

# An Introduction to Blockchains

Can Umut ILERI

[c.u.ileri@tudelft.nl](mailto:c.u.ileri@tudelft.nl)

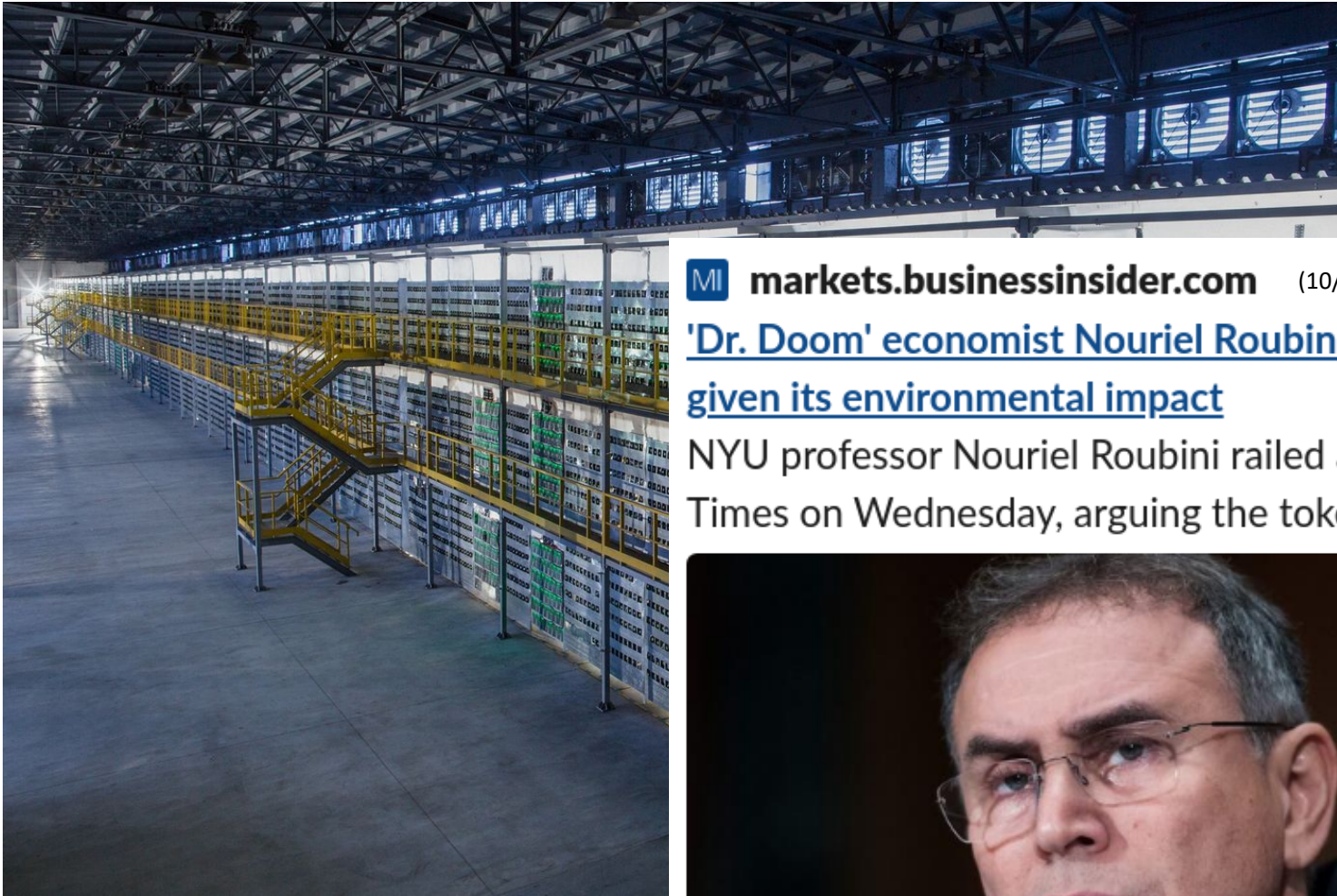
TU Delft

# Bitcoin Sets New All-Time High of \$49.7K, Putting \$50K Within Striking Distance

The record comes as traders analysts have described institutional investors' interest in bitcoin as growing "at a staggering pace."



<https://www.coindesk.com/bitcoin-sets-new-all-time-high-of-49-7k-putting-50k-within-striking-distance>



**M** [markets.businessinsider.com](https://markets.businessinsider.com) (10/02/2021)

'Dr. Doom' economist Nouriel Roubini says bitcoin's fundamental value is negative given its environmental impact

NYU professor Nouriel Roubini railed against bitcoin in an op-ed for the Financial Times on Wednesday, arguing the token has a negative value. (45 kB) ▾



<https://markets.businessinsider.com/currencies/news/bitcoin-value-negative-environmental-impact-nouriel-roubini-cryptocurrencies-2021-2-1030067687>

# Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** 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. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

## 1. Introduction

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. Completely non-reversible transactions are not really possible, since financial institutions cannot

# Dombrovskis: 'We need a digital euro'

Commission economics chief is confident the ECB will decide to launch the virtual form of its currency.



