manufacturing (AM) started in 1984 when Charles Hull invented a "layer by layer" printing process (stereolithography) to create an object from a digital file. The term "3d printing" was coined in the 2010s by the media and has now become the popular vernacular for consumers and the maker community.

Through the 1980s 3d printing was used for prototyping. Over the years, technological development led to cheaper printers offering better quality output.

The 1990s was the decade of rapid tooling. 3D printing was used to make jigs and fixtures and molds faster and cheaper than the traditional processes. Where a traditional mold would take 3–4 weeks and thousands of dollars to make, a 3d-printed one could be made within a week at far lower costs.

The 2000s made 3d printers more affordable for home with prices dropping below US$500. The cheapest printer from a major manufacturer XYZ printing is available on Amazon at US$295. Although printer prices have dropped dramatically in two years, 3d printers are still not as easy to use as your 2D printer for the average consumer. Early adopters like tinkerers, engineers, and hobbyists find them to be extremely useful and tend to print a lot of objects.

22.2 The 3d Printing Landscape

The 3d printing landscape is typical of a high growth sunrise industry, heavily fragmented with very few large players (Fig. 22.1). Stratasys and 3D Systems are the largest incumbents with a global footprint. Apart from them, there are hundreds of small to very small local or regional players across the world. To put it in perspective, 3D Systems (DDD), the largest player, has a market capitalization of $2bn (Sept. 30, 2016) compared to hp(HPQ) at $26bn.

All 3d printer manufacturers alike are in a race to offer "Faster, Cheaper and Better" i.e. *"Faster and Cheaper"* printers producing *"Cheaper and Better Quality"* prints.

www.elsevierdirect.com

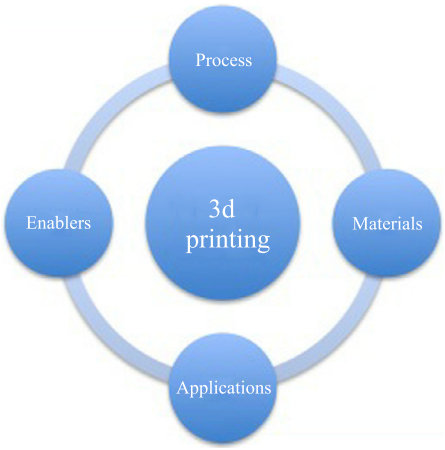


Figure 22.1: The 3d printing landscape.

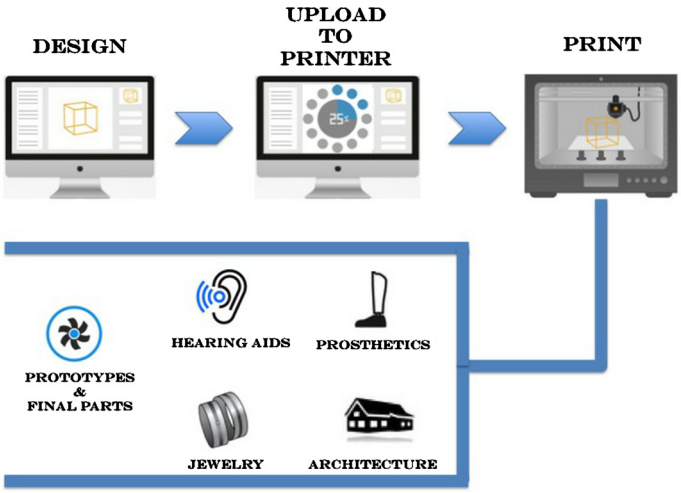


Figure 22.2: The 3d printing process.

Global spending on printers is forecasted to rise to 27bn by 2019, according to IDC, a leading market research firm. US and Europe drive this demand. The technological adoption in Asia (apart from Japan) is lagging behind the first world economies.

22.2.1 The 3d Printing Process

(See Fig. 22.2.)

Step 1 – Digital Design or Capture – There are multiple ways to capture a design.

1. A 3d digital design file is made for an object using 3d Design software like Google Sketch Up, Onshape, Solidworks and Autocad. Google Sketch Up and Onshape are easier to use and targeted at the novice user. Solidworks and AutoCAD are used more by professionals.
2. 3D scanners or phone-based apps are also used to scan objects and convert them to 3d files.

Step 2 – Upload to printer or Design File processing – The 3d files are made print-ready and then uploaded to your home printer or to an online printing service like Shapeways, Sculpteo, 3d Hubs, etc.

Step 3 – 3d Print Post-Processing – The printout is cleaned and finished as per requirement. Post-processing finishing involves removing excess material, sanding to a smooth finish, painting, lacquering with varnish and mounting.

In the 2d printer world, most printers use either inkjet or laserjet technology. In the 3d printer world, most 3d printers are typically based on seven primary technology processes:[2]

1. Vat photo-polymerization – A liquid photo polymer (i.e. plastic) in a container is cured by light. Also referred to as SLA (Stereolithography) and DLP (Digital Light Processing).
2. Material jetting – This process is similar to a 2d inkjet printer. The printhead deposits materials in droplets and a UV light cures or hardens the material. Also referred to as MJM (Multi Jet Modeling).
3. Material extrusion – This is the most prevalent of all the 3d printing processes. Plastic wire is fed into a heated print head and then extruded (quite like pasta) onto a build platform. Also referred to as FDM (Fused Deposition Modeling).
4. Powder bed fusion – A layer of material powder is deposited on the built platform and a laser is used to fuse the particles together. Also referred to as EBM (Electron Beam Melting), SLS (Selective Laser Sintering) and DMLS (Direct Metal Laser Sintering).
5. Binder jetting – This is similar to powder bed fusion except that a liquid binding agent is used instead of a laser. Inks can also be deposited to get a full color print.
6. Sheet lamination – Thin sheets of material are fused together using glue or ultrasonic welding. A laser or a knife is used to cut away the unnecessary material and form the object. Also referred to as LOM (Laminated Object Manufacturing) or UC (Ultrasonic Consolidation).
7. Directed energy deposition – Focused thermal energy is used to fuse material (usually metal) as it is being deposited.

www.elsevierdirect.com

22.2.2 Materials for 3d Printing

The table below shows the range of materials that are used in 3d printing. Newer materials are being launched with increasing frequency (see Fig. 22.3).

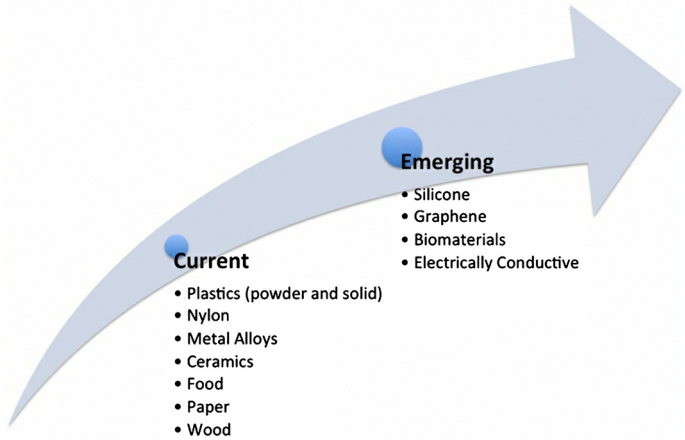


Figure 22.3: Materials for 3d printing.

22.2.3 Enablers to Accelerate Adoption

1. *Entry of large companies* with deep pockets like HP, Xerox, GE will drive printer and material development. HP announced their Multi-jet Fusion technology to be 10x faster than the nearest competitors. Incumbents like Stratasys and 3D Systems have to innovate rapidly to keep up. Newer players like Carbon 3D unveiled their ultra-fast CLIP technology and raised $100mn through Google Ventures and other VCs. Faster, Cheaper, and Better is the mantra.
2. *Development in the range of printable materials*. Today 3d printers can print a large range of materials from plastics to metals to ceramics. New materials are announced almost every month. Metals and alloys are important for getting an acceptable quality of final engineering parts especially in the aerospace and automotive sectors. The quality of the 3d-printed part has to meet durability, surface finish and other standards. A larger range of Biocompatible material could drive acceptance by regulatory authorities like the FDA and subsequently adoption by the healthcare industry.
3. *Easy to use software*. Free and easy to use software like Autodesk's 123D Design and Google's Sketch Up democratize the design process and accelerate the adoption process. An Israeli start-up has launched "Onshape," a cloud-based design software. It offers col-

www.elsevierdirect.com

laboration tools as one of its key selling features. The software is free for individuals. Businesses pay a nominal license fee per user annually.

4. *3D design and printing skills*. Coding skills have exploded in the last 10 years. Now a ten-year-old can write code for an app and publish it on Apple's App Store or the Android Playstore. This is not the case yet for 3d design. There is an acute shortage of talent for 3d design and printing. Designing for 3d printing is different from 3d design for gaming or virtualization programs. The gaming and virtualization industry has been around for many more years than the 3d printing industry and consequently has a pool of skilled resources. 3D printing does not and therein lies a problem. Introducing 3d printing programs in schools and universities can solve the lack of skilled resource. MOOCs (Massive Open Online Course) in 3d printing are being offered free by Deloitte University Press and Coursera. NTU in Singapore is one of the first Universities to offer a Masters in 3d printing. The Singapore Government subsidizes the course fees.

Within the venture funding space, Venture Scanners reports that Material development and Software development have been the top two funded categories in 3d printing.

22.2.4 Applications

The chart represents the spectrum of applications in the 3d printing world (see Fig. 22.4). The mature applications like 3d-printed prototypes, dental implants, and personalized hearing aids make up the highest number of 3d prints worldwide and have a very sustainable business model. The embryonic applications are still in the research phase. All the remaining applications fall in the middle. They have been commercialized though may not be profitable.

3D printing has significantly reduced the time it takes for prototyping. The traditional process took months and could potentially cost thousands of dollars. Now it can take a week and cost mere hundreds of dollars. Companies can also make many more iterations at negligible marginal costs.

There are 10mn 3d-printed hearing aids in circulation globally. US companies converted to 100% 3d-printed hearing aid shells in less than 500 days.[3]

Hearing aid manufacturers adopted 3d printing very quickly because 3d printing could lower their costs of manufacturing while improving quality and reducing returns. Earlier hearing aids were generic and took nine steps to manufacture. Now they are personalized and it takes three steps to manufacture. This results in lower manufacturing costs and higher customer satisfaction. An additional benefit was that the designs were digital and could be reproduced very quickly if needed. Another large application is personalized dental implants and dental braces. Invisalign, a company with a revenue of $850mn uses 3d printing technology to make 18–20mn personalized orthodontic treatment devices (dental braces) annually.

