Course name: Blockchain

Lecture: Blockchain

Lecturer Radjabov Jamsher

BLOCKCHAIN IN RESEARCH & EDUCATION

1. Blockchain's Bitcoin origins
   - Libertarians and Wall Street get into bed together
2. Using blockchain in research & education
   - Rounding up some potential use cases
3. What's next?

ABOUT JISC

- Not-for-profit company serving the HE, FE and skills community:
  - 18 million users of **shared services** like Janet, eduroam, JiscMail, shared data centres
  - Devising **national deals** with IT vendors and publishers, e.g. Amazon, Google, Microsoft, Elsevier and Springer
  - Providing **advice & guidance** to the sector on digital technologies in research and education
- My role:
  - Leading a small group exploring emerging technologies like Augmented Reality and brain computer interfaces
  - Helping institutions devise/implement digital strategies and building evidence base around new technologies

1. BLOCKCHAIN'S BITCOIN ORIGINS

BLOCKCHAIN'S BITCOIN ORIGINS

How we got here, part 1

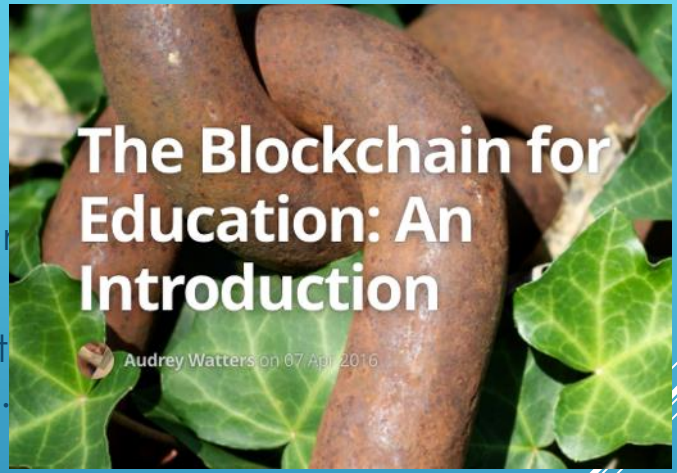
- 2007: "Satoshi Nakamoto" allegedly begins development of the Bitcoin virtual currency
- 2009: Version 0.1 of Bitcoin is released on SourceForge, and the first transaction takes place
- 2010: Programmer buys pizza for 10,000BTC (now worth $39,454,600!)
- 2011: Silk Road "dark web" marketplace opens
- 2011: 25% of the 21 million possible Bitcoins now generated through mining operations
- More at http://historyofbitcoin.org/

Photo CC BY-SA Flickr user fstorr

BLOCKCHAIN'S BITCOIN ORIGINS

How we got here, part 2

- Blockchain is the underlying distributed ledger technology that powers Bitcoin:
  - "The blockchain is a distributed database that provides a
    unalterable, (semi-)public record of digital transactions.
  - Each block aggregates a timestamped batch of transact
    to be included in the ledger – or rather, in the blockchain.
  - Each block is identified by a cryptographic signature.
  - These blocks are all back-linked; that is, they refer to the signature of the previous block in the chain, and that chain can be traced all the way back to the very first block created.
  - As such, the blockchain contains an un-editable record of all the transactions made."



From Audrey Watters / Hack Educatio

How we got here, part 3

- Interest in virtual currencies (honourable mention for Dogecoin here) parlayed into platforms…
- Ethereum's programmable blockchain: "how to abstract decentralised transfer of value to a generalised state transition function, supporting any application" https://www.ethereum.org/
- Namecoin's decentralised naming: "Bitcoin frees money – Namecoin frees DNS, identities, and other technologies" https://namecoin.org/
- Libertarian ideas embraced by Wall Street, government - e.g. UK's blockchain welfare trial

Dogecoin logo CC BY-SA Flickr user flyingblogspot.
More Shiba Inu goodness at http://dogecoin.com/

