# Blockchain and Cryptocurrency

## Engineering Guild

Jakub Horcicka

02. 12. 2020

# Agenda

## Blockchain and cryptocurrency

- Blockchain.
- Bitcoin.
- Ethereum.

## History

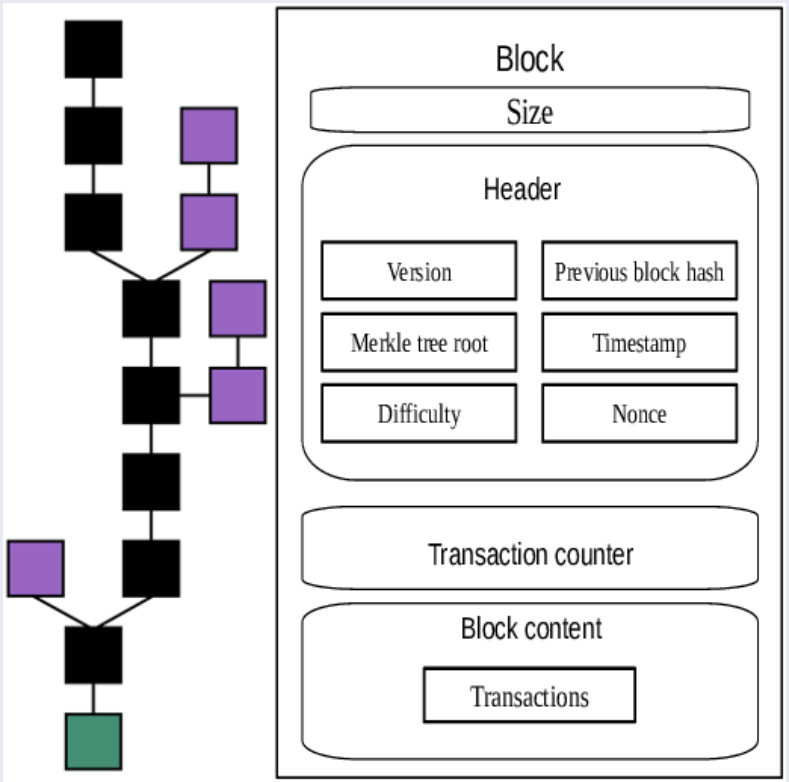
- 1991: Stuart Haber and W. Scott Stornetta, documents with timestamps.
- 1992: Bayer, Haber and Stornetta, performance optimization.
- 2008: Satoshi Nakamoto, no signing by a trusted party.
- 2009: Bitcoin.
- 2014: 20GB Bitcoin blockchain.
- 2017: 100GB Bitcoin blockchain.

# Blockchain

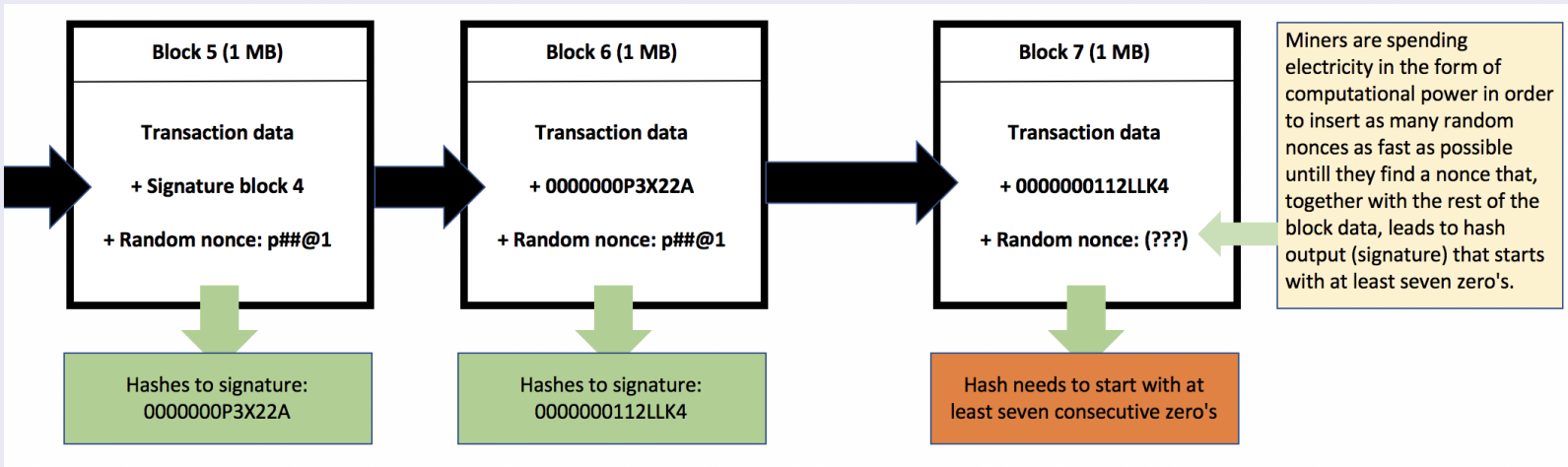
## Characteristics

- Database, system of records (ledger for cryptocurrency).
- Distributed.
- Decentralized.
- Append-only.
- Peer-to-peer network.
- Chain of blocks of transactions.
- Private key cryptography.
- Public (Bitcoin, Ethereum).
- Private, access is restricted.