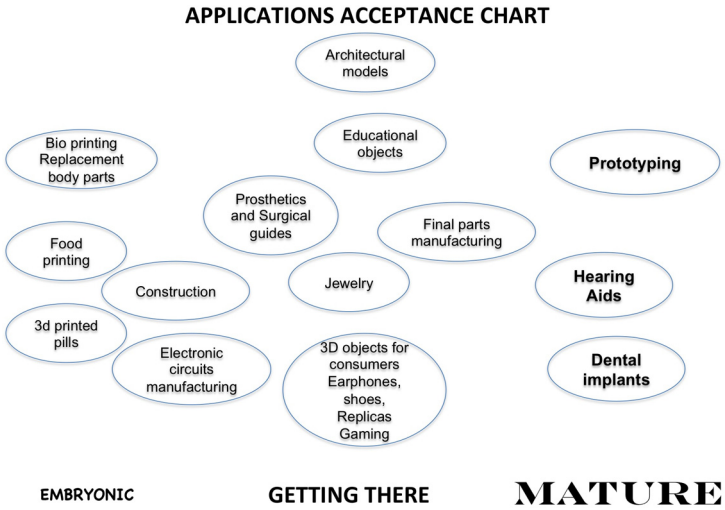


Figure 22.4: 3d printing applications.

Companies are adopting 3d printing to make final parts. GE's fuel nozzle that is used in their latest LEAP jet engine is a prime example.

Daihatsu, Japan's oldest car manufacturer, introduced 15 types of 3d-printed "Effect Skins" on their Copen model of cars. These skins are available in geometric and organic patterns in ten different colors. Customers can tailor the skins to their own requirement after which they are 3d-printed and installed on the fender or bumper.

Medical applications for 3d printing can be classified into three categories:

1. Creation of anatomical models, customized prosthetics, and implants.
2. Pharmaceutical printing for drug dosage and delivery.
3. Tissue and Organ printing.

Prosthetics makers both functional and cosmetic are increasingly turning to 3d printing. Advanced scanning and body modeling techniques can make better fitting prosthetics. Functional prosthetic hands that earlier could cost thousands of dollars can now be made for hundreds of dollars. Open Bionics is partnering with Disney to give kids the "Ironman hand" or the "Star Wars Light Saber Hand". Now kids can get excited about their prosthetics. If you think, 3d printing prosthetics is only restricted to humans, think again. Derby is a Husky mix born with stunted forelegs. It was impossible for him to walk around like a normal dog. Last year Tara, an employee at 3D Systems fostered Derby. Determined to help him, Tara and her colleagues at 3D Systems developed a set of prosthetic legs that have enabled Derby to move around freely.

www.elsevierdirect.com

Surgeons are finding that 3d-printed surgery planning models and tools can reduce operating time and lower the risk from errors or complications. Surgeons can also plan complex surgeries with CT scan data of a patient's bones, blood vessels or other organs, converted to a 3d-printable digital file. Doctors also use 3d printers to create surgical guides that are attached to the skeletal structure of the patient to provide a map for reshaping bone structure to perfectly accommodate standard-size implants.

J&J is an active user of 3d printing with different partners. It has partnered with a biomedical start-up Organovo to evaluate the use of 3d bio-printed tissue in a drug-discovery setting and with Carbon 3D to develop custom, complex surgical devices. J&J recently also announced a partnership with HP to create custom 3d-printed devices for customers and patients.[4]

The FDA has already approved 85 3d printed medical devices. Some examples are spinal cages, dental devices, and hearing aids with 3d-printed components.

Materialise, a Belgian company, makes customized hip and knee implants from titanium so that they fit the patients better and accelerate post-surgery recovery. China's equivalent of the FDA approved the use of 3d-printed hip implants last year. Johnson & Johnson's DePuy Synthes is collaborating with Materialise to offer patient-specific titanium craniomaxillofacial (CMF)[5] implants under the DePuy Synthes TRUMATCH portfolio.

In Aug. 2015, the FDA approved the world's first 3d-printed drug. The Zipdose epilepsy drug "Spritam" is 3d-printed so its dosage can be customized and it is easy to swallow.

A panel in the World Economic Forum held in Tianjin this year discussed the implications of 3d printing medicines at home. The consensus was that this is a distinct possibility in the next ten years. It may not be at home but under professional supervision at neighborhood pharmacies. It would be a huge step in delivering medicines that are personalized and precise. Personalized for your DNA with the precise dosage for maximum effectiveness. 3D-printed recreational drugs are expected to take off faster than medicinal drugs.

A McKinsey report says that 3d scanning and printing is one of the seven technologies that are making mass customization profitable. Profitable mass customization of products and services requires success in identifying the opportunity supported by a swift and cost effective transaction and keeping costs under control with rising manufacturing complexity. Apart from hearing aids and dental implants, there are very few successful case studies for 3d-printed mass customization. However the number of new customized products that have been launched in the last couple of years points to the inevitability of its happening.

1. Nike, Under Armor, and New Balance launched limited edition sneakers using 3d-printed components. New Balance is printing the entire sole and Under Armor is printing just the midsole. The sneakers are expensive but it is a matter of time before costs decline and millions of personalized shoes become a reality.

2. Norml.com and Ownphones.com are two start-ups personalizing Bluetooth earphones. The customer downloads a proprietary app to take photos of their ear. These images are uploaded to the website and the earphone shell is 3d-printed. The electronics are assembled and the earphones are shipped to the customer. These personalized headphones are not cheap. They start from $200 onwards.
3. Personalized jewelry is more successful than sneakers and earphones. Customers and designers can create the designs together or the customers create the designs from online templates. The rings or the pendants are not 3d-printed directly. The jewelry industry uses a hybrid of 3d printing and traditional metal casting processes to make the pieces. The design is 3d-printed with a wax-like resin to make a pattern. This pattern is sacrificed to make the mold. The piece is then cast using gold, silver, platinum or any other precious metal. Thanks to 3d printing, ornate designs that were impossible to make earlier are now being manufactured. Rob Wright of Ringcraft Moana, a New Zealand jeweler, has 3d printed rings embossed with the fingerprints of the bride and the groom. The 0.1-mm or 100-micron finish level that 3d printers offer allows Rob to print fingerprints without losing resolution.

In the education segment, 3d printing can bring a number of benefits to students and educators:

1. It makes learning more fun.
2. Fosters creativity and problem solving skills.
3. Vastly improves retention and quality of learning.
4. Creates excitement and engagement.
5. Can improve rate of learning amongst special needs individuals. E.g. visually challenged, autistic, etc.
6. Not expensive.

Some of the potential areas of learning that 3d printing can improve are:

1. Geography. A 3d print of the Grand Canyon can be a better learning aid than a 2d computer image or a photograph in a text book.
2. Biology. 3D printed body parts can significantly enhance learning. Feeling the texture of a brain is different from seeing it in a book or on screen. Complex structures of protein molecules in DNA can be very easily appreciated with 3d prints.
3. History. Important historical artifacts and monuments could be 3d-printed to allow students to appreciate history. The 3d printing manufacturer LeapFrog, in conjunction with Dutch Museum De Nieuwe Kerk, recently recreated China's entire Forbidden City from the Ming Dynasty period in 1:300 scale. Students from around the world are able to view, map, and understand the Chinese imperial palace. A total of 980 buildings make up the

Forbidden City, all available for download to classrooms worldwide. Staff at the Smithsonian are also using 3d printing and scanning to recreate artifacts throughout the museum, easily available and ready to print by students. From an exact replica of the 1776 Gunboat Philadelphia to St. Lambert's Cathedral in Belgium, history teachers are using 3d printers to bring cultural treasures of the past into classrooms.[6]

4. Anthropology and Archaeology. Darryl R. Ricketts, M.S., Adjunct Instructor, Anthropology at Indiana University South Bend is using 3d-printed replicas of fossil specimens for a more hands-on learning experience. The famous fossil, Lucy the Australopithecus, is now available for any amateur paleontologists to download and 3d-print for free. 3D printing the bones has helped scientists come up with a working hypothesis about her death.

Zaha Hadid, the world famous architect, was an extensive user of 3d printing. Hob's studio, a model making workshop in the UK, whose primary clients are Zaha Hadid Architects and Fosters + Partners, has seen their demand skyrocket over the past two years. Michelle Greeff, the firm's director of 3d technologies, says: "*Our main clients are Zaha and Fosters, but we've also seen more medium-sized architects start to approach us with requests for 3d printing. The costs are coming down, so it is becoming a real option for many architects now*."[7]

The construction industry is also trying their hand at 3d printing. There were some reports in the past about a Chinese developer 3d printing a villa. They turned out to be more hype than reality. The developer had built the supporting beams and columns in the traditional manner and 3d-printed a few walls on the ground floor. Recently however another Chinese construction company, Huangsha Tengda, 3d-printed a house in 45 days.[8] The team made the entire skeleton of the house with the plumbing and the rebar and then a 3d printer using concrete encased the skeleton. Twenty tons of concrete were used to print the 250-cm thick walls. The villa can withstand earthquakes as powerful as 8 on the Richter scale, which usually flattens cities.

Dutch 3d printer manufacturer byFlow is opening the first 3D Food Printing Restaurant in The Netherlands, under the name of "Food Ink."[9] At Food Ink the main draw isn't even the food, but the way in which it's made. Everything at this concept restaurant is 3d-printed; from the food to the dishes it is served on and unbelievably the furniture. Self-described as a "conceptual pop-up dinner series where fine cuisine meets art, philosophy, and tomorrow's technologies," this exceptionally unique experience uses 3d-printing to make everything.

We have heard of 3d printing chocolate or pasta but have you ever thought of 3d printing meat? Food Technician Peter Verstrate and Maastricht University professor Mark Post have been working on 3d-printed meat grown from beef stem cells since 2013. The first beef patty looked and tasted like the real thing but it cost $331,000.

The process begins with stem cells extracted from cow muscle tissue. These are cultured with nutrients and growth-promoting chemicals and put into smaller dishes, where they coalesce

into small strips of muscle just a few centimeters long and a few millimeters thick. Finally, these strips are layered together, colored, and mixed with fat using a 'bio-cartridge' and 3d printing technology to precisely layer each element together. The resulting pink substance, whether in its raw or cooked form looks like the real thing. In fact, at a taste-test, the prototype was said to taste almost like a real burger, except less juicy. Their clean meat start-up Mosa Meats has now hired scientists, lab technicians and managers to create a more reasonably priced and tastier version that can be mass-produced. If they meet their objectives, their beef could cost $3.60 per pound.