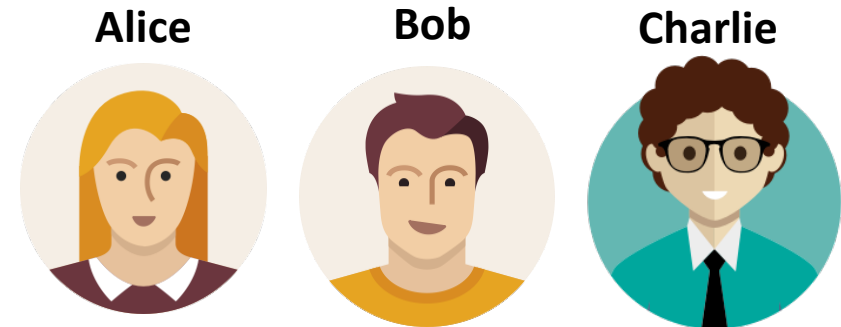
BY BJARKE SMITH-MEYER

January 21, 2021 | 7:15 am

<https://www.politico.eu/article/valdis-dombrovskis-i-want-a-digital-euro-ecb-commission/>

# Outline of this lecture

- Blockchain Background
  - Hashing
  - Asymmetric cryptography
  - Digital Signatures
- Bitcoin
  - Transactions, Blocks
  - Consensus (Proof of Work)
- Smart contracts
- Other Blockchain Solutions
- Trustchain
- Future: DAO



# Bitcoin vs. Blockchain

- Both starts with



## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** 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. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

### 1. Introduction

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. Completely non-reversible transactions are not really possible, since financial institutions cannot

# Motivation

## Concerns on Fiat currency



- Issued by governments
- Delay between transaction and settlement
- Financial institutions serving as trusted third parties
- The cost of mediation increases transaction costs
- We need a mechanism to make payments **over a communications channel without a trusted party**

# Solution (from Nakamoto's paper)



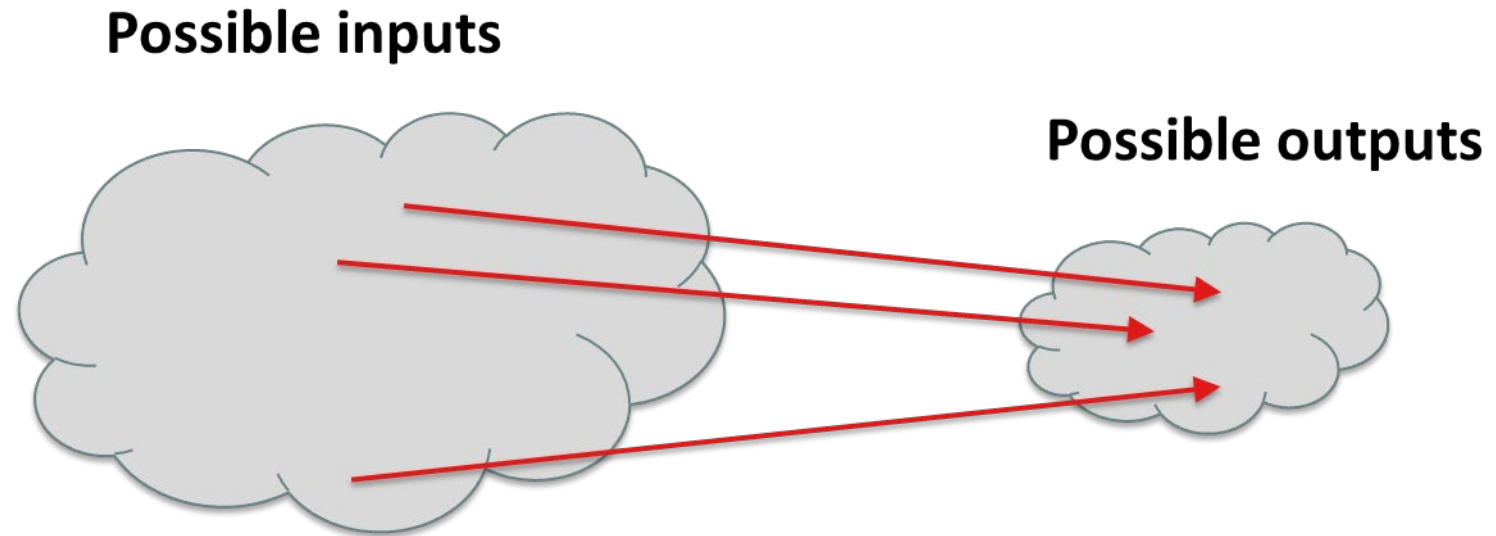
- An electronic payment system based on **cryptographic proof instead of trust**,
- Transactions that are **computationally impractical to reverse** would protect sellers from fraud.
- A solution to the double-spending problem by generating computational proof of the **chronological order of transactions**.