BLOCKCHAIN'S BITCOIN ORIGINS

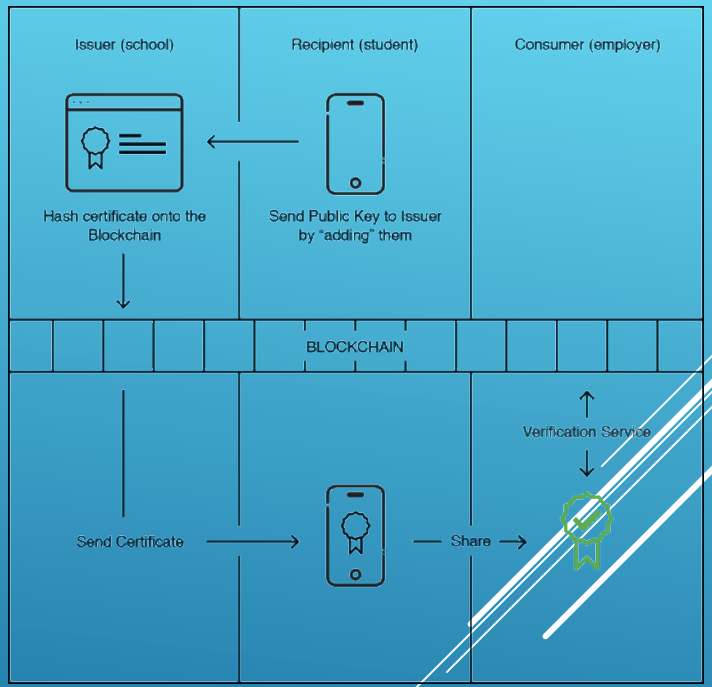
How we got here, part 3

- Interest in virtual currencies (honourable mention for Dogecoin here) parlayed into platforms…
- Ethereum's programmable blockchain: "how to abstract decentralised transfer of value to a generalised state transition function, supporting any application" https://www.ethereum.org/
- Namecoin's decentralised naming: "Bitcoin frees money – Namecoin frees DNS, identities, and other technologies" https://namecoin.org/
- Libertarian ideas embraced by Wall Street, government - e.g. UK's blockchain welfare trial

2. USING BLOCKCHAIN IN RESEARCH & EDUCATION

Credentialling

- e.g. Blockcerts from MIT et al - "Build apps that issue and verify blockchain-based certificates for academic credentials, professional certifications, workforce development, and civic records" https://www.blockcerts.org
  - Is Martin really a medical doctor? Should I let him perform brain surgery on me? (apparently he qualified in Nambia…)
  - Martin wants to transfer course to another university and take his academic credit with him
  - Martin has been doing a work placement and his employer has some feedback to add
  - Martin has lost his A Level / degree certificates…



Blockcerts activity flow - from blockcerts.org

Research provenance and reproducibility

- Blockchain could "reduce overhead and accelerate the scientific process", from http://www.blockchainforscience.com/
  - Where is the code and data linked to Martin's paper? (maybe stored on IPFS?)
  - Who has cited Martin's paper / code / data?
  - Who has re-used Martin's code and data?
  - What grants has Martin brought in?
  - What collaborators and what equipment has Martin been working with?
  - Has Martin published in enough prestigious journals to get a bonus / tenure?

Please find *document status* at the bottom of this document

MAJOR REVISION IN PROGRESS
For reading check out FILE/VERSIONHISTORY/NAMEDVERSIONS

Blockchain for Open Science and Knowledge Creation

PD Dr. med. Sönke Bartling (corresponding author, initiator and maintainer, @soenkeba, soenkebartling@blockchainforscience.com)
Founder of Blockchain For Science &
Associate researcher at the Humboldt Institute for Internet and Society

Many more contributors - please see document history.

Isn't "really good science not always a break with orthodoxy – and how could the orthodox then fairly assess it?"
(Michael Polanyi - potentially wrongly attributed or cited by the maintainer)

Efficiency, effectiveness and social value

- "Blockchain provides a new way for organisations to engage with technology to reduce cost, improve speed and transparency and integrate social value" - Nick Petford, University of Northampton VC & CEO
  - Martin's student loan is automatically approved and tuition fees paid on confirmation of his place
  - Martin's institution tracks provenance of goods and services, e.g. https://www.provenance.org
  - Martin's library fine is automatically deducted from his eduCoin account
  - Martin decides to switch to a course at another institution - credit transfer takes place automatically

CCEG SOCIAL VALUE & INTANGIBLES REVIEW

Is Blockchain Procurement the Future for UK Universities?

by **Nick Petford**
Vice Chancellor and CEO, University of Northampton, UK

Procurement in UK universities has undergone something of a mini-revolution in recent years. The renewed interest is evident in the 2013 establishment of Procurement UK, a sector-wide body with strategic oversight of procurement issues. An initiative originating from the 2011 influential report *Efficiency and Effectiveness in Higher Education* by Universities UK (UUK).

The report came out at a turbulent time. The country was in the midst of a recession, with falling governmental budgets and the cap removed from tuition fees. From a political point of view, it was clear universities had to show they were taking positive action to improve efficiencies.