The pitch for lab grown meat is less on cost and 3d printing but more on environment friendliness. According to the BBC, an independent study found that lab grown beef uses 45% less energy than the average global representative figure for farming cattle, produces 96% fewer greenhouse gas emissions, and requires 99% less land.

According to Gartner's 3d printing Hype Cycle published in July 2015, bio-printing for organ transplants or for life sciences R&D is 5–10 years away from mainstream adoption. However Dr. Atala, a leading authority in regenerative medicine and the Director at the Wakeforest Institute of Regenerative medicine, may prove Gartner wrong. He and his team have printed ear, bone, and muscle structures and successfully implanted them in animals. The structures have matured into functional tissue and sprouted new systems of blood vessels, and their strength and size mean that they could feasibly be implanted into humans in the future. L'Oreal announced a partnership with Poietis, a French bio-printing firm, to print hair follicles in an effort to offer a solution for baldness.

22.3 The Future of Spending by Consumers, Businesses and Governments?

22.3.1 Consumers

Patrick and Naomi are avid Star Wars fans and want something special to celebrate their first wedding anniversary. They log on to polychemy.com, a site that offers innovative personalized 3d-printed jewelry and order two solid platinum Galaxy Couples rings for $2100. This is the future of consumer spending on bespoke items. 3D printing enables a production run of one bespoke unit and consumers are willing to pay for it.

3D objects marketplaces like CG Trader, and 3d Printing service bureaus like Shapeways and Sculpteo have sprung up in the past three years to satiate this demand for unique objects. Designers put up their designs in virtual stores. Consumers visit the marketplace, select a design that is subsequently 3d-printed and delivered. The designer gets a cut of the final price. Designs range from a few dollars for the frivolous items to thousands of dollars for jewelry. The

most printed item on Shapeways in 2015 was a Fitbit Flex Pocket Clip for $8.99. Fitbit does not offer the clip as an accessory.

Thingiverse is the world's largest "Free" repository for 3d printable objects. All the designs are published under the Creative Common's License and are free to download. At last count, Thingiverse had more than 600,000 designs.

The bespoke philosophy is not only restricted to jewelry but also extends to earphones (Normal.com), shoes (New Balance and Adidas), prosthetics (Bespoke Innovations), eyewear (a whole plethora of start-ups).

The adult industry is one of the biggest drivers of new technology. They pioneered online credit card transactions and video streaming among a lot of other innovations. They are not behind in adopting 3d printing either. Sexshop3d.com offers over 250 designs for sex toys that can be downloaded and printed at home.

The above are examples where consumers pay for the finished product. Consumers expect 3d printing to be quick, fast, and cheap and unfortunately it is not cheap, or fast.

This also leads us to how much a customer would spend on designing and printing a customized or personalized item. Most consumers would get sticker shock at the $50 price of a bespoke keychain. The pricing is not as atrocious as it sounds. Margins aside, the single largest cost is the design cost. It is not material costs and it definitely is not machine time. It is the designer's time.

For low value items, design costs could be as high as 80% of the cost. Hence bespoke 3d printing for low value items works only if the personalization engine is algorithmic (like 3dtrophyfactory.com). This brings down the design costs to a negligible amount and hence the retail price can be more palatable.

Jewelry is perfect for personalization because of its high intrinsic value and premium price it commands in the consumer's mind. The design costs would be a marginal component of the total cost.

Given consumers' willingness to spend on a unique design and to reduce sticker shock, 3d printing companies are coming up with different pricing models to "take money from the customer's wallet." An Israeli start-up 3Dshook.com launched a Netflix-like subscription service for 3d printable content. Pricing goes from US$10 for a 12-file pack to US$50 for a 100-file pack. Replicas or "mini me" figurines is another burgeoning application in 3d printing. Consumers pay hundreds of dollars for figurines of themselves. Figurines are now quoted as part of the wedding photography package. What better way to make your wedding more memorable?

Consumer spending fueled the huge surge in desktop 3d printers over the last two years. Wohler's latest report shows that 110,000 desktop printers were sold in 2015 resulting in a 67% increase over the previous year. All these printers are being used to print items from Thingiverse and other 3d object websites.

Platform printing services will offer a myriad of ways for consumers to pay for their purchases. 3dHubs one of the platform print service aggregators has partnered with BitPay to accept bitcoins as payments for 3d prints in over 140 countries. Brian deZwart, cofounder of 3DHubs says "*3DHubs and Bitcoin are platforms that enable communities to change industries with a bottom up approach to manufacturing and payments*".

22.3.2 Commercial or Businesses

In Sept. 2016, GE announced that they were buying SLM solutions of a German 3d printer company and Arcam, a Swedish 3d printer company for $1.4bn.

CEO Jeff Immelt remarked,

> *"Additive manufacturing is a key part of GE's evolution into a digital industrial company. We are creating a more productive world with our innovative world-class machines, materials, and software. We are poised to not only benefit from this movement as a customer, but spearhead it as a leading supplier."*

GE said in the press release that it expects to grow its new 3d printing business to $1 billion in revenue by 2020, while generating attractive returns, and also expects $3 to $5 billion of product cost savings across the company over the next 10 years. Earlier GE had made a big push into 3d printing through a $50 million investment to beef up a production facility in Alabama by installing 3d printers and hiring 300 full-time employees. That was in addition to the close to $140 million invested into its GE Aviation Additive Development Center near Cincinnati, Ohio.[10]

What is in this technology that giants like GE are taking an interest in it and betting big dollars on its future?

The answer lies in its ability to disrupt traditional design, manufacturing, and supply chain processes. It can shift profit pools and revenue streams thereby impacting the survival of some businesses.[11]

McKinsey Global estimates that the economic impact could be $550bn by 2025. 3D printing allows manufacturers to deploy capital more efficiently either through lowering the

units to achieve economies of scale or increasing the variety of units that can be produced at marginally higher costs. An evaluation to integrate 3d printing into the value chain has to consider the costs and benefits for each component of the value chain: Design, Manufacturing and Supply Chain.

Lets look at each aspect in a little more detail:

A. Design –

Arie Kurniawan, a young Indonesian engineer participated in a global challenge hosted by GE to redesign a bracket that attaches a jet engine to the wing of the aircraft. Arie's design won. What was surprising was that Arie had no experience in industrial manufacturing and his design was 3d printable. The bracket passed all tests for durability, stress, and reliability. And it weighed 83% less than the part it replaced.

The ability to 3d-print any object has liberated the design community and allowed them to enter into a "Constraint-free design" world. GE's fuel nozzle is another example of constraint-free design. Historically the nozzle was made from 18 components that had to be assembled in a time-intensive process. Now the whole nozzle is 3d-printed as a single piece leading to a 25% reduction in weight and a 5x increase in the durability.[12] Constraint-free design allows companies to consolidate many parts into fewer parts, eliminate part numbers, inventory, labor, inspection, maintenance, and certification paperwork. Parts that are 50% lighter can be produced using "Topology optimization" – a mathematical tool that decides where to put material to optimize the strength-to-weight ratio. It is possible to redesign parts with thinner skins and internal lattice structures instead of solid material without affecting strength or durability in any way. The new Airbus A350 XWB contains over 1000 3d-printed parts to reduce weight and improve its buy-to-fly ratio.

> *"We are on the cusp of a step-change in weight reduction and efficiency – producing aircraft parts which weight 30 to 55 percent less, while reducing raw material used by 90 percent."*
>
> ***Peter Sander, head of emerging technologies and concepts at Airbus***

Companies need to focus on the design element because it can

i) Save costs
ii) Reduce time between each iteration
iii) Introduce features offering a competitive advantage.

Surgical guide designs that are 3d-printed is an example in the health care industry. 3D printing is also creating the perfect fit through printed custom guides and tools. This is done for

operations involving cutting or drilling into skeletal structures — such as jaw surgeries, knee replacements and other joint-related procedures.

Personalized prosthetics either functional or as a fashion accessory would not have been possible without constraint-free design.

Artists, sculptors, and creative professionals can let their imagination run free to create objects of beauty. John Edmark, a professor at Stanford University, created Fibonacci Zoetrope sculptures that wouldn't have been possible without 3d print technology.

In the near future AI would be generating 3d printable designs. In December 2015, Autodesk manufactured the world's first 3d-printed automobile chassis designed with AI.

B. Manufacturing

Modern manufacturing despite all the technological advances is a very inefficient global system. It operates on economies of scale. The more you produce, the lower is the per unit cost. In 3d printing, however, the unit costs are not tied to the volume produced. The cost is the same whether you produce 10 items in a one location or 1 item in 10 locations. Now that is disruptive and hence it caught the attention of many CEOs.

PWC's 2016 Disruptive Manufacturing Innovation Survey shows increased adoption of 3d printing amongst US manufacturing companies.[13]

1. More than two-thirds of US manufacturers are using 3d printing. The highest increase in adoption is for final parts manufacturing or production of end products.
2. Manufacturers anticipate greater use of 3d printing for high volume production.
3. In the next 3–5 years, 3d printing will be used to produce obsolete parts.
4. Expensive printers and uncertain finished product quality are the top adoption barriers to 3d printing.

3D printer manufacturers are racing to make printers that are faster, cheaper and produce higher quality output. 3D Systems has announced plans to create an end-to-end solution geared to the company's latest technology, which promises to offer production speeds 50 times faster than older models.

In a recent press release, Stratasys announced partnerships with Boeing and Ford to "explore applications enabled by advances in Stratasys technology to ensure future systems are optimized for large scale manufacturing applications."

3D printing is used in manufacturing for

- Production parts
- Tooling patterns and components

- Functional models
- Jigs and fixtures
- Visual aids
- Concept models
- Fit and assembly testing
- Patterns for casting

Aerospace companies are adopting 3d printing rapidly because it has become easier and cheaper to 3d-print with metals. Metal 3d printer sales exploded with a 47% growth in 2015. Airbus is printing functional parts like an elbow for a fuel line that consolidates 126 separate parts into one 3d-printed part. Airbus is planning to 3d-print 30 tons of metal monthly by the end of 2018.

