Course title: Innovation in FinTech

Lecture: Blockchain and Cryptocurrency Explained

Lecturer Radjabov Jamsher

Learning outcomes

Give an account of the advantages and disadvantages of the features of a specific blockchain application, namely in terms of security, decentralization and consensus attainment

Knowledge

Introduction

- Blockchain terminologies
- Distinction between databases and blockchain ledgers

Cryptographic component

- Cryptography, hash functions and digital signatures

Consensus components

- Principles and paradigms of distributed systems
- Blockchain consensus algorithms

Blockchain structures

- Blockchain structure
- Types of blockchain

Learning outcomes

Give an account of the advantages and disadvantages of the features of a specific blockchain application, namely in terms of security, decentralization and consensus attainment

Skills

- Identify blockchain characteristics in a given setting
- Analyse existing blockchain applications according to a given context
- Critically evaluate cryptography features to a blockchain application
- Identify crucial security attributes in a blockchain
- Differentiate decentralized autonomous systems, such as distributed ledgers suitable to a given blockchain application

Learning outcomes

K2 Autonomously explain the operation of a smart contract in a given blockchain scenario

Knowledge

Smart contract theory

- Smart Contract Theory and architecture
- Architectures and decentralized autonomous systems

Smart contract application

- Existing blockchain applications, related structures and architectures

Learning outcomes

K2 Autonomously explain the operation of a smart contract in a given blockchain scenario

Skills

- Select consensus algorithms suitable for specific blockchain applications
- Formalise and assess smart contracts adequate to given blockchain contexts

- Introduction
  1. Blockchain terminologies
  2. Distinction between databases and blockchain ledgers
- Cryptographic component
  1. Cryptography, hash functions and digital signatures
- Consensus components
  1. Principles and paradigms of distributed systems
  2. Blockchain consensus algorithms
- Blockchain structures
  1. Blockchain structure
  2. Types of blockchain

Table of Contents K1

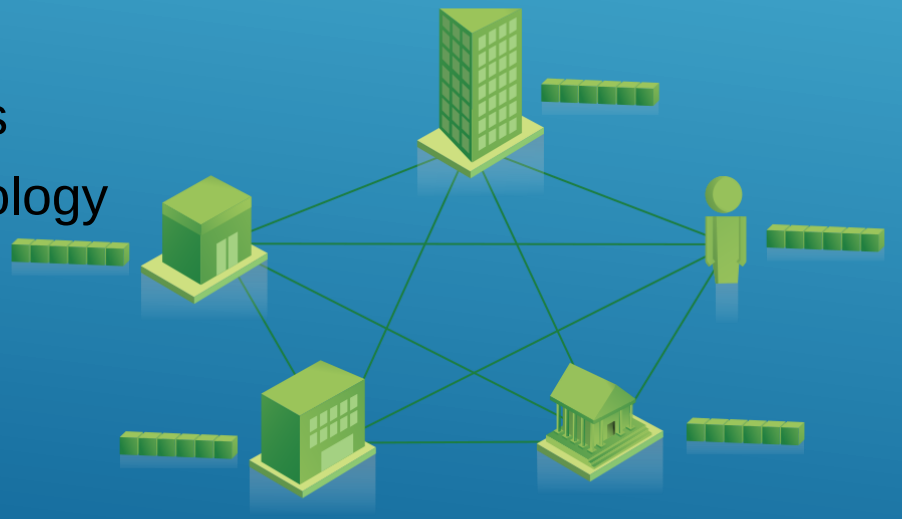
Introduction

“To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it and the idea of blockchains in general.”

- Introduction
  1. Blockchain terminologies
  2. Distinction between databases and blockchain ledgers
- Cryptographic component
  1. Cryptography, hash functions and digital signatures
- Consensus components
  1. Principles and paradigms of distributed systems
  2. Blockchain consensus algorithms
- Blockchain structures
  1. Blockchain structure
  2. Types of blockchain

Blockchain terminologies

- **Blockchain – What is it?**
  - Aka DLT (Distributed Ledger Technology) - rudimentary shared accounting system
  - Technologically, it is :
    - Distributed database – public ledger (you can insert, select data, but **can't** update or delete data.
    - Distributed computer – execute digital contracts
    - Based on **p2p** (peer-to-peer) technology, cryptology and API

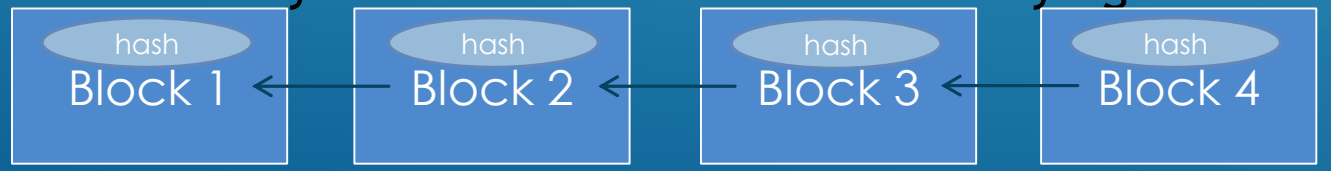


Blockchain terminologies

- **Blockchain – What is it?**

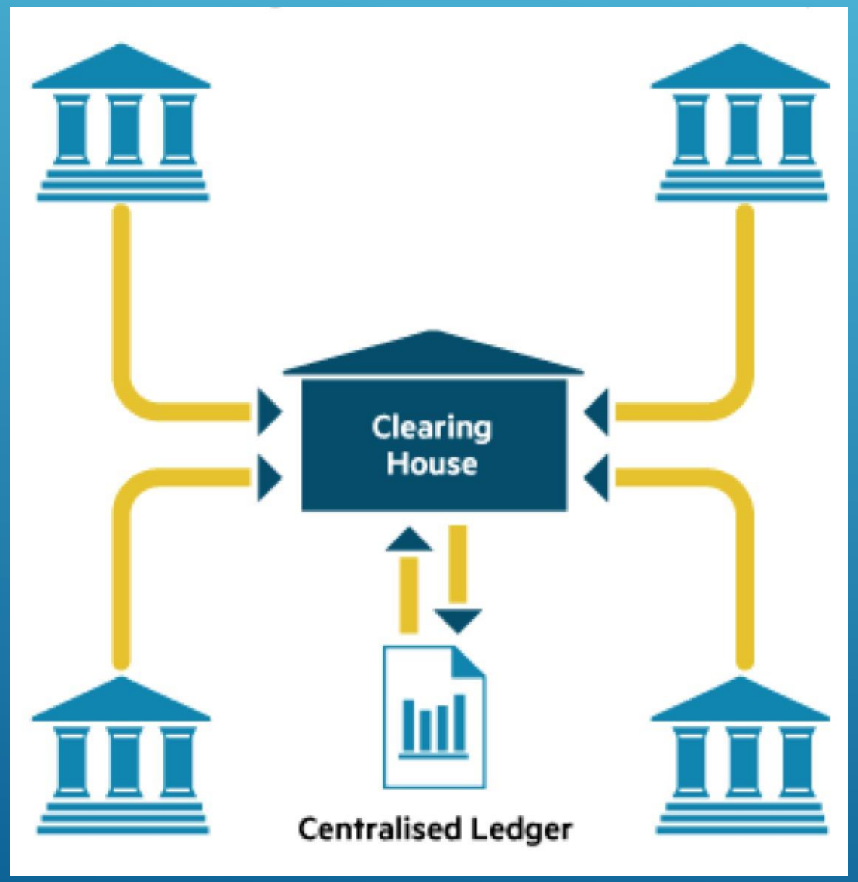
  In fact, the blockchain is more than a technology, it