Every year UK universities spend around £10bn buying goods and services, everything from energy and catering to IT systems and major construction projects. Procurement is the second biggest part of a university's budget after pay. However, procurement need not be about lowest price. There are significant opportunities for innovation and creativity in the purchase of goods and supply chain management more broadly. The UK Social Value Act 2012, yet to live up to its noble aspirations, nonetheless gives permission to develop a strategic approach to procurement that factors in both social and environmental returns. At the same time, Blockchain technology provides a new way for organisations to engage with technology (specifically Web 3.0 and the Internet of Things) to reduce cost, improve speed and transparency and integrate social value across the procurement function.

Blockchain technology provides a new way for organisations to engage with technology to reduce cost, improve speed and transparency and integrate social value across the procurement function.

University procurement is getting better, fact!

Procurement UK, working closely with regional purchasing consortia across England, Scotland and Wales and associated regulatory bodies, has helped raise the game of procurement in UK universities. For example, we have improved the profile of procurement with the inclusion of procurement themes in leadership programmes and engagement with government. We have created a Higher Education Procurement Academy (now the Higher Education Procurement Association) to aid training and development. There is now a more coordinated approach to collaborative procurement in England, helped and supported by the newly established Procurement England Ltd. The sector has moved from a baseline collaborative procurement spend of circa 10% in 2010 to close to 30% in 2016, a significant achievement. Finally, we have seen a roll-out of Procurement Maturity Assessments (PMAs) across English higher education institutions.

49 February 2017

Social Value and Intangibles Review - February 2

Your questions and potential use cases

- Blockchain for CPD & Accreditation
- Records management
- What/How should library prepare to start using blockchain applications? (e.g. IT infrastructure, knowledge)
- Blockchain for financial transactions, peer review, data management
- Transaction time and cost for ledger entries

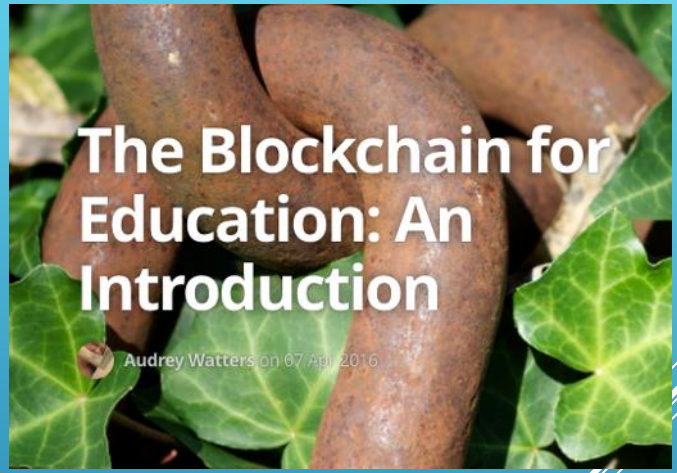
3. WHAT'S NEXT?

Avoiding the pointless blockchain project

- From Coin Sciences CEO Gideon Greenspan:
  1. Must be a database
  2. Must have multiple writers / updaters
  3. You don't trust the folk updating the database
  4. You don't need a trusted intermediary to vouch for updates / updaters
  5. Transactions are often dependent on each other
  6. Database contains rules for assessing the legitimacy of transactions
  7. Database contains a mechanism for conflict resolution
  8. Information / asset in database can be drawn down, e.g. funds transfer

How we got here, part 2 (reminder!)

- Blockchain is the underlying distributed ledger technology that powers Bitcoin:
  - "The blockchain is a distributed database that provides an **unalterable, (semi-)public record** of digital transactions.
  - Each block aggregates a timestamped batch of transactions to be included in the ledger – or rather, in the blockchain.
  - Each block is identified by a **cryptographic signature**.
  - These blocks are all back-linked; that is, they refer to the signature of the previous block in the chain, and **that chain can be traced all the way back to the very first block created**.
  - As such, the blockchain contains **an un-editable record of all the transactions made**."



From Audrey Watters / Hack Educatio

Some issues

- Public/private? cf. GDPR + initiatives like Sovrin self-sovereign identities https://sovrin.org
- Immutable? See Accenture's "chameleon hash" work http://fortune.com/2016/09/20/accenture-blockchain/
- Permissionless or permissioned?
- Real data on the blockchain, or just a cryptographic hash (fingerprint) of the real data?
- Proof of work versus proof of stake, aka "do I need to use vast amounts of compute time to mine virtual coins?"
- Transaction speed and potential scaling issues
- Hippies versus nerds ☺