LITE-ON, a Taiwanese smartphone manufacturer installed 3d printers in their Guangzhou factory. These printers use a process called Aerosol Jet to focus a mist of micro-droplets into a beam as small as 10 microns (1/10th the diameter of a human hair). LITE-ON uses this technology to print antennae and sensors directly on motherboard instead of assembling these components individually. This saves money and increases efficiency.

The latest trend in 3d printing as applied to manufacturing is hybrid manufacturing. This is a combination of 3d printing combined with a traditional machining process. The Korean Air Force uses hybrid manufacturing for maintenance on their F-15s. A metal seal in the engine cowling gets worn down over time which means that the engine cannot be used. A new metal seal would cost hundreds of dollars and would mean engine downtime. Now, the Air Force technicians use metal 3d printers to add more material to the circumference of the seal and then machine it down to the required specifications. The net result is lower cost and lesser engine downtime.

The healthcare segment has adopted 3d printing very actively. Apart from hearing aids and dental aligners, knee joints and hip joints made from medical grade titanium are now being used. The biggest benefit here is not cost savings but other vectors like lower operation times, better fit for customer, and hence quicker recovery leading to happy patients and less stress for the surgeons and the nursing staff.

3D-printed prosthetics have life altering effects on the patient. The current cost of prosthetics is upwards of $15,000 each. A UK start-up Open Bionics is creating affordable bionic hands. Their bionic arms combine art, engineering, and science fiction so that the wearer can show it off with pride.

Decentralized Manufacturing

One of the biggest opportunities for 3d printing is decentralized manufacturing. "Customer proximity" will be the new mantra. Cost was the single largest driver for locating manufacturing facilities. Economies of scale combined with Government incentives led to garment factories in Bangladesh and Mexico and all kinds of production facilities in China. Cost of shipping to customers was secondary. In the near future, 3d printing could potentially take away the economies of scale proposition and you could locate factory hubs in countries or even cities. Imagine this scenario… You want to buy a customized pair of shoes. You log onto say Adidas and design your shoe online. Color, size (left foot half a size larger than right), pattern, sole, insole, etc., and lastly your zip code. The Adidas online order system routes your order to an Adidas 3d printing location closest to your zip code. A delivery drone drops off your personalized pair of shoes at your doorstep. This is decentralized manufacturing. The famous inventor Sir James Dyson said,

> *"You can be independent. You don't need toolmakers. You don't need molders. You don't need casters. You don't need foundries. You can do it all yourself with a relatively simple (I hope) machine. So you can make things all over the place. You can make them very locally to each country that you are selling it and get rid of freight costs and import duties and all those sort of things. I think it will eventually transform the ways products are made".*

C. Supply Chain

Supply Chain has many interpretations. For the purposes of this discussion, let's restrict it to moving product from manufacturing locations to customer locations. NASA 3d-printed a wrench in space. Why? Because it was cheaper to print than to spend $400 to ship it to the ISS.[14]

Causing disruption in last mile fulfillment or print on demand can happen when some of the following enablers fall in place.

1. Inventory becomes digital.[15]
   Products digitization for 3d printing can not only be done by designing using CAD software but also by 3d scanning finished parts. Either way results in an electronic file that is of high quality and easily transportable across the world.
2. Product quality checks and tests are documented and can be implemented off site. 3D printed parts should look the same and function as well. Quality standards and processes to test for surface finish, functional strength and reliability have to be in place. New material development and progress in printer technology are driving towards achieving these standards.

3. Trained manpower is available at all locations. Skills shortage is one of the barriers for on demand manufacturing. Companies need to invest in training and reskilling workers. The hiring policies need to take the new skill sets into consideration for new younger hires.
4. IP risks are contained in some manner. It is common knowledge that once a digital file is in the ether, it cannot be contained. How does a company retain its IP for their digital design? Authentise, a start-up born from Singularity University, is at the leading edge of this technology. They are building the middleware for distributed manufacturing. Lowe's one of the top home improvement chains in the US is using Authentise technology to let customers print their own parts.

Maintaining physical inventory of parts in multiple locations and fulfilling customer demand for "C" category replacement parts are one of the bigger cost and customer dissatisfaction drivers. The service and support department are always walking the tight rope between estimating demand and stocking parts for quick fulfillment when a breakdown occurs at customer site. "C" category parts are not in high demand but a delayed fulfillment can cause severe customer dissatisfaction. E.g., a gear wheel in your printer breaks and the printer stops working. Gear wheel failure is not a usual occurrence hence the company does not stock the part near your location. It takes 48 hours to replace because it has to be couriered from China (or wherever it is made or stocked). After receiving the part, the technician has to come to your office or home and fix it. Till then, no printouts and a very unhappy You!

Jay Leno, an American television star, has one of the world's best collections of rare and vintage cars. He needed to make a spare part for his 1907 White Steamer. Using 3d printing he reproduced the part and the car is back on the road.

On demand production gives rise to a new class of small service-led businesses like the erstwhile Kinkos. Low on capital but high on customer proximity. Fast Radius is a distributed manufacturing business. The firm has customized its array of systems for an automated distributed manufacturing environment. After a customer places an order, it will automatically find the proper printer and begin printing.

Rick Smith, cofounder says,

> *"I learned that a number of OEMs are already looking to address their physical inventory woes with the advantages of virtual inventories. On average, the rule of thumb for the cost of holding physical inventory is about 25 percent the cost of the part per year," he explained. "There is a significant cost in terms of cost of capital, warehousing space, security and damage. The other major problem with physical inventory is that you've got to produce in large volumes to get the unit costs low. This works great when you're producing iPhones and you know you're going to*

sell 10 million of them. But, when all of a sudden you've got an essential part and you know you're only going to need 15 of them per year—maybe it's a critical part to a machine in a manufacturing operation that doesn't break very often, but is extremely important when it does break—then it doesn't make sense to go through the setup and all of the costs related to doing a larger-scale production."[16]

Shifting profit pools and emerging revenue streams.

The 3d printing revolution has upended some traditional businesses and has forced CEOs to take an active look at their profit pools. It has also opened up additional revenue streams for retailers, developers, and investors.

UPS is a classic example where decentralized manufacturing has the potential of affecting a big chunk of their revenue. Apart from their bread and butter courier services UPS offers a stocking and shipping service for parts on behalf of some large manufacturers. This service accounts for a reasonable size chunk of their revenue and profits. Recognizing this threat UPS partnered with Fast Radius to 3d-print parts. They launched in the US in May 2016 and expanded to Singapore for the Asia hub in September 2016.

However all ventures in 3d printing to extend revenue potential are not successful. Riding the hype of 3d printing, Amazon announced a 3d-printed items storefront in 2014. Now a search on Amazon for 3d-printed items shows only printers, books, and filament. However Amazon's entry into 3d printing is a no-brainer. Like a traditional retailer they have to keep huge stocks in gargantuan warehouses and ship to customers in the most efficient way when they receive orders. Keeping digital design files of 3d printable objects and printing on demand could potentially reduce their inventory holding.

22.3.3 Government

"Our first priority is making America a magnet for new jobs and manufacturing. There are things we can do, right now, to accelerate this trend. Last year, we created our first manufacturing innovation institute in Youngstown, Ohio. A once-shuttered warehouse is now a state-of-the art lab where new workers are mastering the 3d printing that has the potential to revolutionize the way we make almost everything. There's no reason this can't happen in other towns. So tonight, I'm announcing the launch of three more of these manufacturing hubs, where businesses will partner with the Departments of Defense and Energy to turn regions left behind by globalization into global centers of high-tech jobs. And I ask this Congress to help create a network of fifteen of these hubs and guarantee that the next revolution in manufacturing is Made in America."

President Obama in his State of the Union Address on Feb. 12, 2013

"3D printing is an innovation driven developmental tool."
President Xi Jin Ping in G20 summit Aug. 2015

Given the disruptive nature of the technology and its implications on productivity and impact on GDP, it is not surprising that the world's top economies are focusing lots of investments in 3d printing. A significant amount of these resources are going towards R&D and skill development.

1. USA

In 2013, President Obama announced three more NAMIIs (National Additive Manufacturing Innovation Institute). The first one was set up in Youngstown Ohio in 2012 supported by $40mn of public funding. These institutes function under the banner of "America Makes." America Makes facilitates collaboration among leaders from business, academia, nonprofit organizations, and government agencies, focusing on areas that include design, materials, technology, and workforce and help the American three-dimensional (3d) printing industry become more globally competitive. Since then, America Makes has funded various developmental projects for it members. E.g., awarding $8mn in R&D funds to UDRI to support USAF efforts towards safe and more efficient sustainability. They have more than 160 members. Amongst them are Fortune 1000 manufacturers, SMEs, academic institutions, non-profit organizations, and Government agencies.

In a classic example of public private partnerships, New York will be investing along with Norway's Norsk Titanium AS (NTi) in a $125 million facility. State University of New York (SUNY) Polytechnic Institute is involved with the program as well.[17]

This plant is expected to be fully operational, with several dozen 3d printers, by the end of 2016. Warren Boley, NTi's chief executive who was a former executive with Aerojet Rocketdyne said that the 3d printing plant, which will be 200,000 square feet, would be government-owned but operated by NTi. It will be able to 3d-print large components for defense and aircraft industries far cheaper than current technologies used.

2. UK

The UK Government has invested GBP 100mn into a new research center (Aerospace Research Centre and National Centre for Net Shape and Additive Manufacturing) in Coventry. The center will be used to develop 3d printed components for aircraft engines and landing gear as well as automotive and medical devices.

3. Germany

Manufacturing accounts for 21% of the German economy. German manufacturing hinges on superior quality and performance. Despite cheaper Asian competition, German manufacturing

exports have been growing. German SMEs are the reason behind this success. A 2007 study showed that more than 1130 German SMEs held either the number 1 or number 2 position in the world markets for their products. A critical factor in the German SME manufacturing success is the Fraunhofer-Gesellschaft (Fraunhofer Society).[18] It is an independent NGO that provides high quality short-term affordable applied research. It is a 2.45bn$ enterprise that operates more than 60 research institutes with more than 250 business focus areas. It has 22,000 employees. The Fraunhofer Additive Manufacturing Alliance has partnerships with 16 institutions across Germany and is currently focusing on industrial solutions in five areas of application:

1. Bio-medical engineering
2. Micro-system engineering
3. Automotive engineering & aerospace
4. Tool making
5. Handling and assembly

A recent Ernst and Young research study on adoption of 3d printing puts Germany as the worldwide leader. 37% of German companies already use 3d printing. An additional 12% plan to use it in the near future.