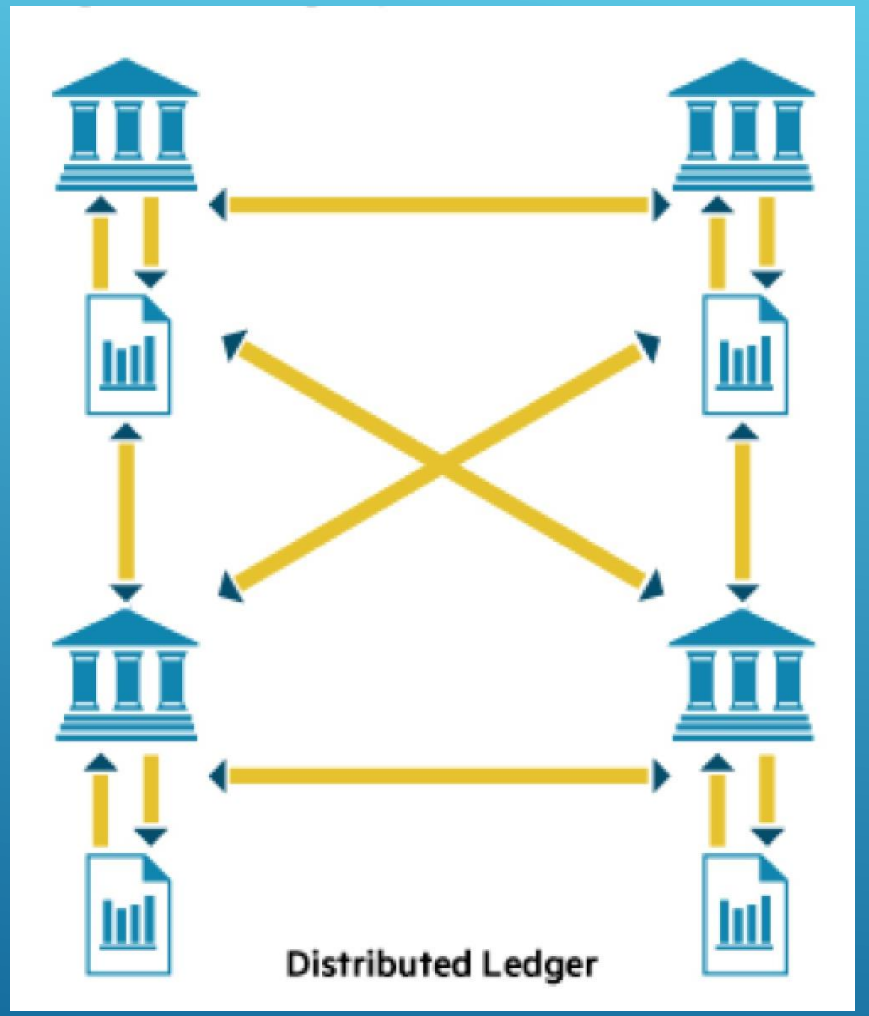
  - Usually contains financial transactions
  - Is replicated across a number of systems in almost real-time
  - Uses cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights
  - Can be written by everyone in a public blockchain (but only certain participants in a private blockchain)
  - Can be read by participants, often a wider audience
  - Has mechanisms to make it hard to change historical records, or at least make it easy to detect when someone is trying to do so



Blockchain terminologies

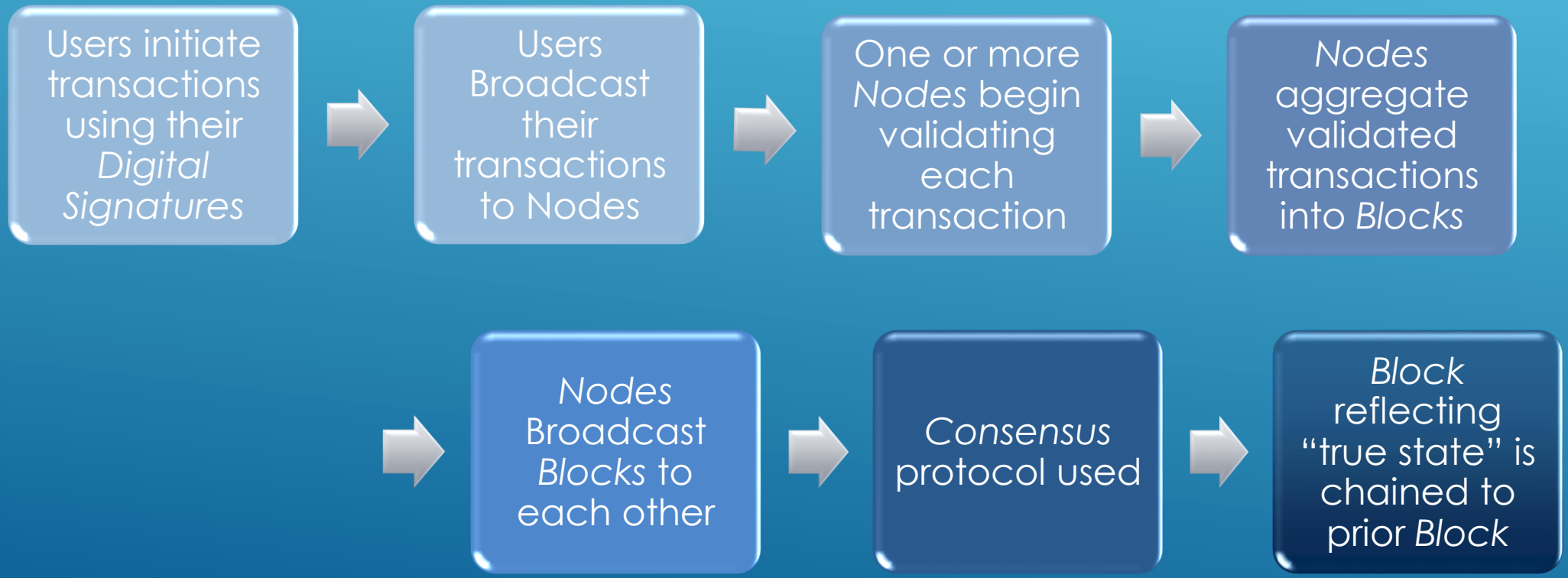
- Distributed ledger – What is it?