Photo CC BY Flickr user arenamontanus

Conclusions

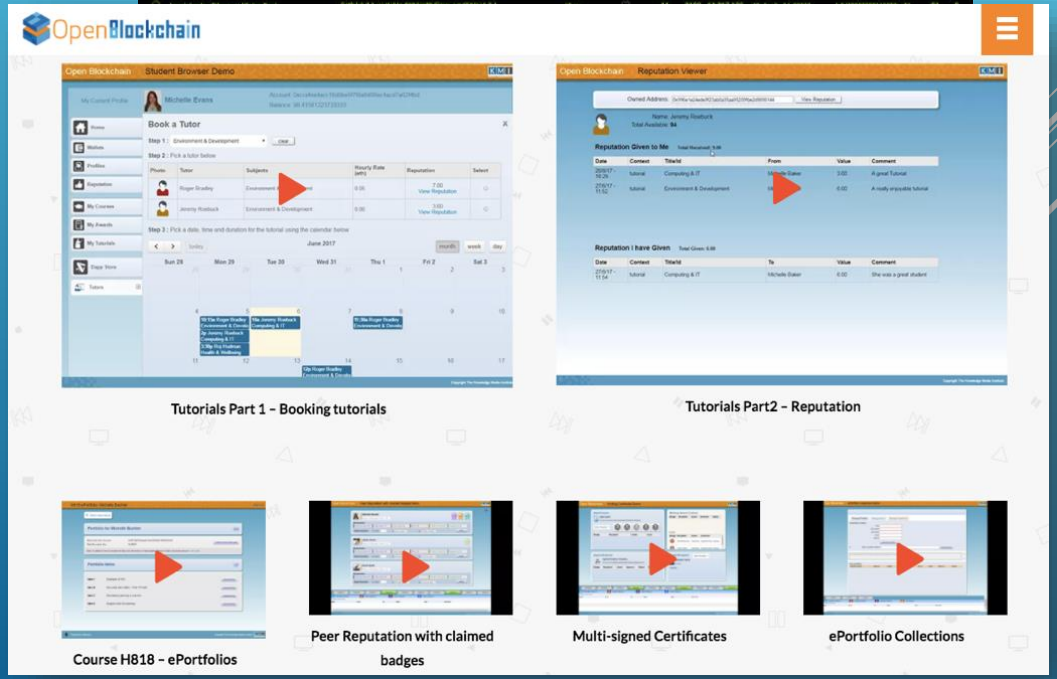
- Lots of potentially transformational applications for blockchain / distributed ledgers in research and education
- But… we are still at the "28k modem" stage, comparable with early web
- Avoid the pointless blockchain project!
- Potential collaborators are global as well as local
- Lots of interesting presentations at the recent Blockchain in Education conference https://www.bcined2017.nl
- Shout out for the OU's Open Blockchain R&D - http://blockchain.open.ac.uk
- Jisc horizon scanning report coming soon - see http://foresight.jiscinvolve.org

Ethereum network stats - from https://ethstats.ne

WHAT'S NEXT?

Conclusions

- Lots of potentially transformational applications for blockchain / distributed ledgers in research and education
- But… we are still at the "28k modem" stage, comparable with early web
- Avoid the pointless blockchain project!
- Potential collaborators are global as well as local
- Lots of interesting presentations at the recent Blockchain in Education conference https://www.bcined2017.nl
- Shout out for the OU's Open Blockchain R&D - http://blockchain.open.ac.uk
- Jisc horizon scanning report coming soon - see http://foresight.jiscinvolve.org

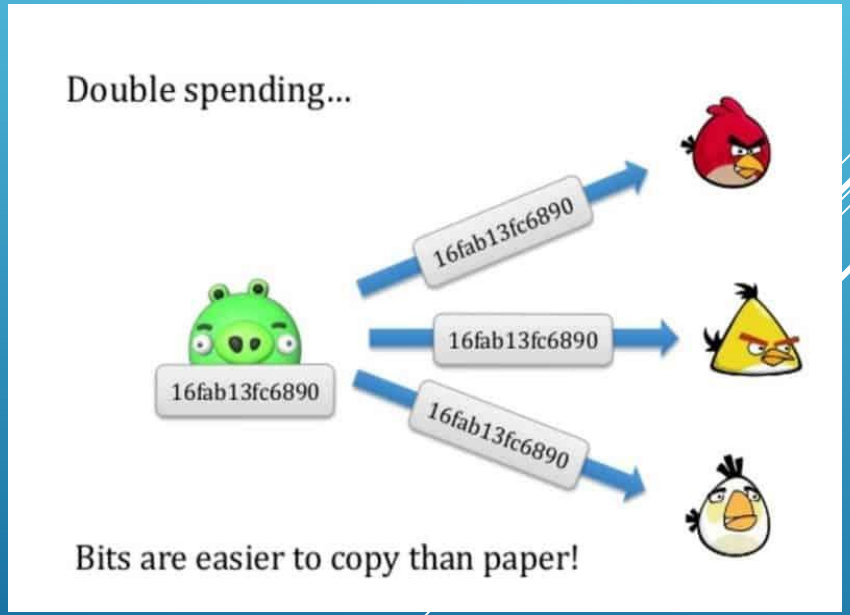


DIGITAL CURRENCY

- The most successful among lot of efforts: Bitcoin
- Replace cash with numbers and codes
- Advantages
  - Fast
  - International
  - Easy accounting
  - Weighs nothing
  - Cheap
- Problems to be solved