4. Netherlands

The Dutch government, industry, and research institutes will invest € 134 million in 3d printing research projects and studies. Recipients include research institutes TNO, Deltares, TU Eindhoven, TU Delft, Twente University and others.

A major part of the funding will go towards studies of TNO and TU Eindhoven, among them "Print Valley 2020". The Print Valley knowledge center revolves around different 3d printing methods, with the aim to take complete control of all aspects of different processes in order to develop new and innovative 3d printing platforms with high speeds, a combination of a variety of materials and other integrated processes. Earlier this year, TNO has introduced their Hyproline additive manufacturing system for the serial production of metal parts.

5. CEEC

Research firm IDC says that CEEC (Central and Eastern Europe) will invest more than $917mn in 3d printing hardware, software, services, and materials in 2016.

6. China

China is the "factory" of the old world. They have the most to lose with increasing global adoption of 3d printing. In a speech given at the G20 summit in 2015, Chinese President Xi Jinping said that sluggish growth needed to be countered by innovation driven developmental

tools like 3d printing and Internet+. He called for the upgrading of traditional industries with 3d printing. The Chinese government plans to invest millions under the auspices of the "Made in China 2025" initiative which is a part of China's 15th 5-Year Plan to promote hi-tech manufacturing in aerospace, aviation and automotive industries. The plan also envisages educating the next generation of workforce to be competent in 3d-printing technology by deploying 3d printers in 400,000 elementary schools. The Chinese Ministry of Science and Technology will invest 2bn RMB (approx. $313mn) in R&D for 3d printers, equipment, and applications.

7. Japan

Japan has allocated 4bn Yen ($39mn) to various national 3d printing projects. 80% of this funding is for R&D of 3d printers that can make metal end use products for industrial use. Another 15% will go towards developing super-precision 3d printing technology including FDM, SLS and technology for post processing and powder recycling.

The Japanese Ministry of Economy, Trade and Industry (METI) plans to launch an initiative with 3 major universities and institutes and 27 Japanese companies including Mitsubishi, Nissan and Panasonic to develop metal 3d printers. Japan's long-term goal is to build the most advanced industrial 3d printer by 2020.

8. South Korea

The Ministry of Trade Industry and Energy is investing $20mn in a 5-year plan (2017–2022) into 3d printing and 3D manufacturing of ships and offshore equipment. The plan also targets to train 10mn creative makers by 2020. The South Korean Government also announced tax incentives for R&D spend towards 3d printing. Businesses can claim up to 30% of their R&D expenses as tax deductible.

9. Singapore

The Government has thrown its support behind the industry, identifying it as one of the key sectors to grow back in 2013 under a $500 million "Future of Manufacturing" scheme. Last September, Spring Singapore and the National Research Foundation announced the formation of the National Additive Manufacturing Innovation Cluster, which will help companies develop capabilities in 3d printing. Led by NTU, the cluster will look at the latest research in 3d printing and study how to translate it into commercial uses in the industry. NAMIC has since engaged more than 50 companies, trade associations, and chambers of commerce across various sectors like precision engineering, oil and gas, and electronics.

The SC3DP (Singapore Centre for 3D Printing) has attracted S$41 million in funds from industry and Government partners, and will receive S$42 million over 10 years from the National Research Foundation's medium-sized center grant. The grant by the foundation will go

towards consolidating research activities across faculties and universities to create a "critical mass" of researchers.[19]

Professor Bertil Andersson, NTU's president, said: "*We aim to groom the next generation of 3d-printing engineers so as to grow the much-needed manpower for this rapidly developing sector*."

US-based safety solutions company Underwriters Laboratories invested US$8 million (S$11 million) to open a Global Additive Manufacturing Centre of Excellence in Singapore, which will focus on training, material and process qualification, advisory and research in 3d printing.

10. South Africa

South Africa has invested more than $25mn of public funds since 2014 for 3d printing research and development.

11. The European Commission

The EC funded more than 60 successful projects in AM, with a total amount of EU contribution of over €160 million and a total budget of €225 million.

22.4 The Future of Borrowing and the Risks of Lending

The most disruptive innovations do not ask for your permission but they do demand your attention.

The Financial Services Industry is sitting up and paying attention to the 3d printing industry. Banks are assessing risks for corporate clients whose business models could be disrupted by 3d printing, angel investors and VCs are looking to invest in the next unicorn, crowdfunding platforms like Kickstarter and Indiegogo are funding smaller pre-sales rounds, Governments are worried about loss of tax revenues and import duties, and insurance companies are worried about IP led liability.

The 3d printing juggernaut is spawning hundreds of small and medium businesses that are hungry for capital. The following list offers good sources of raising funds:

1. VC and angel investors. Venture Scanner is a research firm tracking VC investments across different tech categories like AI, 3d printing, etc. As of Sept. 2015, they report that 257 companies in 9 categories across 27 countries have received a total of $517mn in funding. Not surprisingly, most of the funding is for development of materials followed by software. Google Ventures, Sequoia Capital, Intel Capital, and Lux Ventures are some of the notable names investing in 3d printing.

2. Crowdfunding platforms like Kickstarter and Indiegogo offer good options for small product led businesses to raise capital. As of July 2016, there were 19 live 3d print related projects. Totally there were close to 400 active projects for 3d printing till July 2016. The most successful 3d printer projects are:
   i. M3D $3.4mn and 855 backers.
   ii. Tiko $2.9mn and 538 backers.
   iii. Form 1 $2.9mn and 68 backers.
   iv. 3Doodler $2.4mn and 457 backers.
   v. OLO $2.3mn and 180 backers.
3. Companies like Intel, HP, and Autodesk among other big names have set up corporate venture capital arms to invest in early stage small companies with cutting technology. Autodesk Spark is a $100mn investment fund that recently invested $10m in Carbon 3D. Incumbents like Stratasys and 3D Systems also invest in companies to drive revenue growth. Stratasys participated in a $14mn Series A funding round in Desktop Metal, a company developing metal 3d printers.

Governments stand to lose VAT/GST or any other consumption tax when customers can download objects and print at home.[20] That import duties on material used in these 3d printers may increase but would be a small consolation. One consequence would be to increase other taxes to compensate for this loss.

> *"Governments are already looking to replace lost tax revenue, and pressure will likely mount for a product's digital blueprint to become the taxable item or for a 3D printer to create a taxable nexus."*
>
> ***Channing Flynn Global Technology Industry Leader Tax Services EY***

Companies could use this opportunity to reduce their costs. E.g., a company is selling a toy through retail. Their cost structure would include Cost of Goods and Supply chain and distribution costs. Now they allow the customer to download the design and print at home. All the COGS and Supply chain and distribution costs would be saved.

IP is the core around which will revolve all issues like taxation, liability, copyright, trademark and industrial design protection.

1. Taxation – As mentioned earlier, there could be a move to tax the digital blueprint since there will be significant loss of indirect and direct taxes when 3d printing reaches maturity. The whole taxation area raises some interesting questions like who should be taxed? The company who makes the digital blueprint or the consumer who downloads and prints the object? How does one establish the value of the digital blueprint? At source or in the country where it is printed or both since intangible digital files cross borders undetected.

What are the recovery and enforcement mechanisms to be put in place by Governments? All these questions cannot be answered now but it is well worth thinking about them and attempting to put some policies in place.

2. Liability and Insurance[21] – New technologies raise risk and the insurance industry deals with risk. Different applications for 3d printing throw up very different risk scenarios. Let's examine the risks by going through the 3d printing process.
   a. Design – This would be the area where IP violation would be the biggest risk. How does an insurance company determine IP ownership and professional indemnity exposures? 3D scanning technologies are advancing rapidly and it is very easy to get a high-resolution scan of any object and put it up on the Internet for millions of downloads. Think of Napster and multiply the value of the risk of IP infringement multi-fold.
   b. Making the 3d print – Traceability and attribution of liability is another issue that highlights risk. A consumer downloads a popular toy design from one of the file repositories and prints it. His kid puts the toy in his mouth and swallows some of the material leading to poisoning. Who is liable? The person who put up the design? The company whose design was used? The materials company? Product liability comes under scrutiny and there are no answers.

The economics of Crime – Combining digital design capabilities and 3d printing, the world is your oyster.

1. In Aug. 2016, security experts cloned and 3d-printed the TSA set of master keys used for the screener-friendly locks.[22]
2. In 2014, Bulgarian and Spanish authorities working with Europol's European Cybercrime Center in the Hague took down a Bulgarian organized crime network which was using 3d printing for ATM skimming crimes apart from credit card fraud and forgery. The thieves used 3d printers to make fake plastic card slot bezels they installed on ATM machines and Point of Sale terminals. They used the stolen passwords to print fake cards and used them to withdraw money from ATMs as far as Chile.[23]
3. Cody Wilson successfully printed and fired a plastic gun called the "Liberator". The hand-gun would have made it past all the traditional security scanners.
4. Australian police raided a house in New South Wales and discovered lots of 3d-printed knuckle-dusters and gun parts.
5. The possibility of 3d-printed recreational drugs is not a distant one. The technology is available and drug barons have the capital to make it a reality in the near future.

Criminals will find innovative ways of using the power of 3d printing and law enforcement has to invest in being able to counter this emerging threat.

3d printing is a great technology for counterfeiters. Any digital file can be hacked and 3d-printed. Private firms and government entities are developing high-tech anti-counterfeit measures. Quantum Materials Corp has recently announced to have licensed a technology called 'quantum dots' which could prevent counterfeiting. The company inserts tiny nanocrystals into a product, which function as a unique physical signature that cannot be cloned and that is associated with the manufacturer. The company also implemented a further security layer based on semiconductor nanomaterials that emit different colored lights if properly stimulated. Other anti-counterfeit solutions include shape memory polymer, anti-erasing ink, and DNA marking. Public private partnerships are essential to developing and deploying these solutions.

In summary, 3d printing is about the "Democratization of Creation and Making". Consumers will be "Co-creating, Making and Buying." Manufacturers and businesses have to be able to fulfill the "Demand of One" in the most efficient manner. Governments have to invest to get their citizens ready for the 3d-printed world and regulatory bodies have to come up with policies that mitigate the risks that 3d printing, a new technology, brings with it.

3d printing is going to touch your world softly like a feather or crash into it like a meteorite. It may benefit you or may obliterate you. Whether you are a CEO of a big company, a mother at home caring for her kids, a self-made billionaire or the Prime Minister of a nation, the only question is: are you ready for it? Only time will tell!