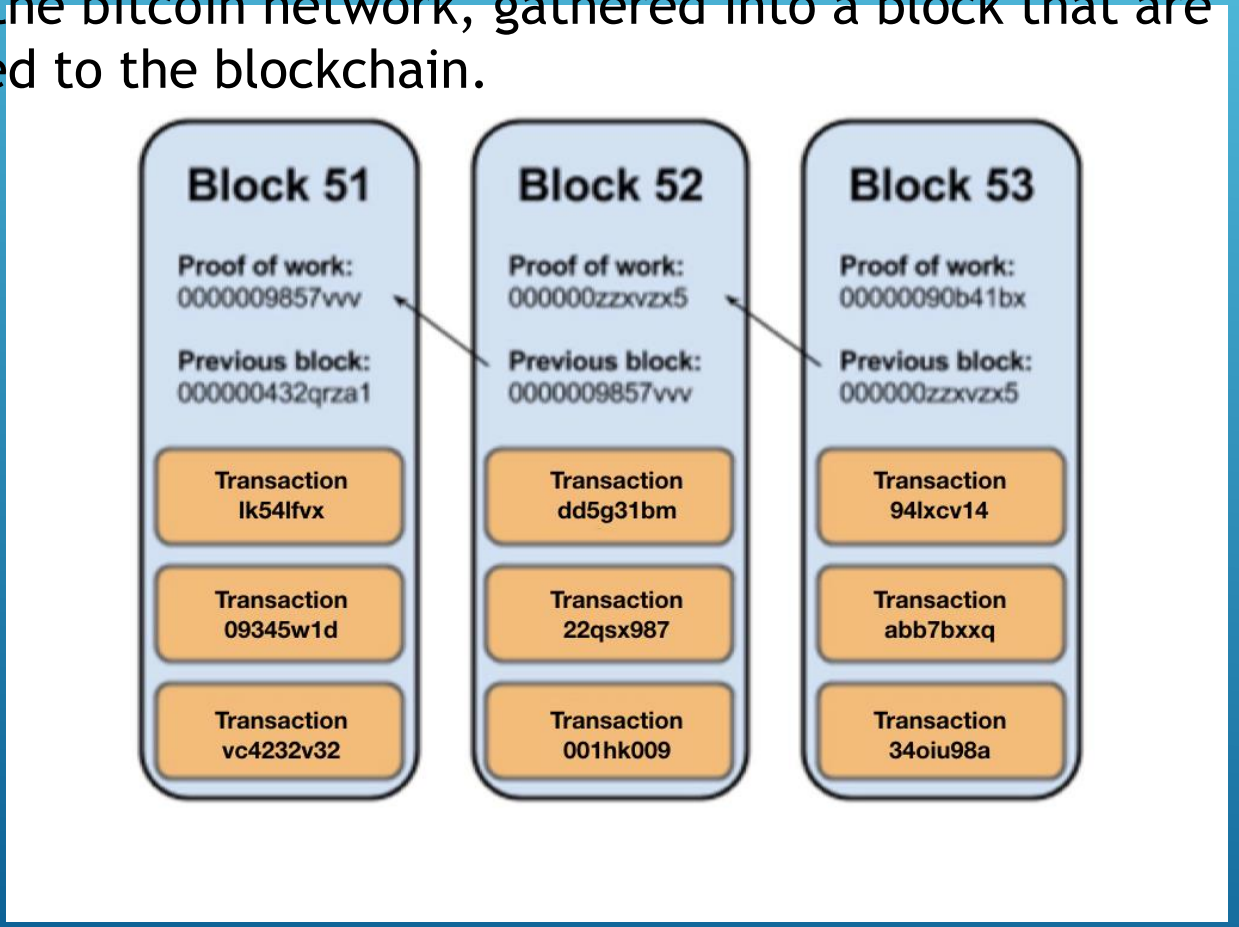
Blockchain terminologies

- **Distributed ledger – How it works?**



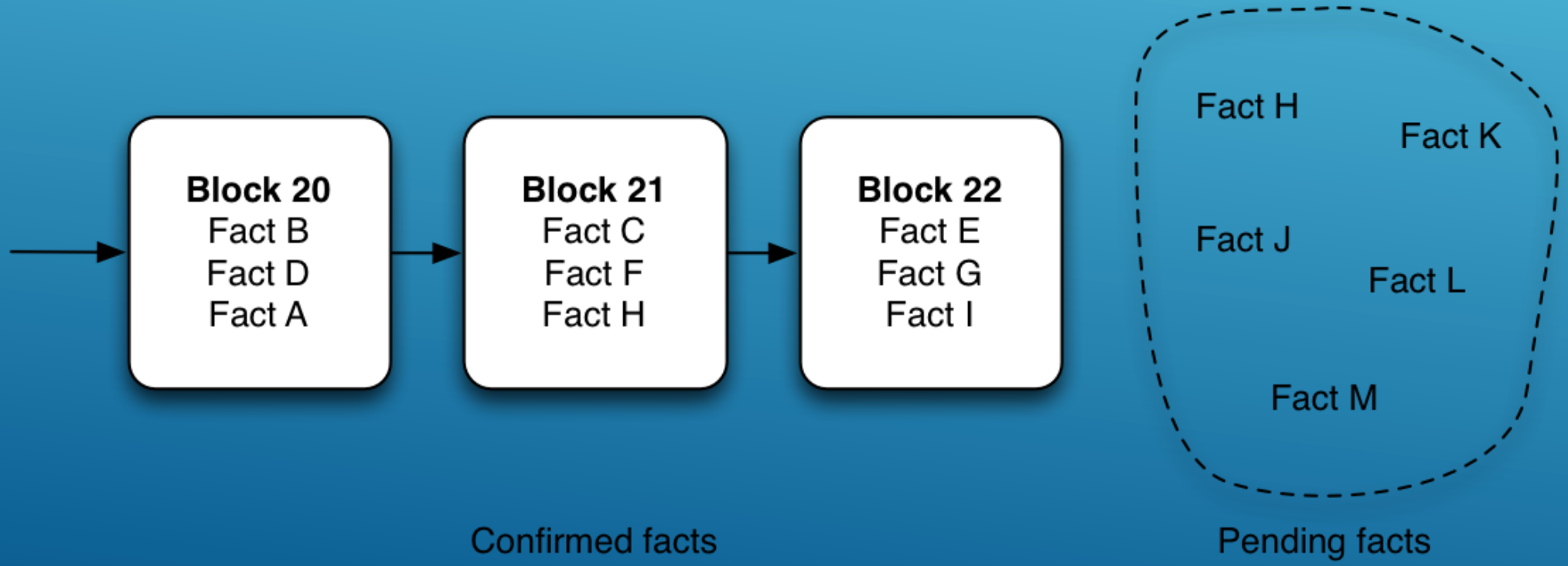
Blockchain terminologies

- **Transaction & blocks**
  - A transaction is a value transfer; a block is a collection of transactions on the bitcoin network, gathered into a block that are hashed and added to the blockchain.