# Preliminaries

- Hash function
- Asymmetric encryption
- Digital signatures

# Hashing



## Collision-free

- Collisions do exist but it is very difficult to find them

## Hiding

- Given an output, it is not feasible to find an input
- Req: No particularly likely input

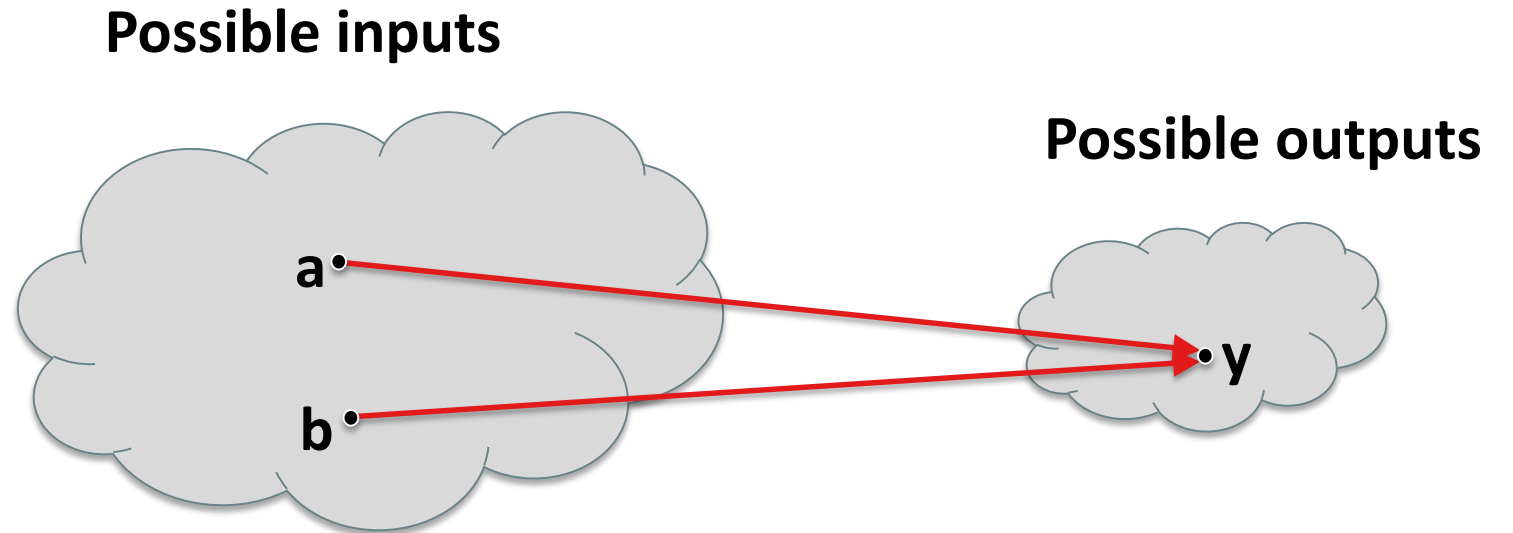
## Puzzle-friendly

- Given an output and only a part of the input, it is not feasible to find remaining part of input