Notes

1. Principal Financial Services, 2016. The High Tech Lever: Technology's Influence on the Economy [online]. Available at: https://www.principalglobal.com/knowledge/insights/high-tech-lever-examining-technologys-influence-economy [Accessed 14 Aug. 2016].
2. Anon, 2016. AM Processes, Technologies and Applications [online]. DU Press. Available at: http://dupress.deloitte.com/dup-us-en/focus/3d-opportunity/the-3d-opportunity-primer-the-basics-of-additive-manufacturing.html [Accessed 11 Apr. 2016].
3. D'Aveni, R., 2015. The 3D printing revolution. Harvard Business Review.
4. Enriquez, J., 2016. JJ HP partner to make 3D-printed medical devices [online]. Meddeviceonline.com. Available at: http://www.meddeviceonline.com/doc/j-j-hp-partner-to-make-d-printed-medical-devices-0001 [Accessed 18 August 2016].
5. Enriquez, J., 2016. JJ materialise partner on 3D-printed custom cranio-facial implants [online]. Meddeviceonline.com. Available at: http://www.meddeviceonline.com/doc/j-j-materialise-partner-on-d-printed-custom-cranio-facial-implants-0001 [Accessed 18 September 2016].
6. Anon, 2016. 3D Printers for History Education | Print the Past! [online]. 3D Supply Guys. Available at: https://www.3dsupplyguys.com/3d-printing-education-center/3d-printers-for-history-education/ [Accessed 13 Jul. 2016].

7. Clark, T., 2014. Use of 3D printing up 400 per cent over past year, says leading modeller [online]. Architects Journal. Available at: https://www.architectsjournal.co.uk/news/use-of-3d-printing-up-400-per-cent-over-past-year-says-leading-modeller/8665048.article [Accessed 26 Sep. 2016].
8. Scott, C., 2016. Chinese construction company 3D prints an entire two-story house on-site in 45 Days [online]. 3DPrint.com. Available at: https://3dprint.com/138664/huashang-tengda-3d-print-house/ [Accessed 28 Aug. 2016].
9. Chang, L., 2016. At this restaurant the chef is a 3D printer [online]. Digitaltrends.com. Available at: http://www.digitaltrends.com/cool-tech/food-ink-3d-printing/ [Accessed 29 September 2016].
10. McKenna, B., 2016. 3D printing stock investors: general electric aims for a $1 billion 3D printing empire by 2020 – the motley fool [online]. The Motley Fool. Available at: http://www.fool.com/investing/2016/09/09/3d-printing-stock-investors-general-electric-aims.aspx [Accessed 13 September 2016].
11. Mckinsey, Quarterly, 2014. 3-D printing takes shape [online]. Available at: http://www.mckinsey.com/business-functions/operations/our-insights/3-d-printing-takes-shape [Accessed 21 July 2016].
12. Zaleski, A., 2015. GE's bestselling jet engine makes 3-D printing a core component. Fortune [online]. Available at: http://fortune.com/2015/03/05/ge-engine-3d-printing/ [Accessed 8 April 2016].
13. Anon, 2016. 3D printing comes of age [online]. Available at: http://www.pwc.com/us/en/industrial-products/publications/3d-printing-comes-of-age.html [Accessed 27 June 2016].
14. Smith, R., 2016. Forbes welcome [online]. Forbes.com. Available at: http://www.forbes.com/sites/ricksmith/2015/06/22/henry-ford-3d-printing-and-the-new-economics-of-manufacturing/#48d1013c1b42 [Accessed 23 Aug. 2016].
15. Charron, T., 2014. Building your 3-D digital inventory to include everything you manufacture [online]. Appliancedesign.com. Available at: http://www.appliancedesign.com/articles/94190-building-your-3-d-digital-inventory-to-include-everything-you-manufacture [Accessed 9 Sep. 2016].
16. Moulitch-Hou, M., 2016. Fast Radius Introduces Virtual Inventory for 21st-Century Manufacturing > ENGINEERING.com [online]. Engineering.com. Available at: http://www.engineering.com/3DPrinting/3DPrintingArticles/ArticleID/12222/Fast-Radius-Introduces-Virtual-Inventory-for-21st-Century-Manufacturing.aspx [Accessed 12 Jul. 2016].
17. Anon, 2015. NY Investment in 3d Printing [online]. 3DPrint.com. Available at: http://www.3dprint.com [Accessed 8 Aug. 2016].
18. Anon, 2013. How Does Germany Do It? [online]. Asme.org. Available at: https://www.asme.org/engineering-topics/articles/manufacturing-processing/how-does-germany-do-it [Accessed 21 Aug. 2016].
19. Khew, C., 2016. New 3D printing centre at NTU for precision engineering and manufacturing technologies. The Strait Times [online]. Available at: http://www.straitstimes.com/singapore/education/new-3d-printing-centre-at-ntu-for-precision-engineering-and-manufacturing [Accessed 12 Jun. 2016].
20. Anon, 2015. How could 3-D printing upend tax strategies? [online]. Taxinsights.ey.com. Available at: http://taxinsights.ey.com/archive/archive-articles/how-could-3-d-printing-upend-tax-strategies-.aspx [Accessed 14 Sep. 2016].
21. Anon, 2016. 3D printing: state of the industry [online]. Cgd.swissre.com. Available at: http://cgd.swissre.com/risk_dialogue_magazine/3D_printing/3D_Printing_State_of_the_Industry.html [Accessed 14 Aug. 2016].

22. Anon, 2016. Evolution of 3D Printing Technology Raises Security Concerns [online]. Resources.infosecinstitute.com. Available at: http://resources.infosecinstitute.com/evolution-3d-printing-technology-raises-security-concerns/ [Accessed 6 Jul. 2016].

23. Halterman, T., 2014. How 3D Printing Has Already Revolutionized Crime [online]. 3D Printer World. Available at: http://www.3dprinterworld.com/article/how-3d-printing-has-already-revolutionized-crime [Accessed 22 Jun. 2016].

Index

0–9

3D printing, 503, 514, 515, 519, 520
8Securities, 487, 488, 490

A

Access, 388, 389, 392, 397, 398, 401, 402, 411, 413, 417–419, 439, 442, 448, 456–458, 465–469, 482, 484, 487
AI, 42, 80, 488, 507, 515
Airbnb, 358
Alibaba, 2, 3, 13, 15, 29, 32, 40, 48–50, 56, 60, 335, 344, 348, 350, 353–358
Alipay, 2, 32, 40–42, 48–50, 59–61, 121, 131, 138, 141, 332, 347, 354, 355
Alphabet, 357
Alternative trading systems, 189, 196–198, 202, 205, 211, 281
Amazon, 2, 42, 50, 73, 183, 346, 353, 354, 357, 358, 494, 511
Ant Financial Services Group, 38, 40, 49
API, 81, 99, 130, 174
Artificial Intelligence, 21, 80, 488
ASEAN, *see* Association of Southeast Asian Nations
Assets under management, 42, 48, 483, 485, 487
Association of Southeast Asian Nations, 32, 408, 424–426
ATS, *see* Alternative trading systems
Attack, 263
Attacks, shoulder-surfing, 118, 139, 140
AUM, *see* Assets under management
Authorization process, 117–120, 124
Autonomous finance, 474

B

B Kash, 348, 458
Banking sector, 393, 394, 399, 400, 409, 416, 417
BCNs, *see* Broker crossing networks
Big data technology, 39, 42, 66–70
Bitcoin blockchain, 151, 154–156, 174, 214, 215, 223, 224, 226, 229–231, 258, 260, 261, 264
Bitcoins, 147, 148, 158, 171, 172, 181–183, 193, 201, 205–207, 209, 210, 212, 215, 226, 230, 234, 258, 261
BitShares, 151
Blockchain
  permissioned, 244, 273, 274, 310, 311
  permissionless, 224, 244, 273, 310, 311
  unrestricted, 194, 195
Blockchain applications, 171, 196, 236, 238
Blockchain architectures, 273, 274, 306, 310, 316
Blockchain developments, 164, 236, 251
Blockchain network, 153, 195, 225, 226, 263, 265
Blockchain technology, 188, 189, 192–194, 196, 197, 211, 213–215, 217, 223–226, 231, 232, 234, 244–249, 251, 265–267, 273, 274, 309, 310, 313–316
  using, 249, 313–315, 320, 321, 471
Blockchain technology platform, 189, 197–200, 202–205
Blockchain world, 147, 180, 259
Bluetooth, 141, 442, 501
Broker crossing networks, 275, 281, 299
Broker-dealers, 189, 190, 192, 196–201, 279, 304
Brokers, 183, 189–191, 198, 199, 201–203, 205, 211, 277, 278, 287, 290, 293, 302, 318, 320, 321, 481, 484

BTC Trading Corp, 200–203
Burma, 407–413
Burmese, 406–409, 412, 417
Byzantine generals' problem, 148

C

Cambodia, 348, 393–395, 399, 401
CBM, *see* Central Bank of Myanmar
Central Bank of Myanmar, 410, 412, 415
Central securities depositories, 249, 287, 305
Central securities depositories regulation, 274, 287, 305
Centralized governed auditing blockchain, 322
CFTC, *see* Commodity Futures Trading Commission
CGAP, *see* Consultative Group to Assist the Poor
China, 2–4, 7, 9–19, 21–27, 29, 30, 32, 41, 42, 45–52, 54, 57–60, 62–64, 72, 73, 353–355, 358, 464
China financial stability report, 58, 59, 62–64
China Securities Regulatory Commission, 5, 7, 54, 55
China's crowdfunding market, 25, 62, 64
Chinese government, 3, 25, 26, 45, 46, 49, 51, 52, 357
Chinese market, 3, 4, 11, 23, 25, 32
Code
  source, 136, 177, 252, 259
  unique, 293–295, 316
Code of law, 184
Coders, 227, 254, 256–258
Commodities, 185, 196, 205, 207–210, 273, 284–286, 288, 292, 299, 300, 412
Commodity Futures Trading Commission, 189, 192, 205, 207–211, 280, 285, 293, 295, 296, 304, 338
Companies, logistics, 81, 477, 478
Computing platform, trusted, 85, 95, 97, 98, 109, 111
Consensus, 74, 148, 151–155, 158, 159, 170–172, 175, 194, 195, 246, 247, 261, 264, 306, 307, 310, 312, 500
Consensus protocols, 147–155, 158, 162, 172, 173
Consultative Group to Assist the Poor, 59, 388, 399
Consumers, 30, 46, 51, 53, 55, 74, 128, 226, 237, 338, 344, 353, 365–367, 380–384, 503–505
Contracts, 13, 81, 153, 156, 171, 172, 184, 197, 205–209, 226, 231, 233, 234, 293–295, 308, 309, 311–313, 473, 474
Corda, 162, 172
Counterparties, 164, 183, 206, 207, 247, 292–294, 296–298, 391
Countries, poor, 465–468
CreditEase, 2, 18, 20, 72–75, 78–80
CreditEase financial cloud, 75–82
Crowdfunding, 2, 22, 24, 25, 51, 52, 54, 60–62, 64, 236, 332, 344, 345, 351, 516
Cryptography, 172, 185, 217, 229, 247
CSDR, *see* Central securities depositories regulation
CSDs, *see* Central securities depositories
CSRC, *see* China Securities Regulatory Commission