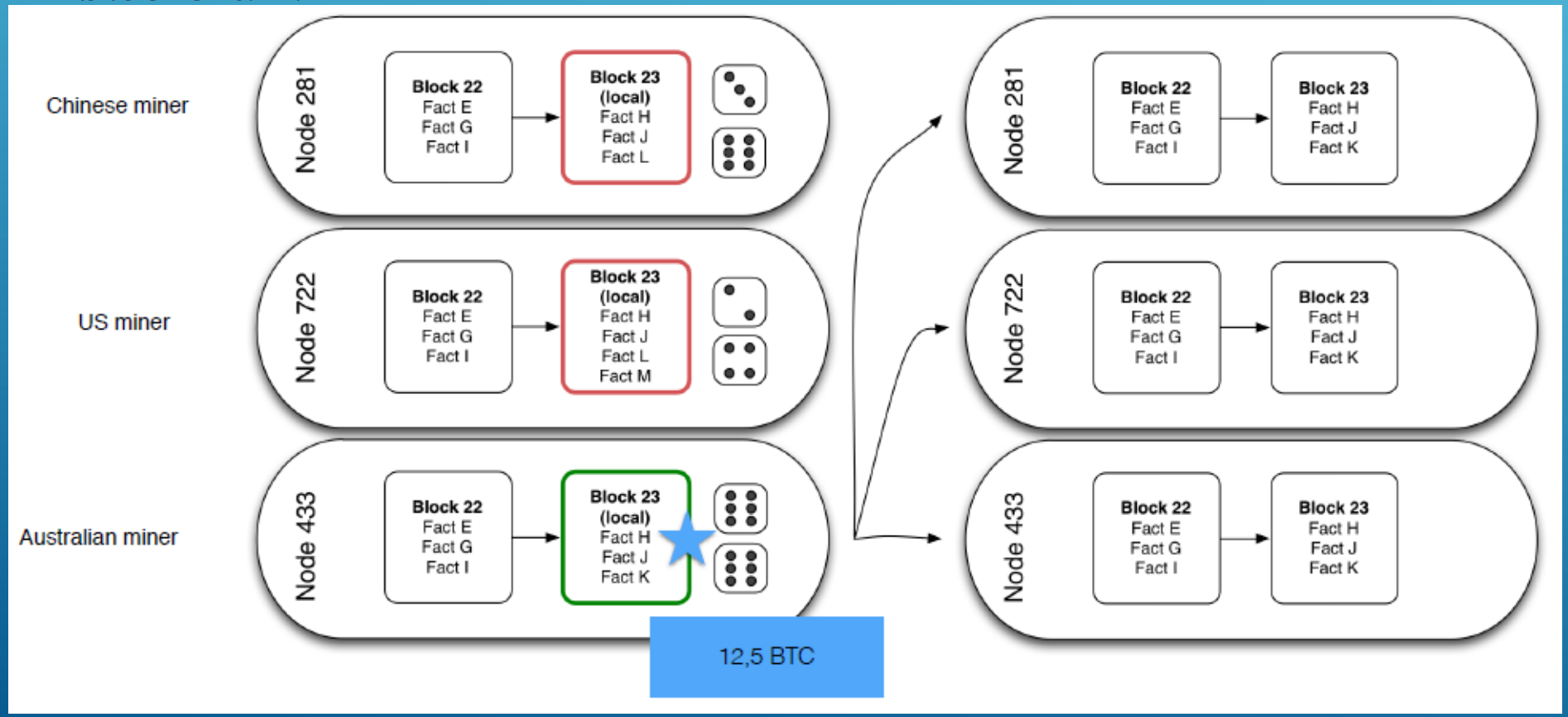
Blockchain terminologies

- **Mining**
  - This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies



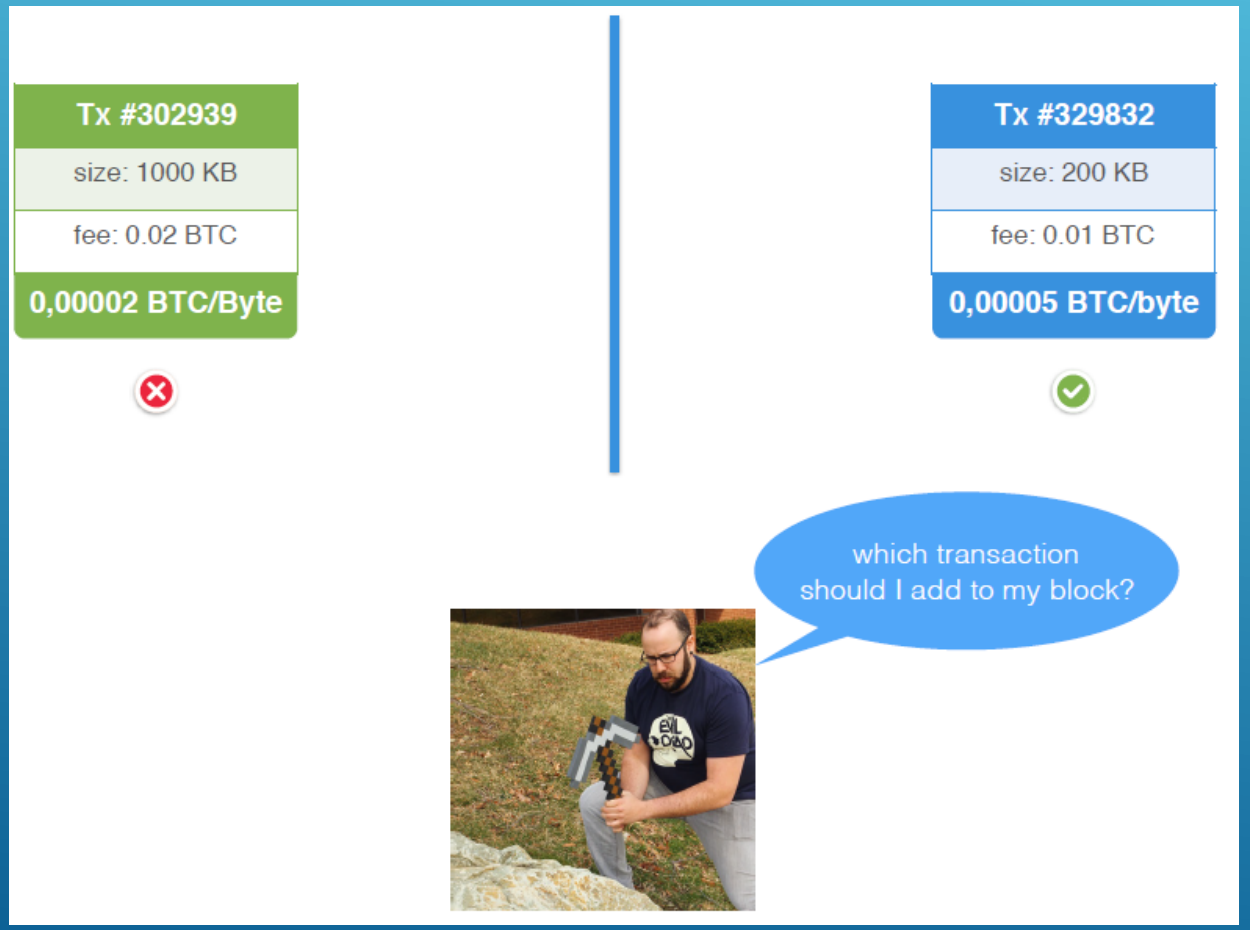
Blockchain terminologies

- **Mining**
  - The process by which transactions are verified and added to a blockchain.



Blockchain terminologies

- **Mining**
  - Miners on the network select transactions from pools and form them into a ‘block’.



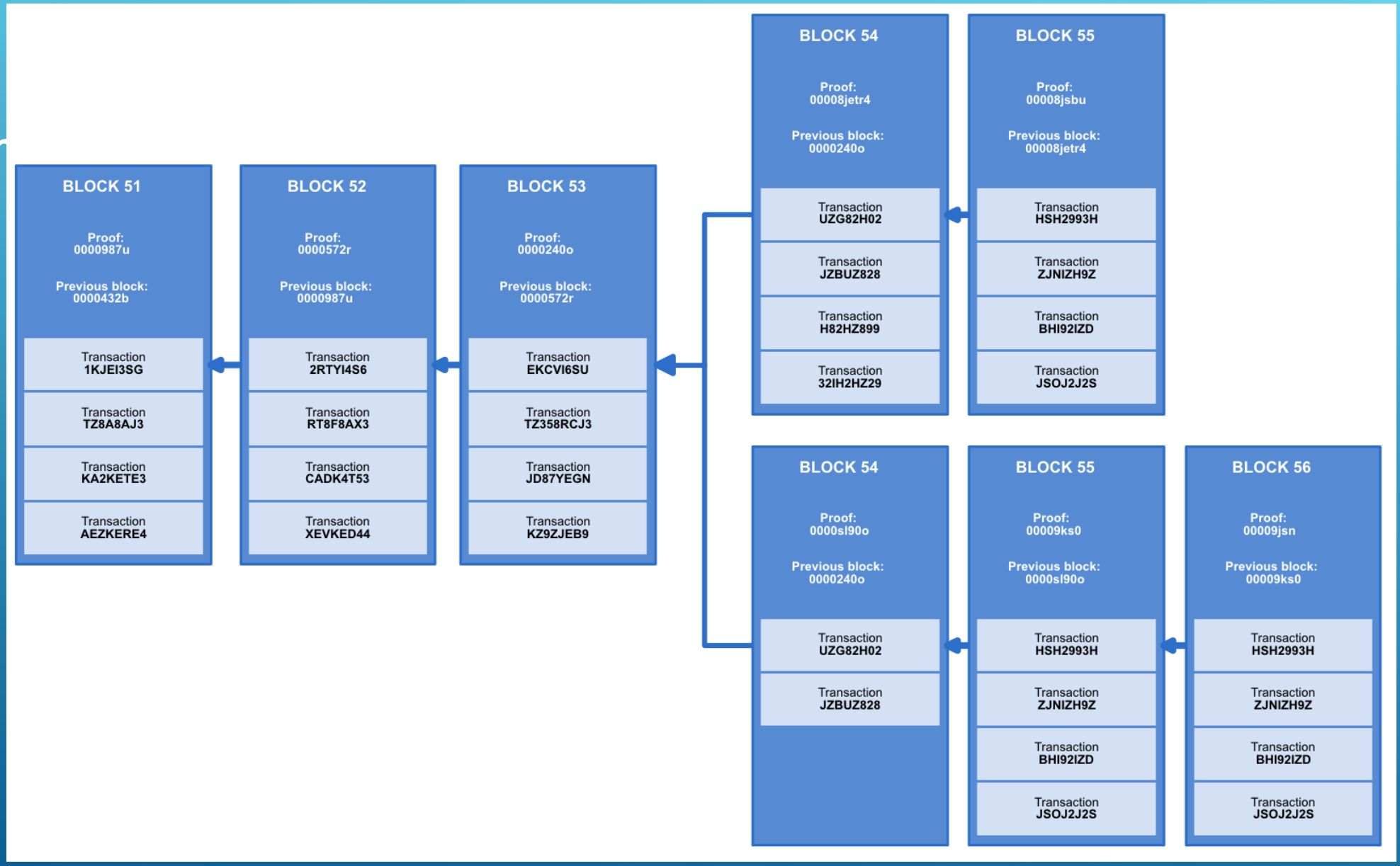
Blockchain terminologies

- **Forks**
  - A fork is the creation of an ongoing alternative version of the blockchain, by creating two blocks simultaneously on different parts of the network. This creates two parallel blockchains, where one of the two is the winning blockchain.

  - When does it happens?
    - Block found at the same time
    - Software incompatibility
    - “We don’t agree” split

Blockchain terminologies

- For



Blockchain terminologies

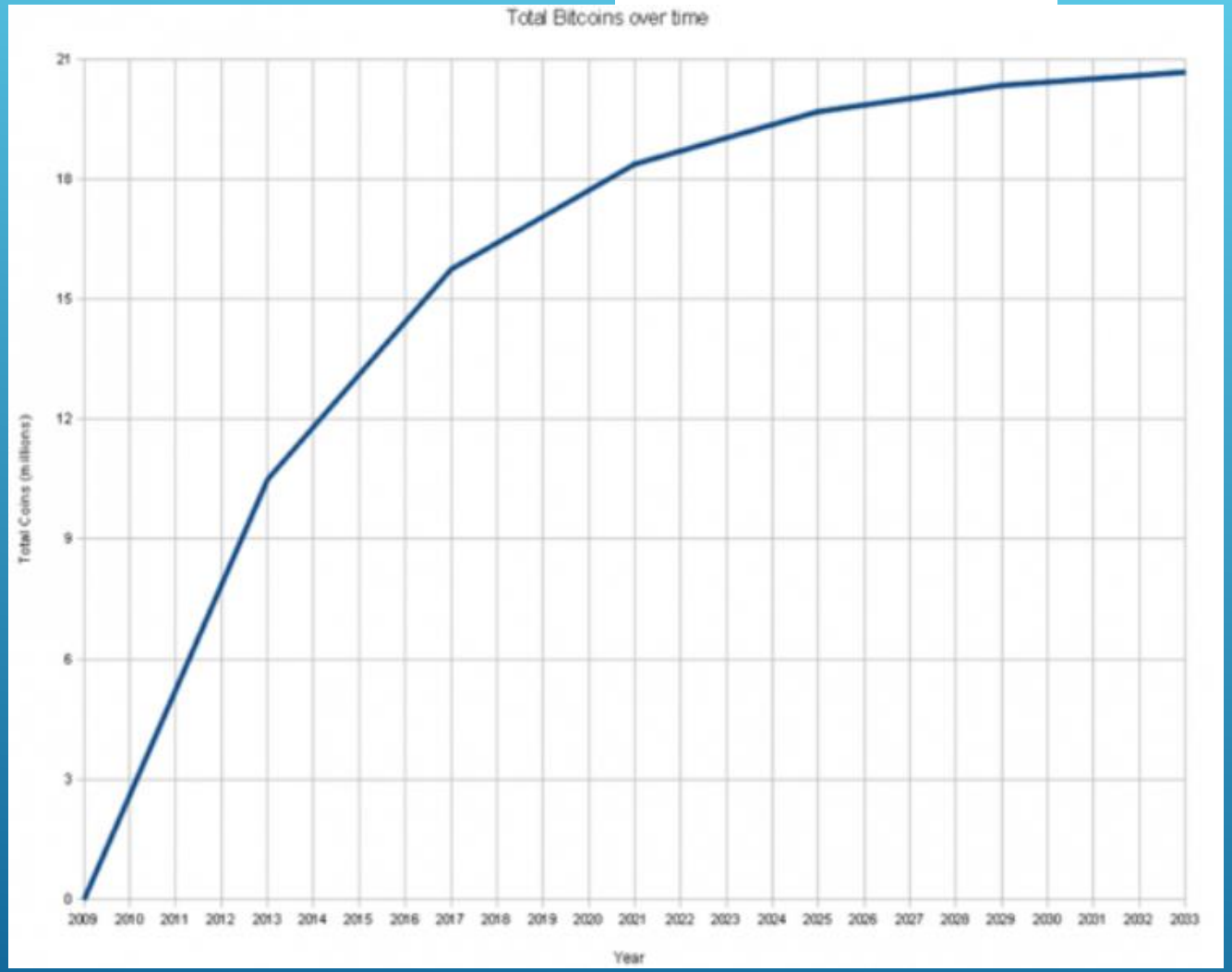
- **Bitcoin**
  - Crypto currency, first asset based on Blockchain
  - Used for drug/weapons e-commerce, ransom ware
  - Used for remittance, speculation, store of value