PROBLEMS OF DIGITAL CURRENCY

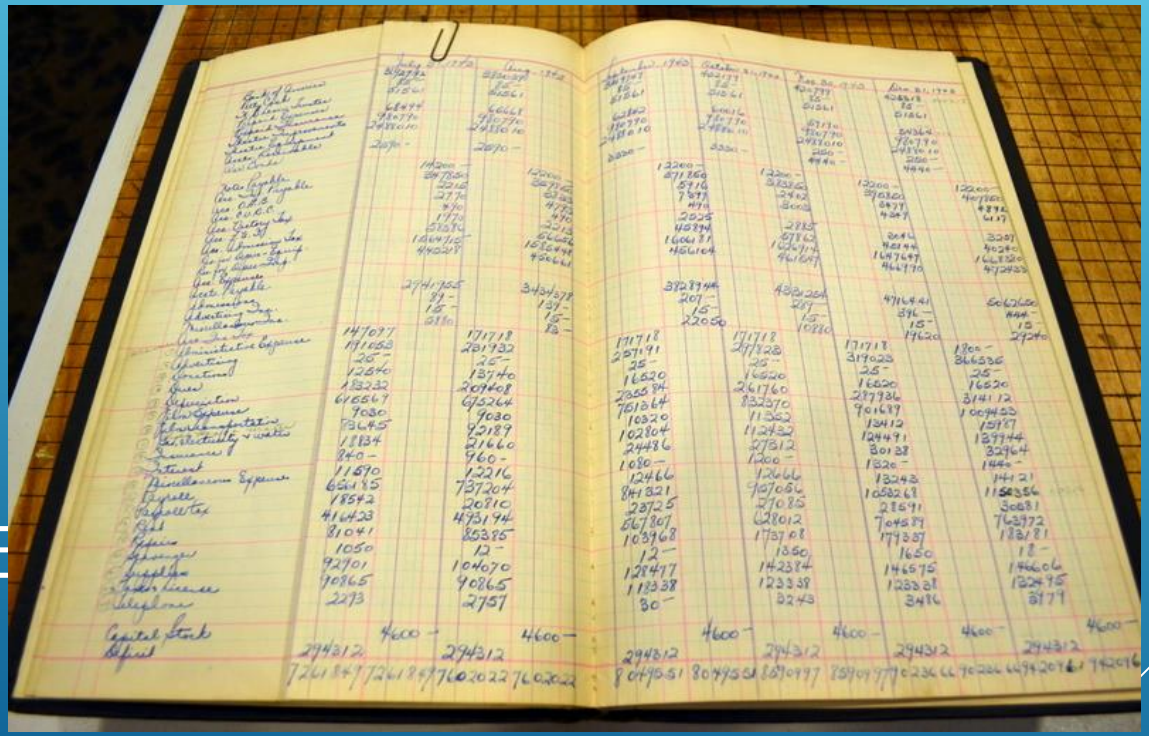
- Perfect Copy
  - Just like downloading attachment from email
  - How to distinguish counterfeits
  - Ownership Problem
- Double Spending
  - Networks are noisy and transmission across networks is far from instantaneous: delay
  - A hacker can capitalize
  - Fraudster Detection Problem



THE LONG ROAD TO BITCOIN

- Centralized Banking: not robust
- Satoshi determined to find the centralized part of banks
  - The ledger
  - "What if I could turn a bank inside out? Instead of one central party controlling the ledger, what if every user were recruited to maintain a constantly updated copy?"
- The strength of the digital was perfect copies, so copy the ledger, everywhere, instantly.
  - Any ledgers with even one common not agreeing with the masses would be discarded, leaving fraudsters powerless
- **Replace cash with Ledger!**

LEDGE



DECENTRALIZATION

- Replace cash with Ledger

Centralized Decentralized Distributed Ledgers

The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

- Permision is required for users to have a copy of the legder and participate in confirming transactions