# Hashing

## Collision-free

- Collisions do exist but it is very difficult to find them

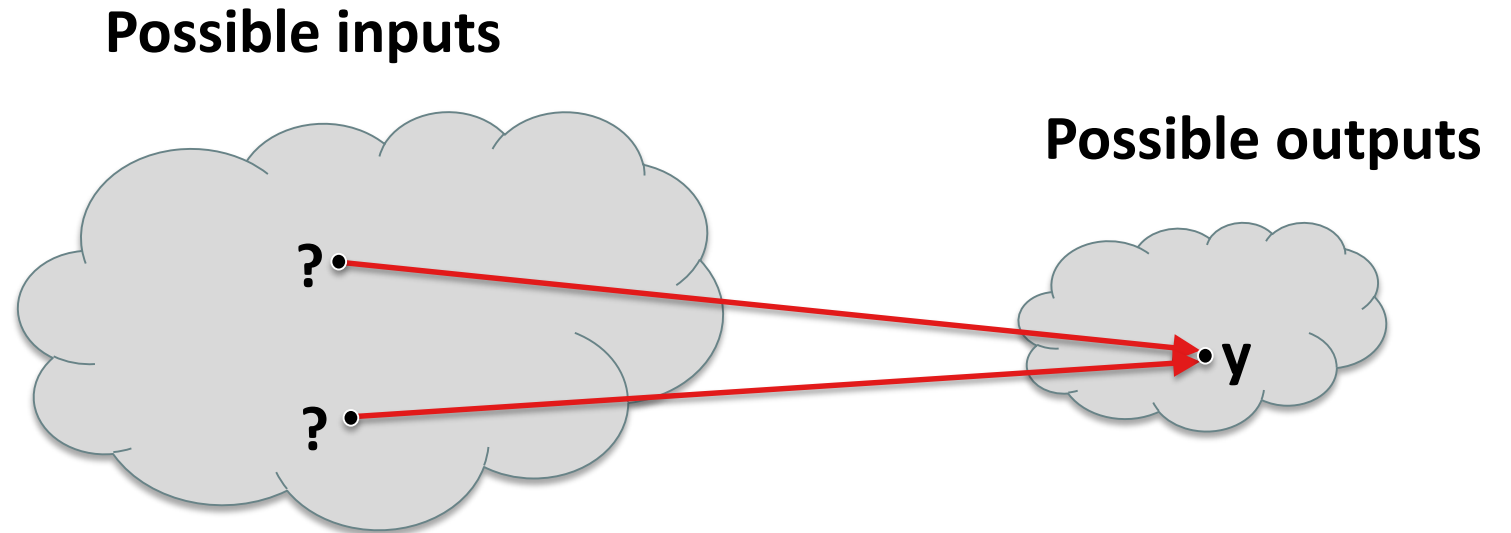


Finding two inputs  $a$  and  $b$  giving the same output  $y$  is infeasible.

# Hashing

## Hiding

- Given an output, it is not feasible to find an input
- Req: No particularly likely input

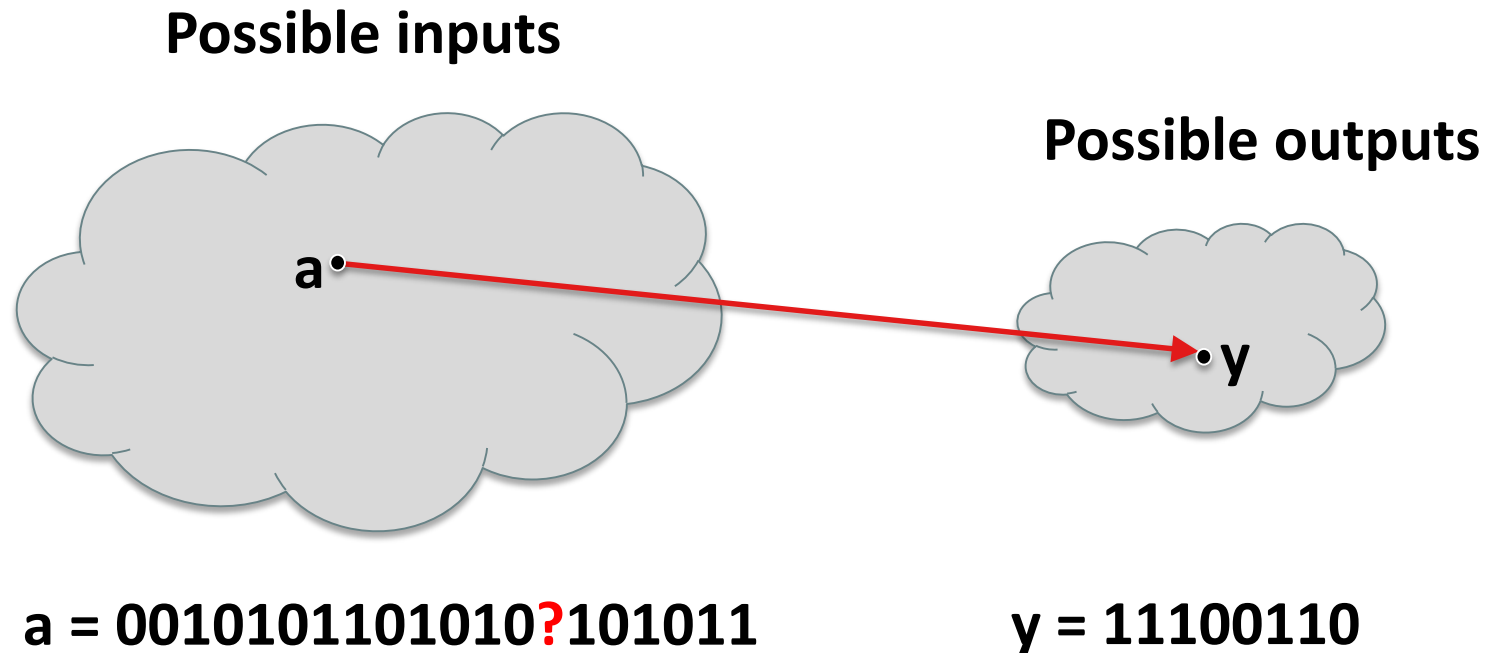


Given  $y$ , it is infeasible to find an input giving  $y$ .