## Chain structure



## Chain

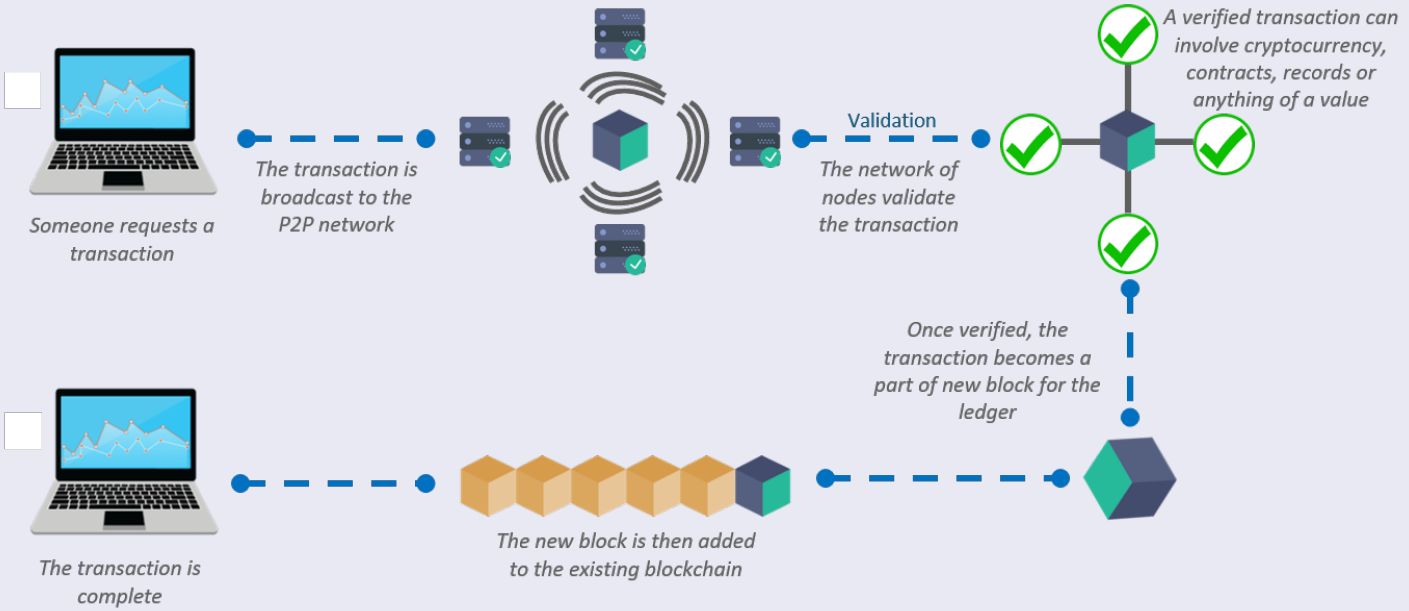

Block 5 (1 MB)
Transaction data
+ Signature block 4
+ Random nonce: p##@1
Hashes to signature:
0000000P3X22A
Block 6 (1 MB)
Transaction data
+ 0000000P3X22A
+ Random nonce: p##@1
Hashes to signature:
0000000112LLK4
Block 7 (1 MB)
Transaction data
+ 0000000112LLK4
+ Random nonce: (???)
Hash needs to start with at least seven consecutive zero's
Miners are spending electricity in the form of computational power in order to insert as many random nonces as fast as possible untill they find a nonce that, together with the rest of the block data, leads to hash output (signature) that starts with at least seven zero's.

# Blockchain

## Principle

- Transactions (data made by users).
- Blocks (confirming records made by miners).
- Valid transactions are added to the blockchain.
- Validity (user's electronic signature, existing user's wallet with enough money, ...).
- Block time (average time between 2 confirmed blocks).
- Shorter block time allows trustworthy transactions (Bitcoin 10m, Ethereum 20s).

## Transaction



# Blockchain

## Advantages

- Each node has the same power.
- Too hard for attackers to edit transactions.
- Automated conflict solving (invalid transactions will not become part of a blockchain).
- Trusted third party is not needed.

## Disdvantages

- Mining power requirements.
- Lacks application development support.
- People do not understand it.
- It can potentially, in theory, replace banks.

## Examples

- Cryptocurrency.
- Personal documents sharing:ID, visa.
- Money transactions among countries.
- Medical history/record.
- Shipping.
- Supply chain monitoring.
- Elections / online voting.

# Blockchain

## Decentralization

- Each node in the network has complete or partial copy.
- Each node can check validity of all transactions.
- Each node can decide if a transaction is part of a blockchain.