"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 – October 31st, 2008

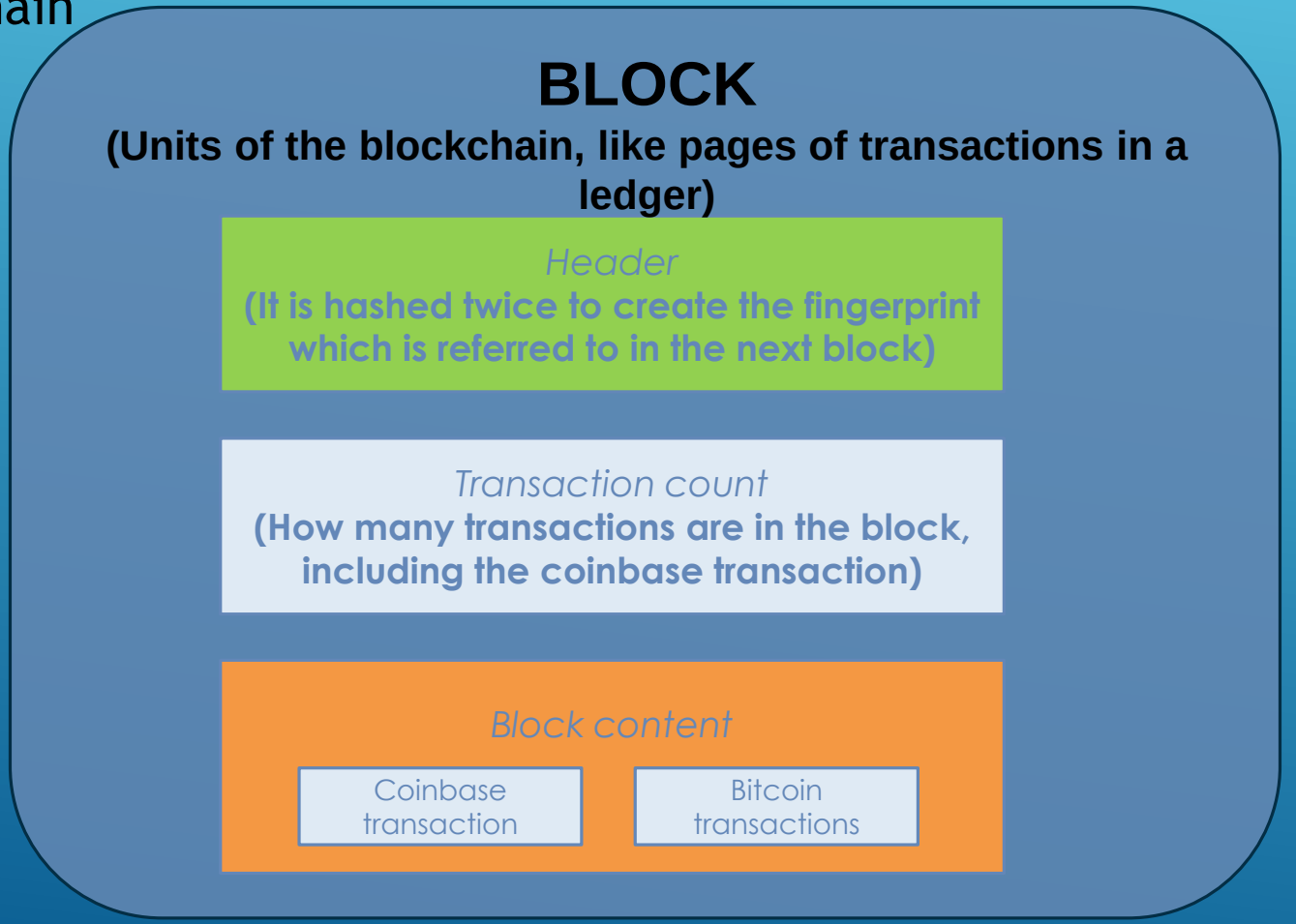
Blockchain terminologies

- **Bitcoin**
  - Monetary creation



Blockchain terminologies

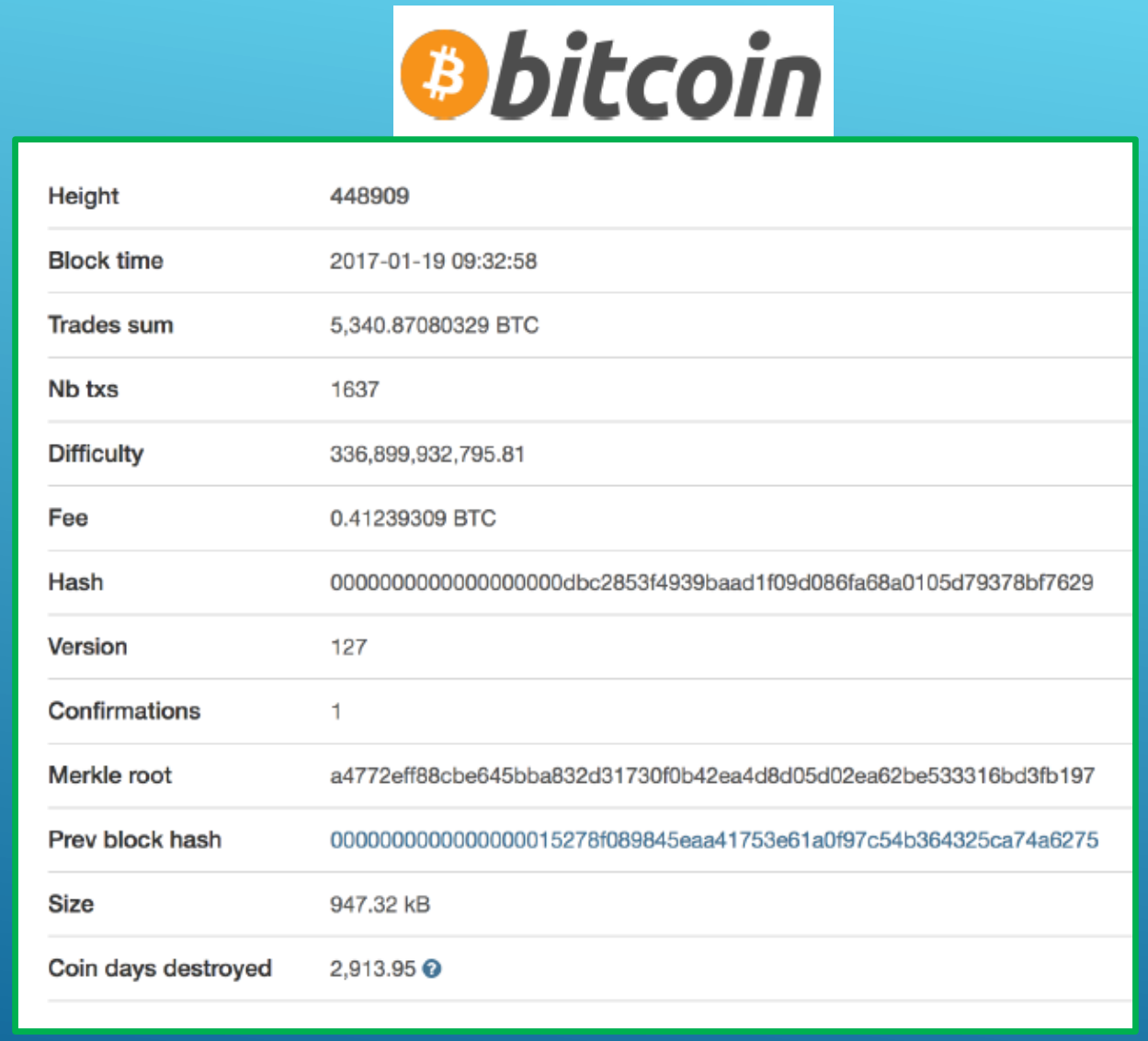
- **Bitcoin**
  - Inside Bitcoin's Blockchain