# Hashing

## Puzzle-friendliness

- Given an output and only a part of the input, it is not feasible to find remaining part of input



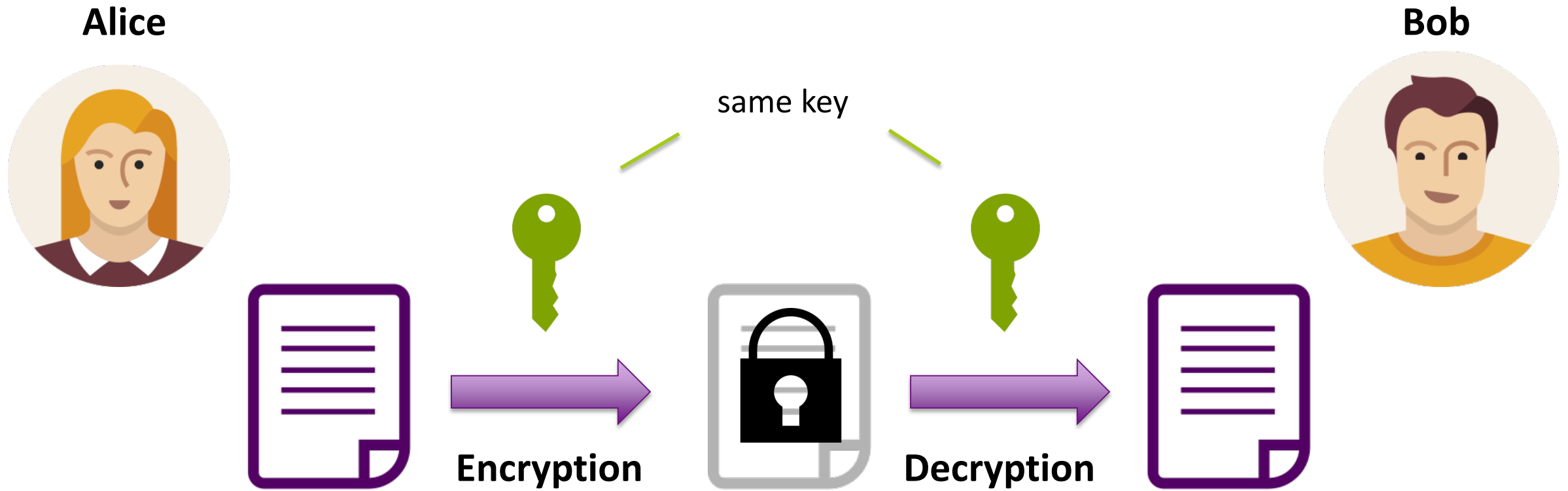
Given  $y$ , and all but 1 bit of its input  $a$ , there is no feasible way to predict the missing bit.

DEMO

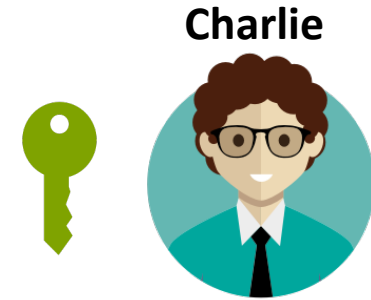
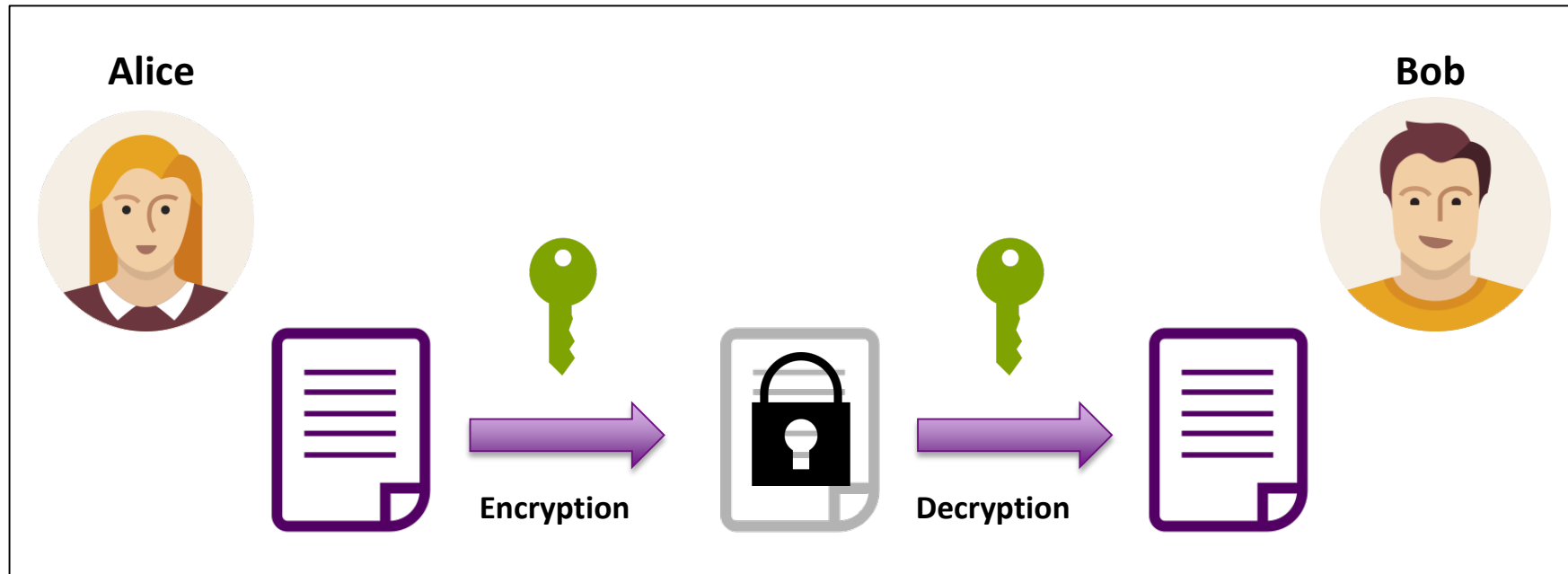
# Secure Hash Algorithm