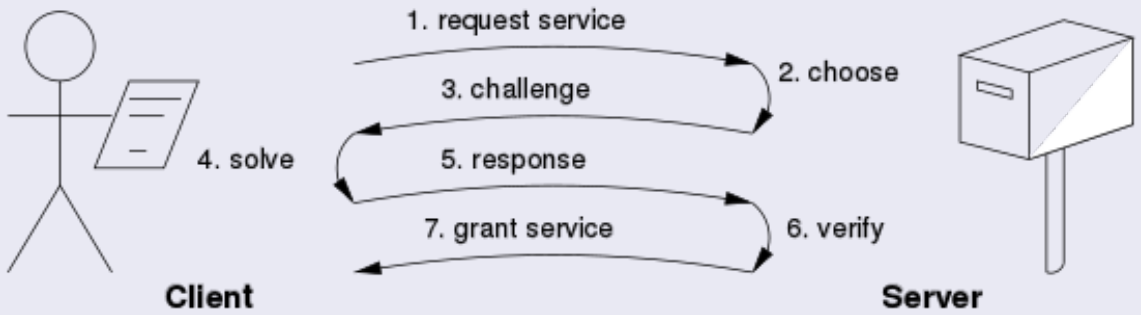
## Double spending problem

- In centralized databases this problem is prevented by operation atomicity.
- 2+ nodes create transactions spending (in sum) more than is available.
- Solution is based on timestamps and voting for order of transactions (Proof of Work, Proof of Stake).

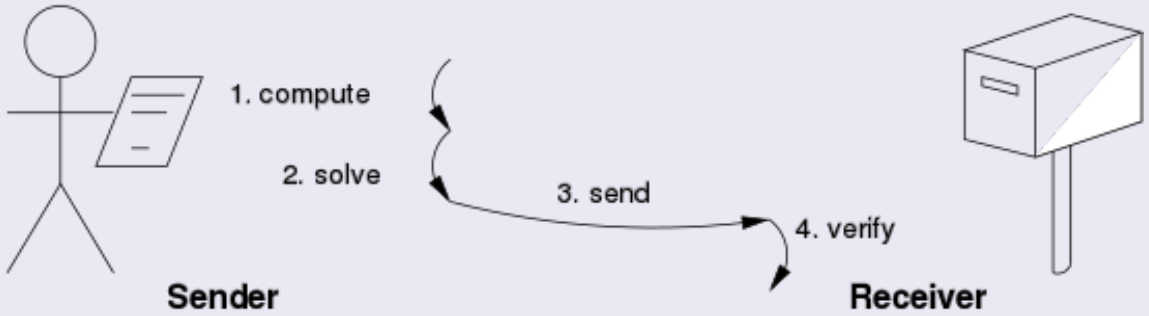
## Consensus – Proof of Work

- Agreement.
- Difficult to generate (mining, energy requirements), easy to validate.
- When a node finds a Proof of Work, it completes a block and broatcasts it.
- Longest chain wins.
- Blocks contain hashes of their parent blocks.
- Alternatives: Proof of Stake, Byzantine fault tolerance.
- Protocols: challenge-response, solution-verification.

## Proof of Work – Challenge-response



## Proof of Work – Solution-verification



# Bitcoin

## Overview

- Decentralized digital currency.
- 2008, Satoshi Nakamoto.
- Peer-to-peer (no bank, central authority).
- New block every 10 minutes.
- Wallet (digital credentials).
- Key pair, public and private key.
- Amount of coins is fixed, from the beginning.
- 2010: first real life payment – pizza order, 10 000 bitcoins, worth $30.

# Bitcoin

## Value


## Value

## Mining 1/2

- Running a PoW to accept a new block.
- Distributed timestamp.
- Identify a block that, when hashed twice with SHA-256, yields a number smaller than difficulty level.
- Verification is possible using one SHA-256 run.
- Increment a nonce until a value is found that gives the block's hash the required number of leading zeros.
- *https* : *//emn*178*.github.io/online* − *tools/sha*256*.html*

## Mining 2/2


Data
Previous Hash: 00000000000000000475e147f5ec98857ffd21fa2af3f49be2f24f56b3726066
Nonce: 349195901
Hash of New Tx's: cd8b654de2467d5afc28c3fa96b5f7b2343d578aecd3d345e5a14cf10b7011bc

# Ethereum

## Overview

- 2013 Vitalik Buterin.
- Distributed open source blockchain based platform.
- Smart Contracts.

## Ether

- Cryptocurrency.
- Block time is 10-15s.
- Mining generates new coins.
- Different PoW (reduces benefits of specialized HW).

## Smart contracts

- Scripting functionality of Ethereum platform.
- Application development.
- Language: combination of C, JavaScript, Python and Go.

# Sources


- *https://en.wikipedia.org/wiki/Blockchain*
- *https://en.wikipedia.org/wiki/Hashcash*
- *https://en.wikipedia.org/wiki/Bitcoin*
- *https://en.wikipedia.org/wiki/Ethereum*
- *https://en.wikipedia.org/wiki/Bitcoin_network#Mining*
- *https://www.coindesk.com*
- *https://mastanbtc.github.io/blockchainnotes/consensustypes/*
- *https://www.youtube.com/watch?v = TD09UhjleK8*

# That's all, folks!

Thank you for your attention.

# Blockchain applications @ HI

## Ideas?

- 1?
- 2?
- 3?