Blockchain terminologies

- **Bitcoin**
  - Inside Bitcoin’s Blockchain

  - *Block Header* : includes Technical data, Previous block hash, Merkle Root, Timestamp, Difficulty target, Nonce. Here is an example:



Blockchain terminologies

- **Bitcoin**
  - Inside Bitcoin's Blockchain

- *Block content* : Transaction Flow

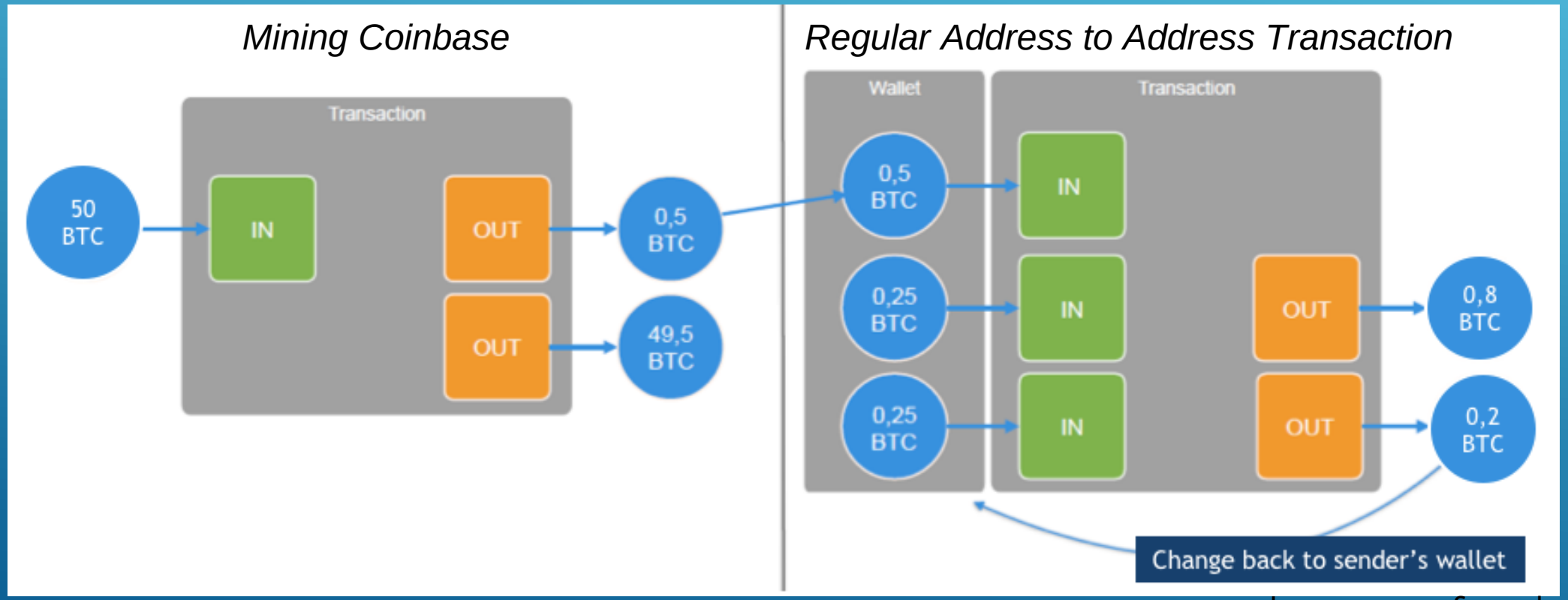
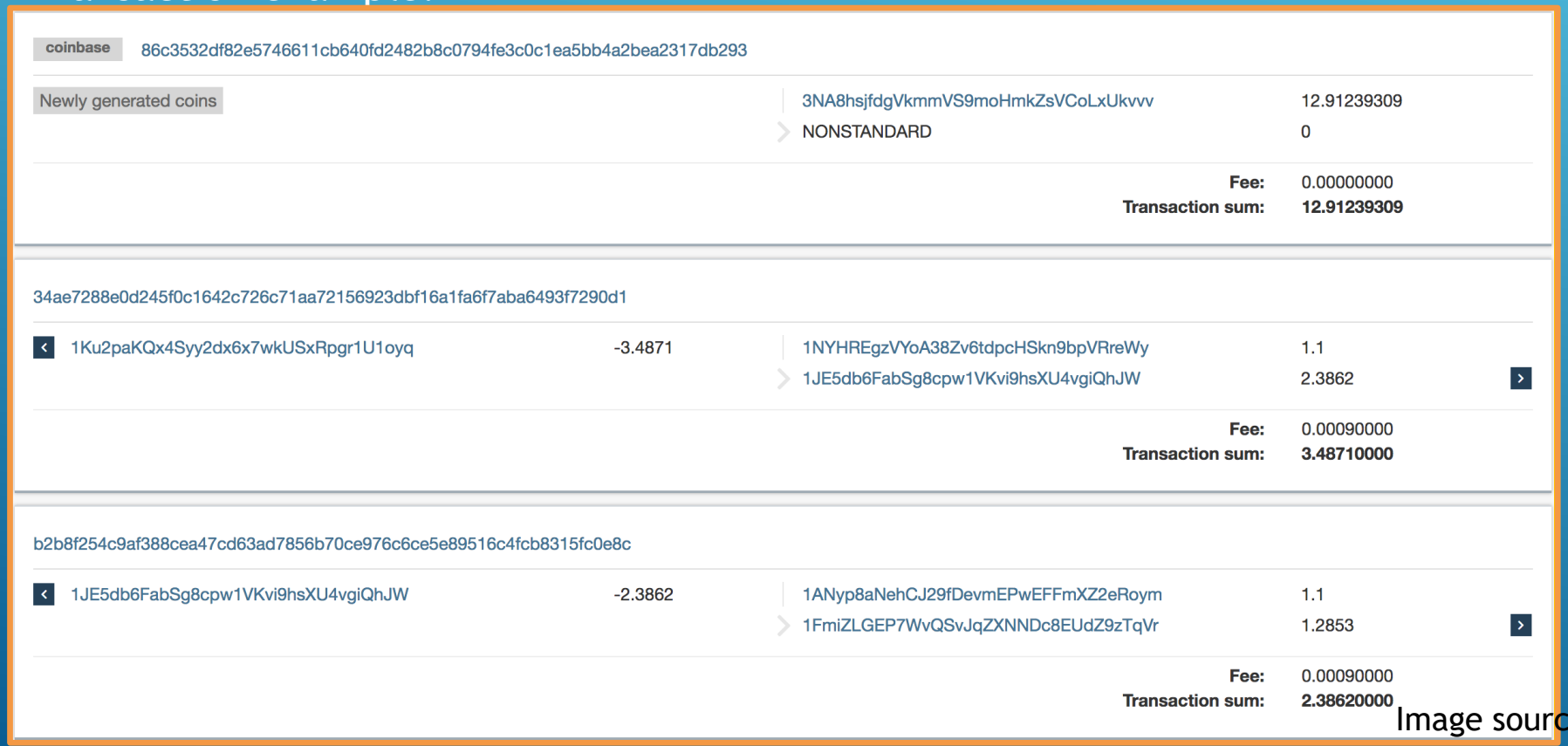


Image source: Scorechain

Blockchain terminologies

- **Bitcoin**
  - Inside Bitcoin's Blockchain

- Block Transaction example:

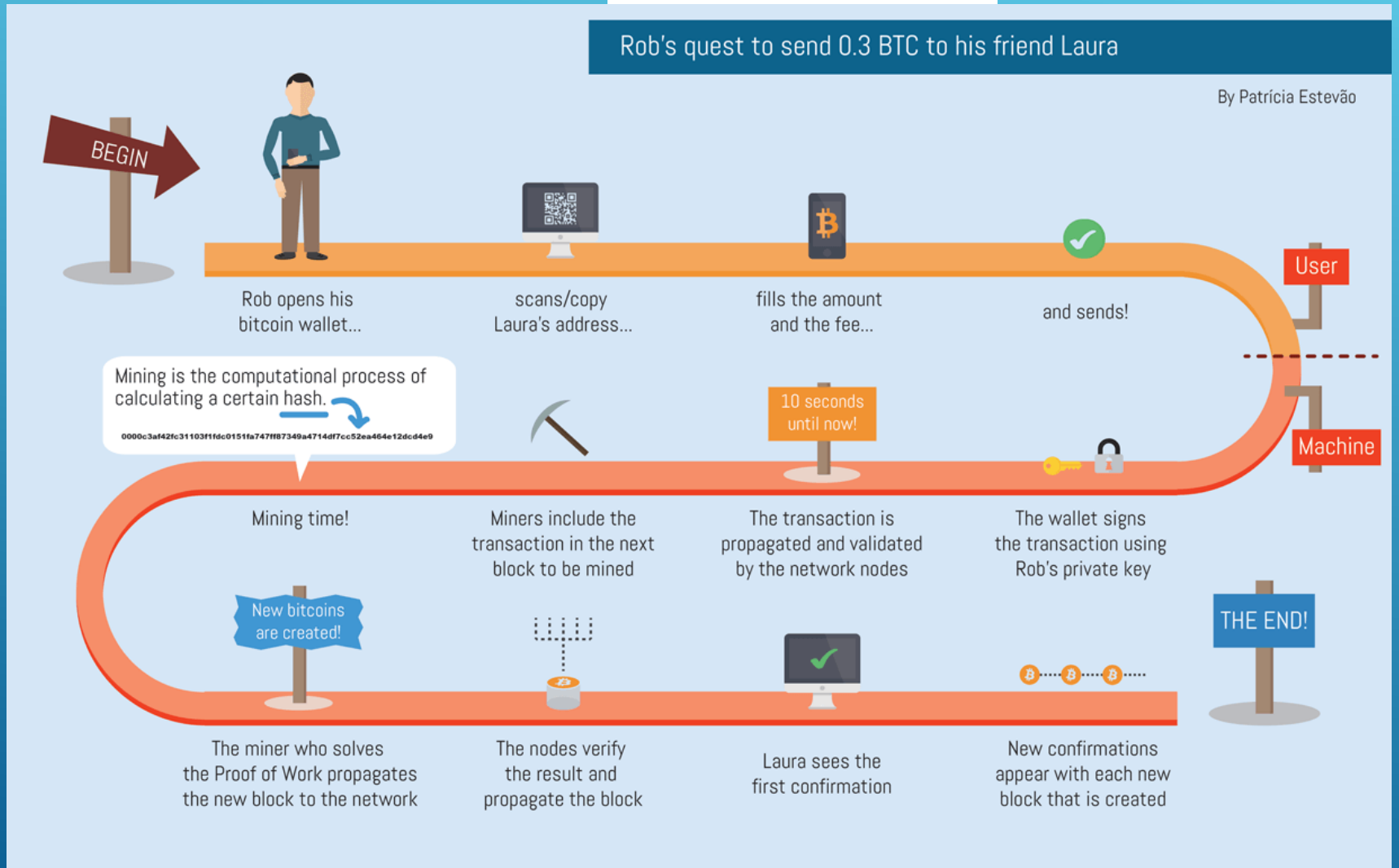


coinbase	86c3532df82e5746611cb640fd2482b8c0794fe3c0c1ea5bb4a2bea2317db293		
Newly generated coins		3NA8hsjfdgVkmmVS9moHmkZsVCoLxUkvvv	12.91239309
		NONSTANDARD	0
		Fee:	0.00000000
		Transaction sum:	**12.91239309**
34ae7288e0d245f0c1642c726c71aa72156923dbf16a1fa6f7aba6493f7290d1			
1Ku2paKQx4Syy2dx6x7wkUSxRpgr1U1oyq	-3.4871	1NYHREgzVYoA38Zv6tdpcHSkn9bpVRreWy	1.1
		1JE5db6FabSg8cpw1VKvi9hsXU4vgiQhJW	2.3862
		Fee:	0.00090000
		Transaction sum:	**3.48710000**
b2b8f254c9af388cea47cd63ad7856b70ce976c6ce5e89516c4fcb8315fc0e8c			
1JE5db6FabSg8cpw1VKvi9hsXU4vgiQhJW	-2.3862	1ANyp8aNehCJ29fDevmEPwEFFmXZ2eRoym	1.1
		1FmiZLGEP7WvQSvJqZXNNDc8EUdZ9zTqVr	1.2853
		Fee:	0.00090000
		Transaction sum:	**2.38620000**

Image source: www.blockchain.com

Blockchain terminologies

- **Bitcoin**
  - How the money transfer works

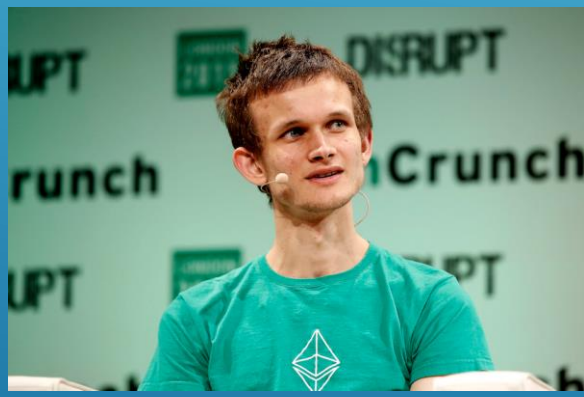


Blockchain terminologies

- **Ethereum**
  - Proposed in late 2013 by Vitalik Buterin (cryptocurrency researcher and programmer)
  - Online crowdsale during summer 2014
  - Bitcoin on steroids!

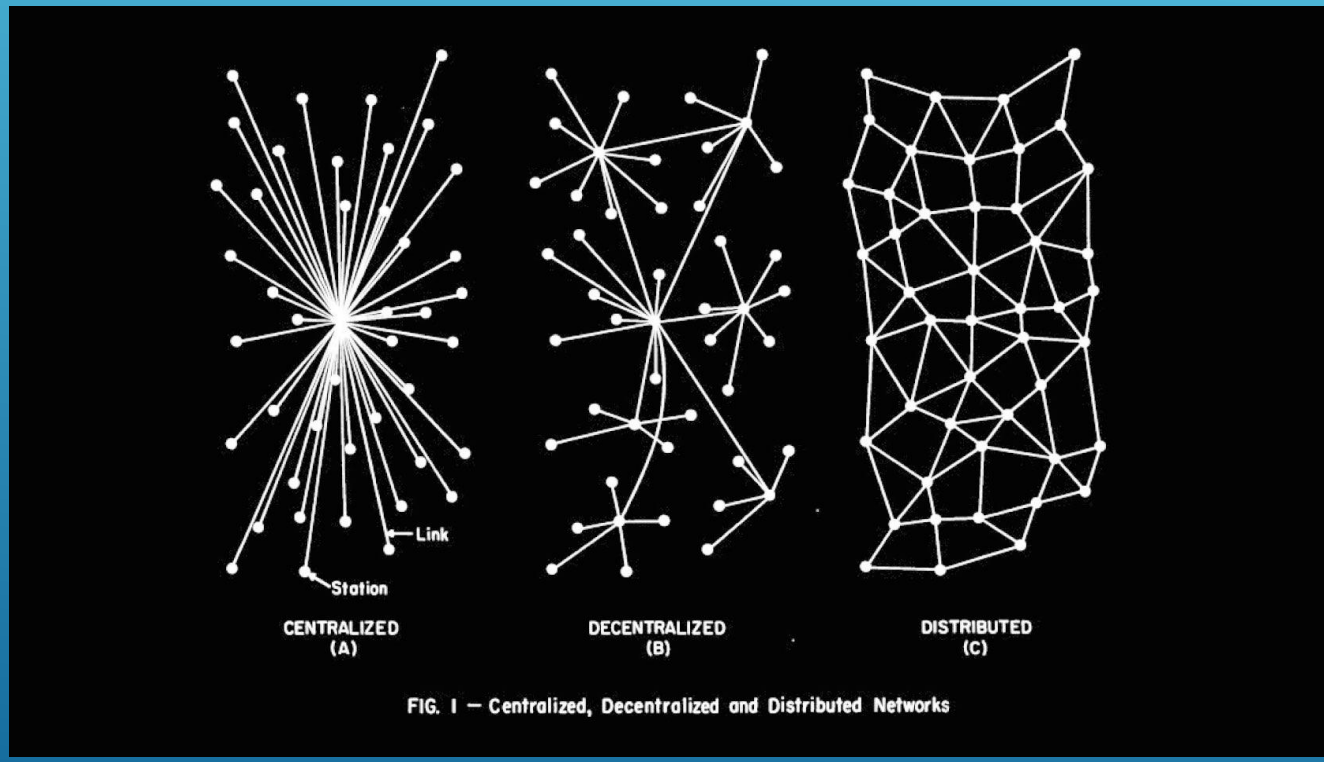
"A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies."