<https://passwordsgenerator.net/sha256-hash-generator/>

# Symmetric key encryption



# Symmetric key encryption



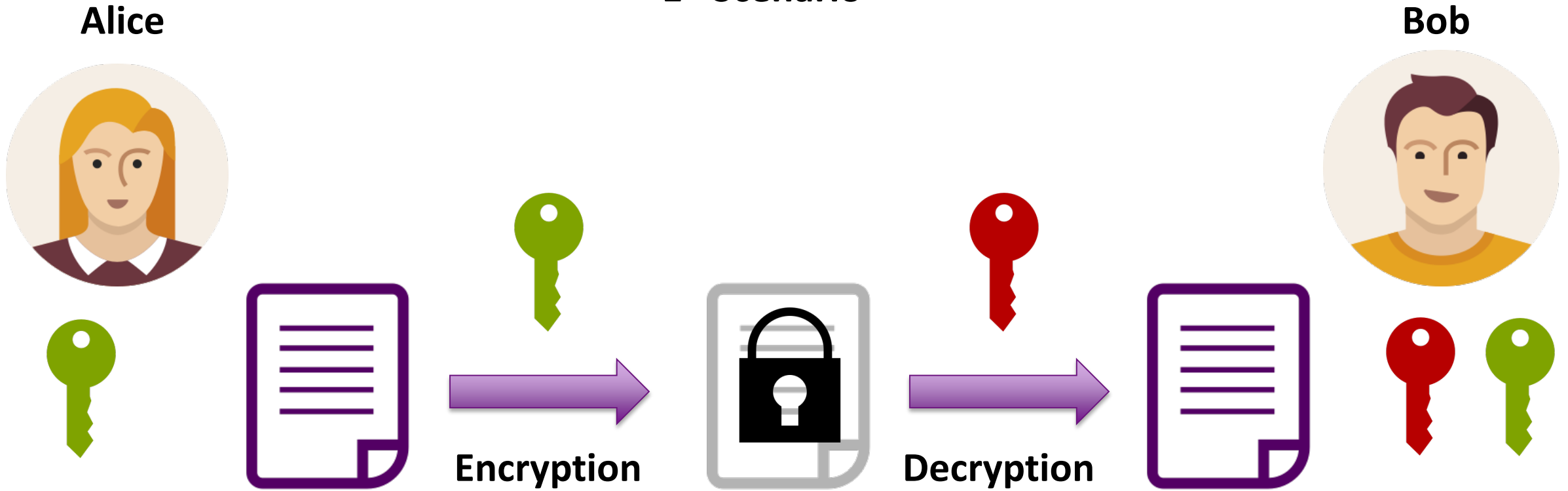
**Charlie can decrypt Alice's message.**