Blockgeeks

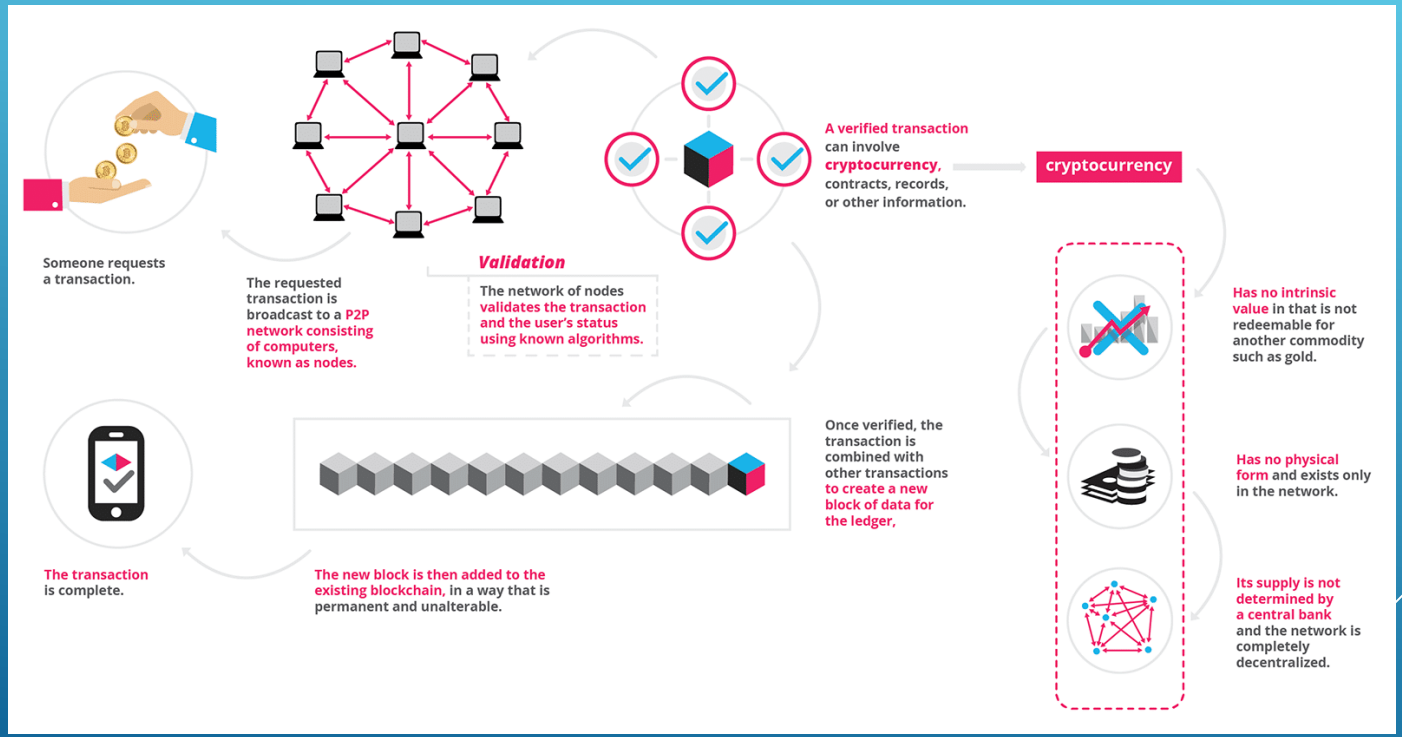
THE DECENTRALIZED LEDGER (BLOCKCHAIN)

- Decentralization: get rid of the Third Party
- Satoshi paired two main technologies
  - Proof of Work: to solve the double spending problem
  - Elliptic Curves: to solve unique access to the ledger
- Nothing was newer than 2001
  1. 2001: SHA-256 finalized
  2. 1999-present: Byzantine fault tolerance
  3. 1999-present: P2P networks
  4. 1998: Wei Dai, B-money
  5. 1998: Nick Szabo, Bit Gold
  6. 1997: HashCash
  7. 1992-1993: Proof-of-work for spam
  8. 1991: cryptographic timestamp
  9. 1980: public key crypto algorithm