VitalVitalik Buterin



Blockchain terminologies

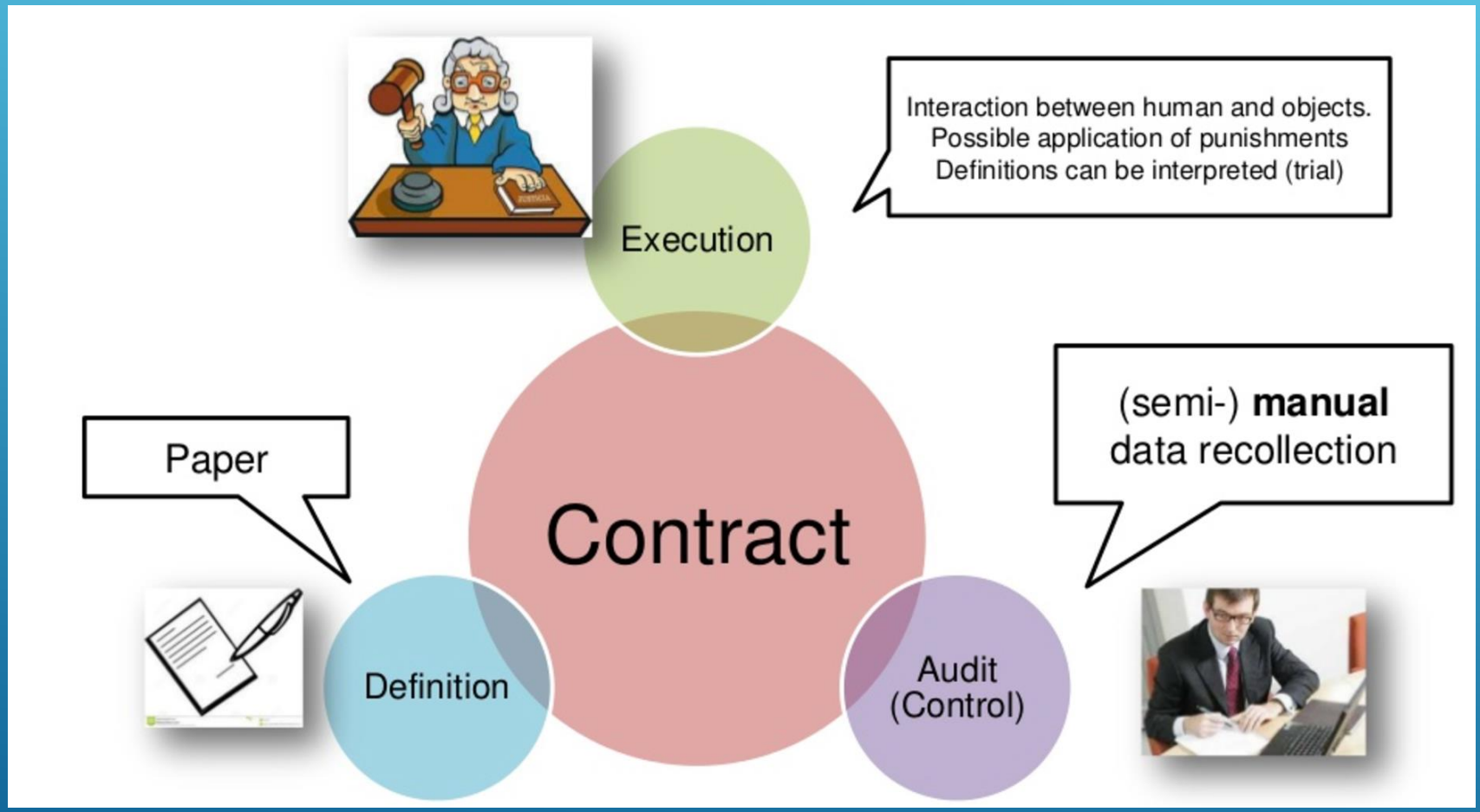
- **Ethereum**
  - Decentralised app platform (dapps)
  - Transaction & smart-contracts ledger
  - Based on the Ethereum Virtual Machine (EVM)
  - Cryptocurrency called ether (ETH)



Blockchain terminologies

- **Ethereum**
  - *Smart Contract*

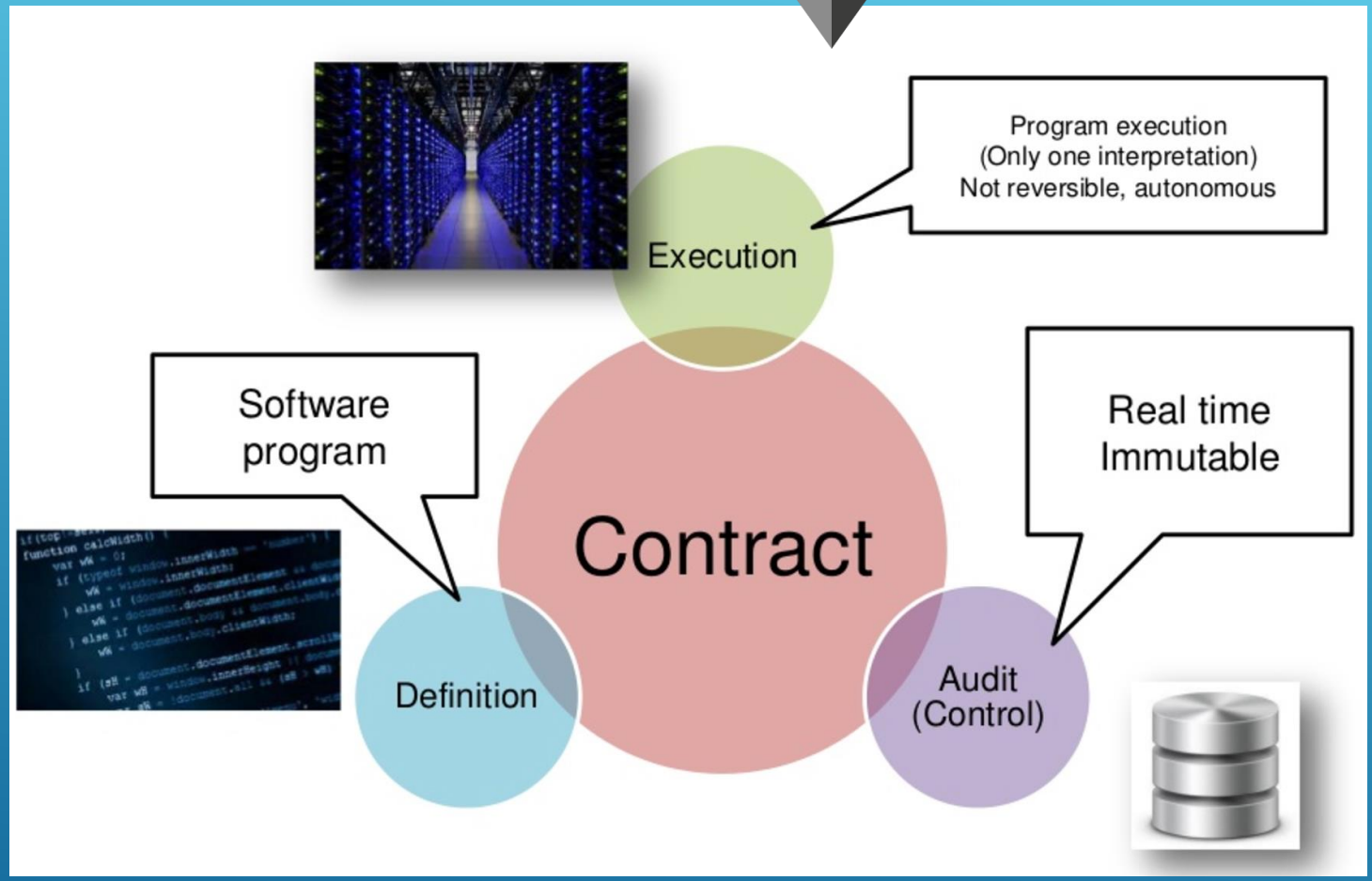
How a “Traditional” contract works:



Blockchain terminologies

- **Ethereum**
  - *Smart Contract*

How a "*Smart Contract*" contract works:



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