**Charlie can encrypt another message and send it to Bob.**

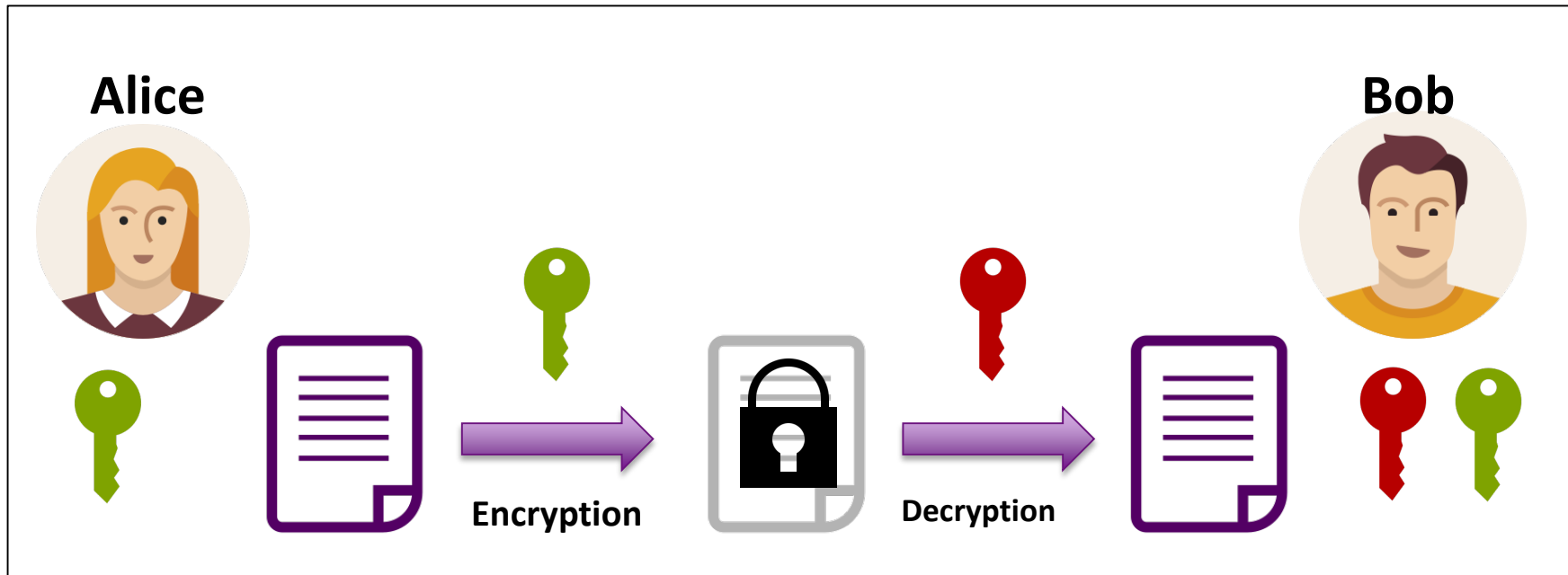


# Asymmetric key encryption (Public key encryption)

## 1<sup>st</sup> Scenario



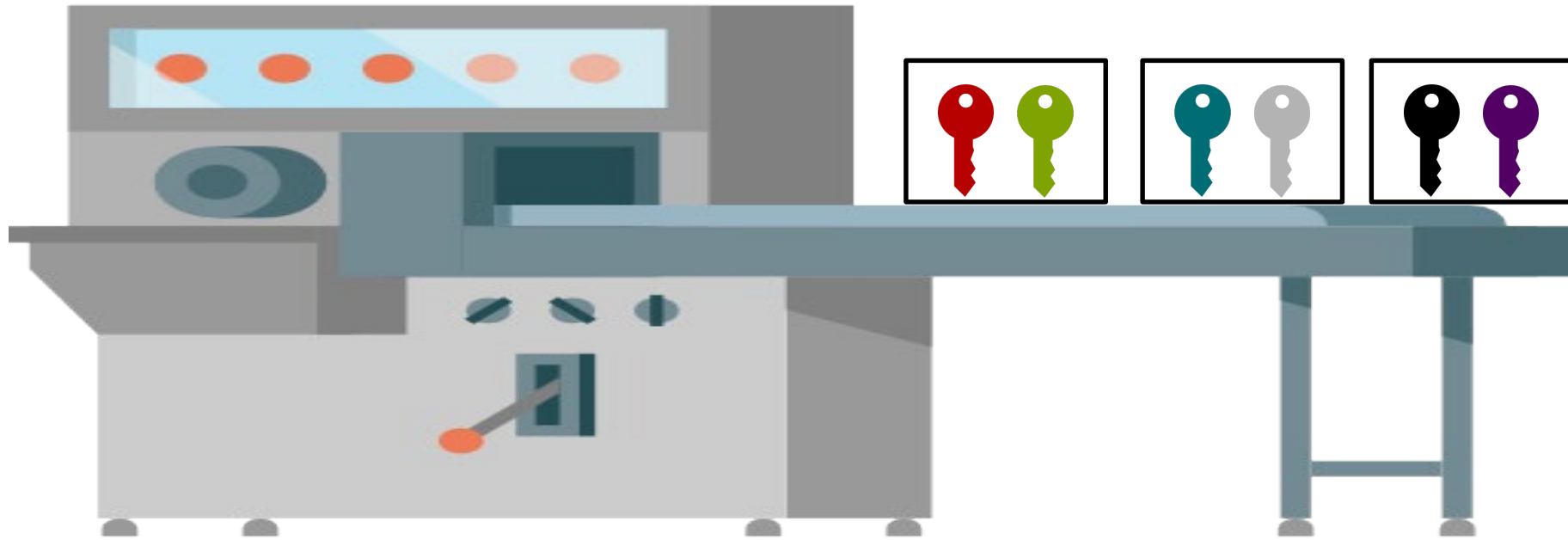
# Asymmetric key encryption



**Charlie cannot decrypt Alice's message.**

**Charlie can still encrypt another message and send it to Bob.