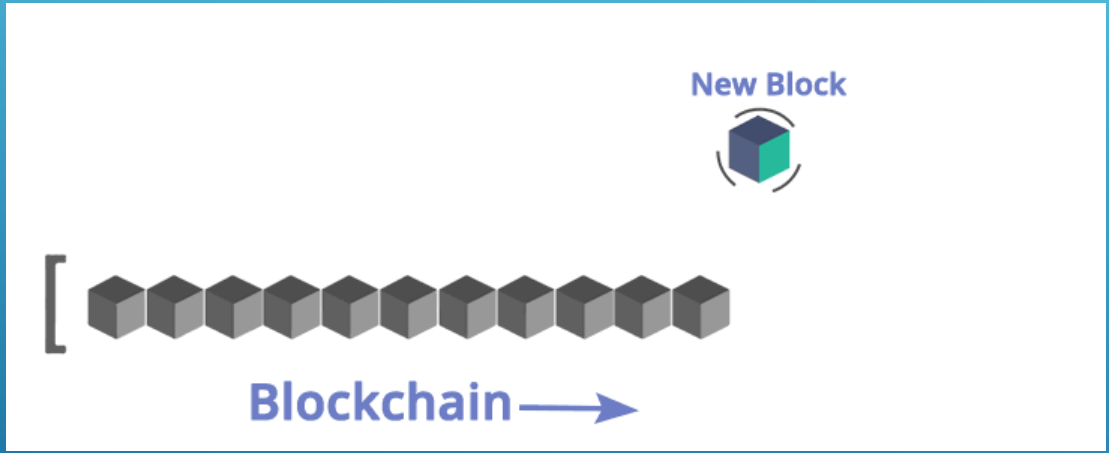
- Bitcoin stores all its transactions onto a public database called as Blockchain

WHAT IS BLOCKCHAIN TECHNOLOGY

HIGHLIGHTS

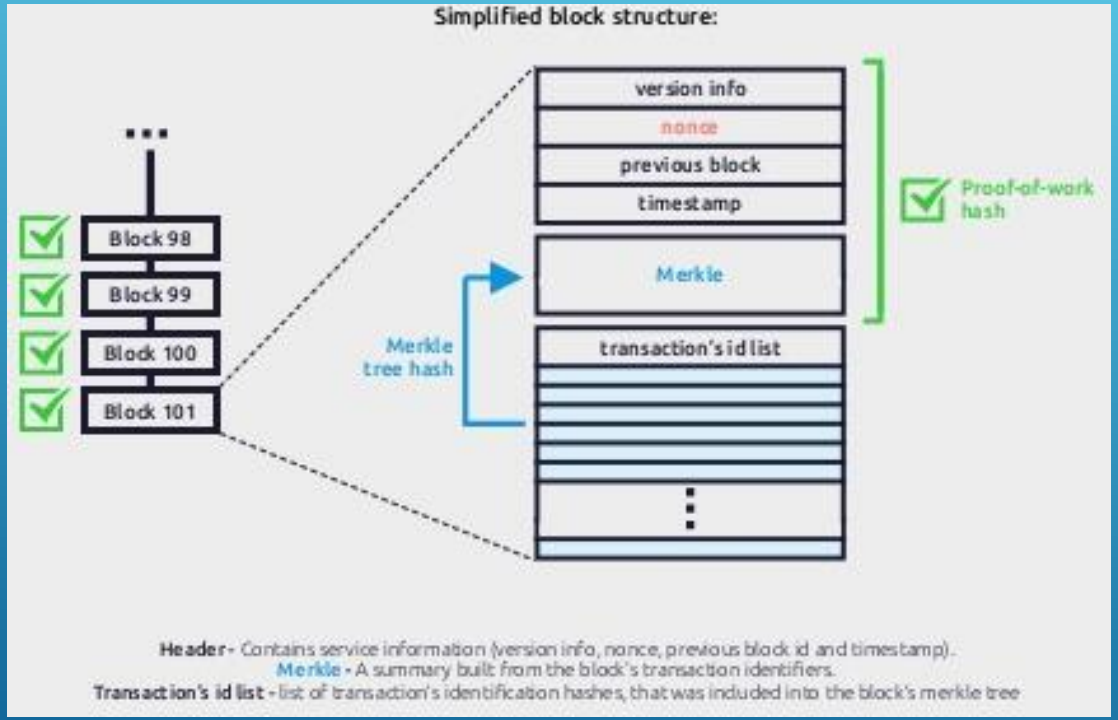

Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
cryptocurrency
Has no intrinsic value in that is not redeemable for another commodity such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger,
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

BLOCKCHAIN STRUCTURE



Source: https://www.edureka.co/blog/blockchain-tutorial/

WHAT DOES A BLOCK LOOK LIKE?