D

DCMs, *see* Designated contract markets
DDoS, 75, 107, 225, 230
Decentralized ledger systems, 152, 154, 162, 170, 172, 174–176
Democratize, 40, 235, 469, 497
Derivative contracts, 233, 286, 289, 292–294, 299, 300
Designated contract markets, 275, 280, 285, 297
DFS, *see* Digital financial services
DFS regulation, 52, 55, 57, 58
DGD, 472, 473
Digital currencies, 148, 183, 185, 194, 200, 202, 205, 210, 211, 214, 215, 228, 231, 234, 240, 241, 362, 376, 377
Digital financial inclusion, 37–40, 43, 388–392, 395, 397–402
Digital financial services, 45, 46, 48, 51, 52, 54, 55, 57–59, 378, 379, 389, 391, 392, 398, 457
Digital technologies, 39, 363, 369, 372, 381, 382, 388, 390, 402
Digix, 472–474, 479
Disrupt, 2, 3, 32, 194, 224, 226, 249, 438, 442, 447, 505
Distributed ledger technologies, 146, 147, 161, 176, 225, 244, 246, 247
Distributed ledger technology, 147, 164, 165, 225, 244, 246, 247
DLS, *see* Decentralized ledger systems

DLT, *see* Distributed ledger technology
Double-spend, 148, 182, 186, 215

E
e-Commerce, 2, 3, 21, 29, 30, 41, 48, 51, 59, 60, 66, 70, 73, 74, 81, 88, 93, 376, 380, 381
eBay, 2, 3, 73, 353, 354, 358
Effecting transactions, 198–200
Electronic exchanges, 274, 279, 280, 282, 306, 311, 315, 324
EMIR, *see* European market infrastructure regulation
EMVCo payment tokenization specification, 117, 125, 126, 128–130, 141
ETFs, *see* Exchange-traded funds
Ethereum, 155–158, 169, 171–174, 181, 245, 247, 251, 254, 256, 258, 262, 264, 265, 312, 472, 474–476
Ethereum blockchain, 173, 258, 259, 262–264, 473, 474
Ethereum Classic, 173, 263–265
European market infrastructure regulation, 274, 284, 286, 288, 291–301, 303–305, 322
Exchange Act, 189–192, 196–199, 201, 202, 204
Exchange-traded funds, 26, 483, 484, 486, 487, 489, 490
Exclusion, 197, 198, 363, 365, 366, 381, 466, 468, 469

F
Facebook, 227, 336, 343, 345–347, 355, 358, 406, 417, 418
Fail-stop fault, 150
Field office managers, 437, 438, 443, 444
Field Officer Mobile Module, 438, 440–443
Field offices, 434, 436, 437, 442, 443, 445, 447
Financial cloud, 75, 77–79, 81, 82
Financial exclusion, 68, 362–367, 369, 451
Financial inclusion, 32, 37–40, 51, 362, 363, 369, 370, 373, 374, 376, 377, 380, 387–390, 397–399, 405, 407, 420, 448, 449, 456–459
Financial innovation, 38, 40, 43, 52, 62, 350, 355, 451–453, 455, 456
Financial institutions, 2, 36, 39, 46, 47, 53, 68–70, 174, 175, 213, 217, 218, 224–226, 228, 229, 234, 248, 249, 375, 376, 451, 452
  traditional, 2, 15, 46, 68, 69, 431, 455
Financial market infrastructures, 195, 244, 245, 248–251, 253–257, 259, 265, 266, 287
Financial sector, 3, 51, 52, 78, 172, 245–251, 266, 409, 421, 452, 455
Financial service net, 364, 376, 382, 384
Financial services, 2, 38–40, 43, 68, 69, 81, 241, 333, 334, 362–371, 383, 388–390, 397–399, 417, 419, 420, 456, 457, 468
Financial services industry, 188, 192–194, 196, 211, 367, 394, 515
Financial technology, 43, 333, 334, 336, 341, 350, 355, 358, 396, 451, 456
Financial Times, 60, 61, 269
Financial world, 245, 246, 251, 452
Fintech, 45, 58, 62, 241, 424, 426, 448, 451, 454–457, 459
Fork, 148, 159, 160, 174, 177, 254, 259–266, 479
Frontier, 69, 158, 406, 417

G
GDP, *see* Gross domestic product
Global financial institutions, 213, 217–226, 228, 230–233, 235
GNU, 167, 171, 173, 260
GoJek, 348
Google, 66, 79, 135, 140, 150, 227, 336, 354, 357, 358, 496, 497, 515
Gross domestic product, 3, 4, 11, 17, 67, 68, 357, 466, 512

H
Hard fork, 158, 260–266, 479
Hash functions, 308, 309, 319
Hashcash, 215, 230, 242
HCE service, 133, 135, 136
HCE-based mobile payment services, 135–137
Homestead, 158
Hyperledger, 151, 152, 161, 162, 172, 173, 246, 311

I
ICO, 184, 258
Immutability, 186, 246–248, 321, 323

In-store mobile payment, 116, 125, 129, 141
Inclusive growth, 448, 464, 468, 469
Indonesia, 341, 348, 368, 389, 393–395, 398, 401, 431–434, 436, 437, 442, 447, 448
Institutions, non-financial, 51, 53, 63
International Organization of Securities Commissions, 249, 285, 287
International organizations, 219, 220, 235, 236, 238, 239
Internet banking, 46, 47, 423
Internet finance, 15, 19, 29, 30, 52, 64, 68–70
Internet payment services, 46, 55, 56
Interoperability, 66, 224, 392, 397, 398, 459
Investigation, big data credit, 69–72
Investment firms, 277, 278, 281, 288, 289, 292, 301, 317, 318
Investment services, 278, 279, 287, 288
Investment Services Directive (ISD), 287–289
IOSCO, *see* International Organization of Securities Commissions
IPFS, 176

K

Kabbage, 349, 352, 358
Kenya, 347, 348, 362, 368, 372, 373, 377, 378, 389, 390, 421, 423, 458, 467
Kickstarter, 344, 345, 349, 358, 515, 516
Knowledge map, 75, 77, 79

L

Largest banks, 2, 375, 397, 398, 419
Latin American Countries (LAC), 376, 380, 381
Layers, 77, 85, 97, 110, 111, 154, 167, 169–171, 236, 238, 307, 382, 496, 503
Leapfrog, 236, 401, 406, 501
Ledger, 163, 168, 175, 195, 214, 223–225, 231, 247, 253, 259, 261, 265, 306–309, 318, 321–323
Limit order book, 275, 277, 280
Linus, 259
Loans, 15–17, 39, 40, 42, 46, 49, 50, 57, 73, 74, 79, 80, 206, 238, 349, 411–414, 432, 435, 436, 442, 443
LOB, *see* Limit order book
London Stock Exchange, 277, 291, 315
LSE, *see* London Stock Exchange

M

M PESA, 347, 348, 372, 377, 390, 421–424, 458
Malaysia, 350, 393, 397, 401
Market capitalization, 4, 14, 494
Market makers, 183, 283, 289
Market participants, 223, 273, 274, 276, 281, 282, 284, 297, 299, 304, 305, 324, 429, 466
MarketRiders, 484–486
Markets in Financial Instruments Directive, 274, 277–279, 284, 286–292, 298, 299, 301–303, 305
Member countries, 219, 220, 240
Metropolis, 158, 353
MFIs, *see* Microfinance institutions
Microfinance, 59, 60, 236, 365, 412–414, 420, 431, 432
Microfinance institutions, 401, 431–437, 442, 443, 445–448
MiFID, *see* Markets in Financial Instruments Directive
Mining, 153, 157–161, 263, 306
MNOs, *see* Mobile network operators
Mobile applications, 72, 85, 102–106, 111, 135, 137, 399
Mobile banking, 375, 381, 383, 395–397
Mobile computing platform, 85, 88, 95, 97
Mobile devices, 102, 103, 105, 106, 109, 110, 116–118, 120–124, 127, 128, 130–140, 142, 378, 433, 438, 442, 445, 448, 457
Mobile money, 368, 371–373, 377, 378, 389, 419, 422, 423, 457, 458
Mobile network operators, 134, 371–373, 392, 396–402
Mobile payment application, 131, 134–137
Mobile payment service provider, 116–118, 121–125, 129–132, 134, 138, 141, 142
Mobile payment services, 116, 118, 120, 122, 133, 136, 138, 141, 142, 373
Mobile platforms, 85, 106, 109–111
Mobile software components, 85, 111
Mobile technology, 39, 102, 362, 371, 384, 390, 392, 395, 398, 401, 442

Mobile trusted computing platform, 98, 99, 109, 110
Money transfers, 381, 396, 397, 458
MTCP, *see* Mobile trusted computing platform
MTFs, *see* Multilateral trading facility
Multilateral trading facility, 275, 278–281, 286, 288–293, 299, 303
Myanmar, 348, 368, 393, 395, 399, 401, 406–427

N

National equities exchange and quotations, 5–7, 9
National market system, 189, 191, 192, 304
NEEQ, *see* National equities exchange and quotations
Network, 146–149, 151, 153, 158, 159, 165, 169, 170, 180, 181, 183, 214–217, 225, 247, 248, 259–266, 310–312, 391, 392, 464–468
  bitcoin, 148, 260–262, 264, 310
  distributed, 169, 215–217, 225
  payment, 116, 117, 119, 122, 123, 132
Network models, 116–118, 120
Network power, 180, 181, 183, 185, 186
New paradigm in branchless banking, 59, 62, 63
New York Stock Exchange, 4, 72, 73, 80, 190, 218, 315, 482
Nodes, 79, 90, 92, 94, 148, 150–153, 155, 157, 159–161, 169, 170, 175, 180, 181, 215, 216, 247, 248, 311
NYSE, *see* New York Stock Exchange