4 Key Concepts of Blockchain

Distributed shared ledger

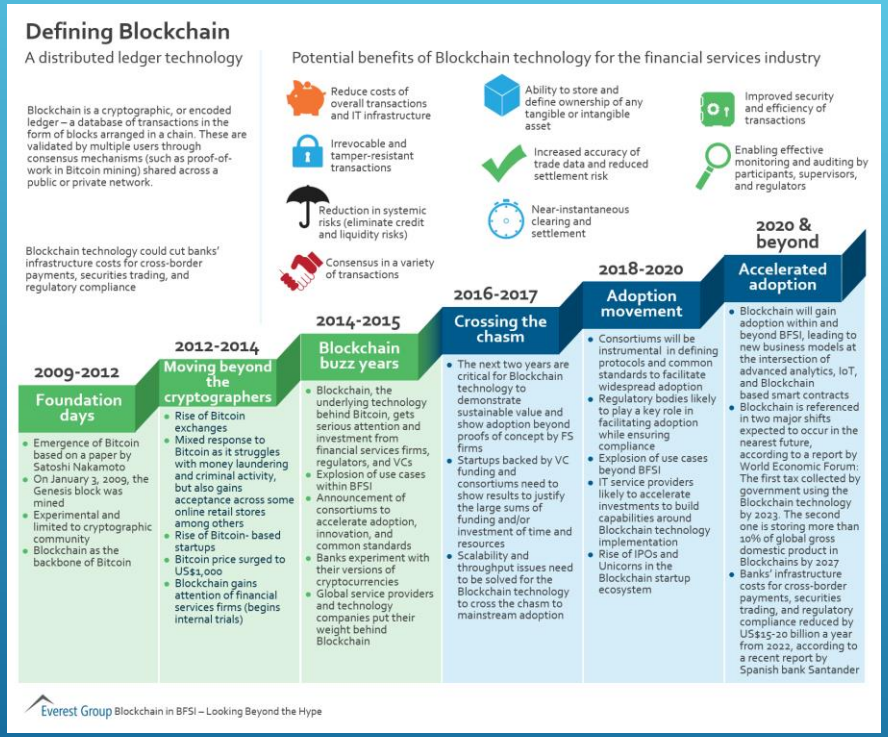
Cryptography

Consensus

Smart contracts

services

BLOCKCHAIN: DISTRIBUTED LEDGER TECHNOLOGY



BLOCKCHAIN ARCHITECTURE

- Revolutionary Technology
  - Protocol
  - TCP/IP, HTTP, Cloud Computation, Big Data, IoT, FinTech…
- Melanie Swan: Blockchain: Blueprint for A New Economy, Jan 2015
  - Blockchain 1.0
    - Bitcoin
    - Programmable Money
  - Blockchain 2.0
    - Ethereum
    - Smart Contract
  - Blockchain 3.0…
    - Non-Financial Uses
- Applications

BITCOIN SYSTEM VS. CURRENT BANKING SYSTEM

- **Decentralized System**
  - The Blockchain system follows a decentralized approach when compared to banks and financial organizations which are controlled and governed by Central or Federal Authorities.
  - Here, everyone who is involved with the system holds some power.
- **Public Ledgers**
  - The ledger which holds the details of all transactions which happen on the Blockchain, is open and completely accessible to everyone who is associated with the system.
  - Even though the complete ledger is publicly accessible, the details of the people involved in the transactions remains completely anonymous.
- **Verification of Every Individual Transaction**
  - Every single transaction is verified by cross-checking the ledger and the validation signal of the transaction is sent after a few minutes.
  - Through the usage of several complex encryption and hashing algorithm, the issue of double spending is eliminated.
- **Low or No Transaction Fees**
  - These transaction fees are however relatively quite less when compared to the fees implied by banks and other financial organizations.
  - If a transaction needs to be completed on priority then an additional transaction fees can be added by the user so as to have the transaction verified on priority.

Reference

1. The Innovation Ultimatum: Six strategic technologies that will reshape every business in the 2020s By Steve Brown.
2. Bank 4.0: Banking Everywhere, Never at a Bank By Brett King.
3. The World of Digital Payments: Practical Course By Pavlo Sidelov.
4. The PayTech Book Edited by a team of Susanne Chishti.
5. The Future Is Faster Than You Think: How Converging Technologies Are Disrupting Business, Industries, and Our Lives By Dr. Peter H. Diamandis.
6. Advances in Financial Machine Learning By Marcos Lopez de Prado
7. Financial Services Revolution: How Blockchain is Transforming Money, Markets, and Banking By Alex Tapscott.
8. The STO Financial Revolution: How Security Tokens Change Businesses Forever By Alex Nascimento.
9. FinTech Founders: Inspiring Tales from the Entrepreneurs that are Changing Finance By Agustín Rubini
10. The Innovation Ultimatum: Six strategic technologies that will reshape every business in the 2020s By Steve Brown