O

Online, 2, 47, 49, 59, 63, 66, 69–72, 78, 381, 442
Open-source software, 244, 252–254, 257, 259, 260, 265–267, 269
Open-source software practices, 245, 249–252, 266
Operational risks, 244, 245, 249–253, 257, 259, 266, 269
Oracle, 50, 157, 164, 165, 174
Organized trading facilities, 275, 279–281, 286, 301, 303
OTFs, *see* Organized trading facilities

P

P2P, 2, 7, 15–21, 46, 51, 52, 54, 56, 57, 62–64, 72–74, 88, 169, 170, 236, 347, 350, 392
PAN, *see* Primary account number
Paxos, 150
Payment cards, 117, 122, 123, 127–130, 132
Payment credentials, 116, 117, 122, 125, 129, 131–133, 135–137
  user's, 116, 117, 122, 125
Payment institutions, 48, 53, 55, 56
Payment services, 50, 52, 53, 63, 121, 133–135, 399
Payment tokens, 116, 117, 120, 122–132, 134–136, 142
Payment transactions, 41, 55, 391, 392
Payment-token-based, 116, 120, 121
Payments, bill, 381, 396, 397, 399
PayPal, 121, 131, 138, 332, 343, 347, 349, 353, 354, 376
PBFT, 151, 152, 155, 160, 161
Peer-to-peer lenders, 74
Peercoin, 158, 159
Permission, 310, 415
Permissionless, 153, 171, 183, 185, 214, 215, 224, 273, 306, 310
Personal data, 229, 316, 318, 319
PEs, *see* Primary exchanges
PFMI, *see* Principles for financial market infrastructures
Philippines, 348, 368, 371, 390, 393, 394, 398, 399, 401
Point of sale, 116–121, 123, 132–136, 140, 158, 362, 517
POS, *see* Point of sale
Practical Byzantine fault tolerance, 151
Primary account number, 116, 119, 120, 122–127
Primary exchanges, 277, 278, 282, 290, 291, 298
Principles for financial market infrastructures, 249, 250, 287
Printers, 494–497, 500–502, 505, 507, 508, 510–512, 514, 516, 517, 519
Printing, 442, 493, 494, 497–520
Printing process, 495, 496, 517
Private, 153, 234
Private banks, 49, 339, 383, 410–412, 414
Private blockchains, 147, 153, 154, 156, 157, 160, 161,

223, 224, 234, 244, 251, 273, 319, 323
Private key, 138, 180, 185, 210, 229, 309
Productivity, 218, 464–470, 512
  democratizing, 469
Proof of stake, 170, 177
Proof-of-work (PoW), 148, 149, 151–153, 157–159, 161, 170, 174, 214, 215, 309, 310
Provenance, 163, 164, 232
PTB, *see* Payment-token-based
PTB and STB payment services, 116–118, 120, 121
PTB payment service, 116, 120, 121, 130, 131
PTB payment service providers, 130–132, 137, 142
Public blockchains, 147, 153, 155, 157, 171, 214, 224, 226, 244–247, 249–260, 262–266, 273
Public key, 138, 165, 167, 168, 180

Q

QFII, *see* Qualified foreign institutional investors
Qtum, 174
Qualified foreign institutional investors, 5, 25, 26

R

RAFT, 150, 174
Rakuten, 348
Regulated markets, 275, 277, 279, 280, 288, 289, 291–293, 299
Regulation of Digital Financial Services in China, 58
Repayments, 414, 436, 438
Reporting requirements, 54, 273, 275, 284, 286, 287, 289, 291, 293, 296–301, 306, 324
Resilience, 43, 170, 245, 248, 298
Retrieve, 169, 317–319
Ricardian contract, 156, 162, 172
Ripple protocol consensus algorithm, 151, 152, 160
Rise of digital finance in China, 58–63
RMB qualified foreign institutional investors, 5, 25, 26
RMs, *see* Regulated markets
Robo-advisory, 484, 486–488, 490
RPCA, *see* Ripple protocol consensus algorithm

S

Scalability, 77, 154, 175, 235, 311, 312, 488, 489
Script language, 155
Securities, engaged in the business of effecting transactions in, 198–200
Securities acts amendments, 191, 192, 196, 202
Securities exchanges, national, 197, 198, 203, 304
Securities financing transactions regulation, 284, 303, 304
Securities industry, 191–193
Securities transactions, 188–191, 200, 202–205, 305
SEHK, *see* Stock exchange
Serenity, 158
Service account credential security, 129, 131
Service account credentials, 129, 131, 138
Service providers, 56, 131, 133, 134, 362, 389
Service tokens, 116–118, 120–122, 124, 125, 130, 131, 138, 142
Service-token-based, 116, 120, 121
Services, mobile money, 418, 419, 458
Settlement, 41, 51, 160, 189–191, 194, 195, 197, 202–205, 225, 248, 249, 287, 290, 305, 313
SFTR, *see* Securities financing transactions regulation
ShangTongDai, 74, 81
Shenzhen Stock Exchange (SZSE), 4
SI, *see* Systematic internalizer
SLORC, *see* State Law and Order Restoration Council
Smart contracts, 154–158, 161, 164, 171–175, 184, 185, 231, 233, 234, 236–238, 308, 310–313, 315, 321, 472–477
Social network, 78, 103, 332, 333, 343, 346, 347, 355, 417, 451, 490
Software, 32, 85, 86, 95, 97–99, 135, 136, 174, 193, 226, 252–255, 257–266, 351–353, 465, 497, 498, 505, 513
Software code, 245, 251, 253, 255, 257, 263, 264
Software developers, 252, 253, 257, 258, 261
Software development, open-source, 244–246, 256, 259
Software development process, 253–255, 257
  open-source, 244, 251, 256, 266
Software system, component-based, 100, 101

South East Asia, 388
Square, 184, 185, 349
Standards, industrial, 126, 131, 132
State Law and Order Restoration Council, 408–410
State machine replication, 151, 154, 159, 160
STB, *see* Service-token-based
STB payment services, 116, 120, 121, 131, 132
Stock exchange, 4, 5, 7, 14, 26, 72, 80, 190, 197, 198, 201, 237, 277, 291, 313–315, 482
Sustainable development, 39, 46, 452, 453, 456, 457
Sybil attack, 148, 161
Synchrony, 152
Systematic internalizer, 280, 281, 288, 290, 299

T

TBOP, 433, 434, 436, 438–442, 444–449
TC, *see* Trusted computing
TCP, *see* Trusted computing platform
Technology companies, 5, 7, 15, 257, 314, 447
TEE, *see* Trusted execution environment
Tendermint, 151, 152, 158–160, 175, 176
Tenpay, 50
Thailand, 393, 397, 401
Third party, trusted, 164, 214, 217, 226, 228
Token assurance level, 117, 126, 128
Token provision, 122, 124, 125
Token provision process, 122, 125, 129, 130, 142
Token requestor, 116–118, 122, 124, 125, 127–130, 142, 292, 296
Token service provider, 116–118, 122–130, 141, 142
Tokens, 116, 120, 127–129, 132, 147, 153, 157, 159, 161, 172, 183, 184, 258, 261, 472, 473
TPM, *see* Trusted platform module
TR, *see* Token requestor
Traders, 206, 207, 274, 275, 278, 280–282, 300, 302, 303, 317, 318, 353, 413, 483, 490
Trading, 188, 189, 194, 197, 198, 202, 205, 210, 211, 275, 279, 280, 282, 283, 285, 286, 290, 291, 299, 301, 314, 315, 482, 483
Trading venues, 273, 274, 278, 279, 282, 290, 294, 298–303, 320
Transaction authorization, 125, 126, 129, 139, 142
Transaction authorization process, 117, 120, 122, 123, 125, 126, 128, 130, 132, 134, 137
Transaction authorization request, 119, 121, 124, 125, 130, 131, 138
Transaction report, 316–318
Transaction value, 55, 56, 136
Transaction volume, 29, 30, 128
Transfer agents, 189, 190, 193, 196, 197, 204, 205, 211
Transform finance, 241, 242
Trust, 40, 84–98, 100, 101, 103, 104, 109, 110, 163, 180, 182, 183, 185, 186, 217, 227–229, 232, 233, 237, 238, 247, 437
influencing, 87, 88, 93
Trust characteristics, 85, 88
Trust concept, 86, 88
Trust evaluation, 85, 88–90, 92, 94, 100, 104
Trust management, 85, 93–97, 100, 101, 106, 109–111
Trust modeling, 85, 87, 88, 95, 110
Trust models, 88, 89, 92, 95, 104, 168
Trust relationship, 84, 88, 93, 94, 101
Trusted computing platform, 85, 95–99, 109, 111
Trusted computing, 85, 95, 97–99, 106, 109, 111
Trusted execution environment, 109, 133, 136, 137
Trusted platform module, 95, 98, 99
Trustee, 84, 86–88, 92, 101
Trustor, 84, 86–88, 92, 97, 101, 102
Trustworthiness, 85, 94, 95, 100, 101, 103, 110, 247, 370
TSP, *see* Token service provider
Turing complete, 155

U

Uber, 227, 354, 358, 422, 423
UBS Group Technology, 231
UFA, *see* Universal financial access
Unbanked, 376
Underserved, 32, 39, 45, 49, 236, 451, 452, 456, 457, 459, 483
UNDP, *see* United Nations Development Programme
Unified payments interface, 373, 375, 376, 382
United Nations Development Programme, 413, 414, 420

Universal financial access, 368, 448, 457
UPI, *see* Unified payments interface

V
Venmo, 347
Venues, 201, 274–281, 287, 289–291, 301, 302, 320, 321
Vietnam, 348, 368, 393–395, 401, 418

W
Wave money, 418, 419, 423
WeChat, 50, 121, 138, 343
Wi-Fi, 32, 406
Workers, 11, 19, 20, 466, 467
World Bank, 219, 240, 369, 371, 387, 416, 457, 470
World Economic Forum, 219, 241, 500

Y
Yirendai, 72–74, 80
YiSou, 75, 78

Z
Zcash, 256, 258, 423
ZhiChengAFu, 74
Zhong An, 336, 337