**

# Asymmetric key encryption (Public key encryption)

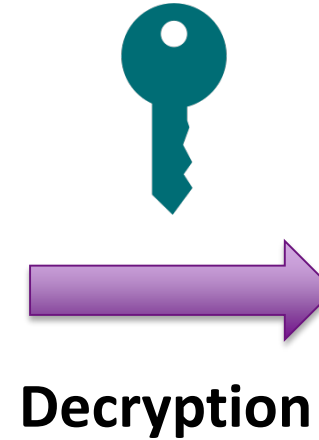
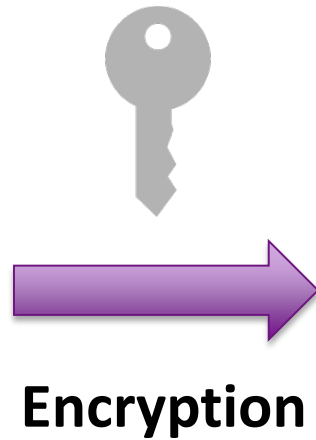


**Key-pair generator**

# Asymmetric key encryption (Public key encryption)

## 2<sup>nd</sup> Scenario

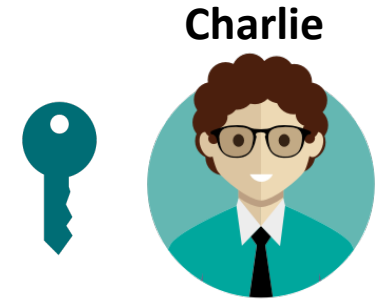
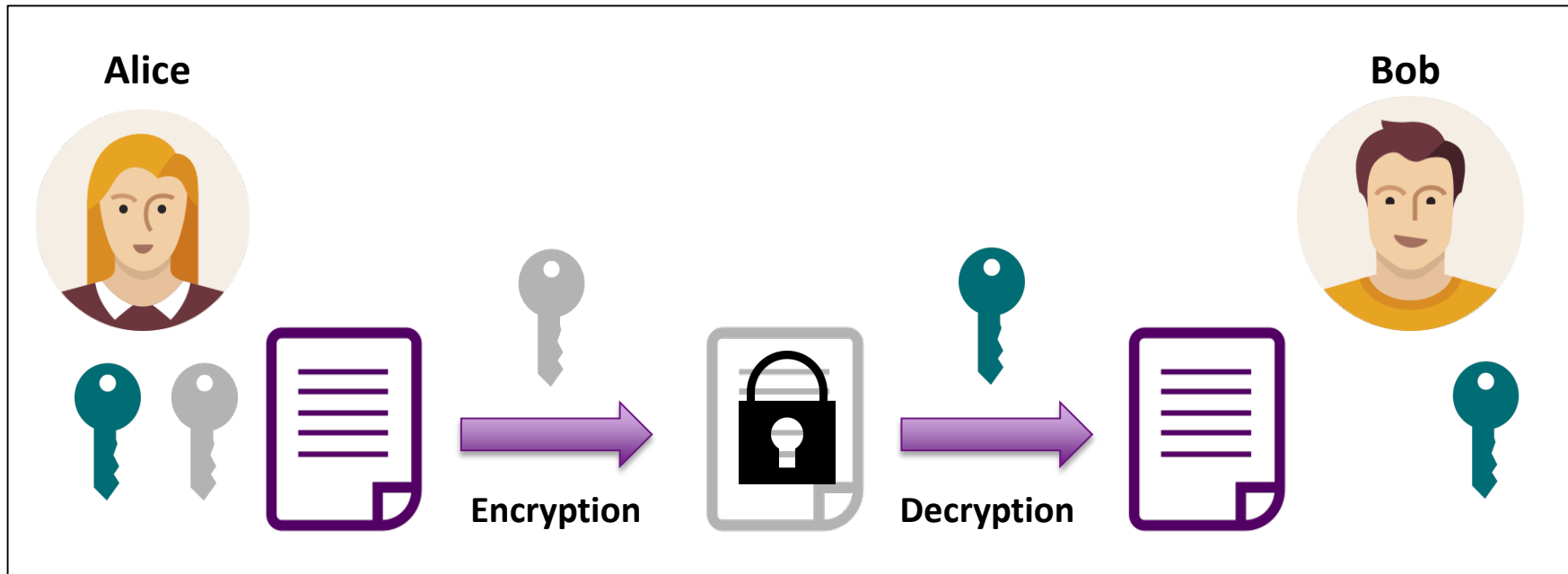
Alice



Bob

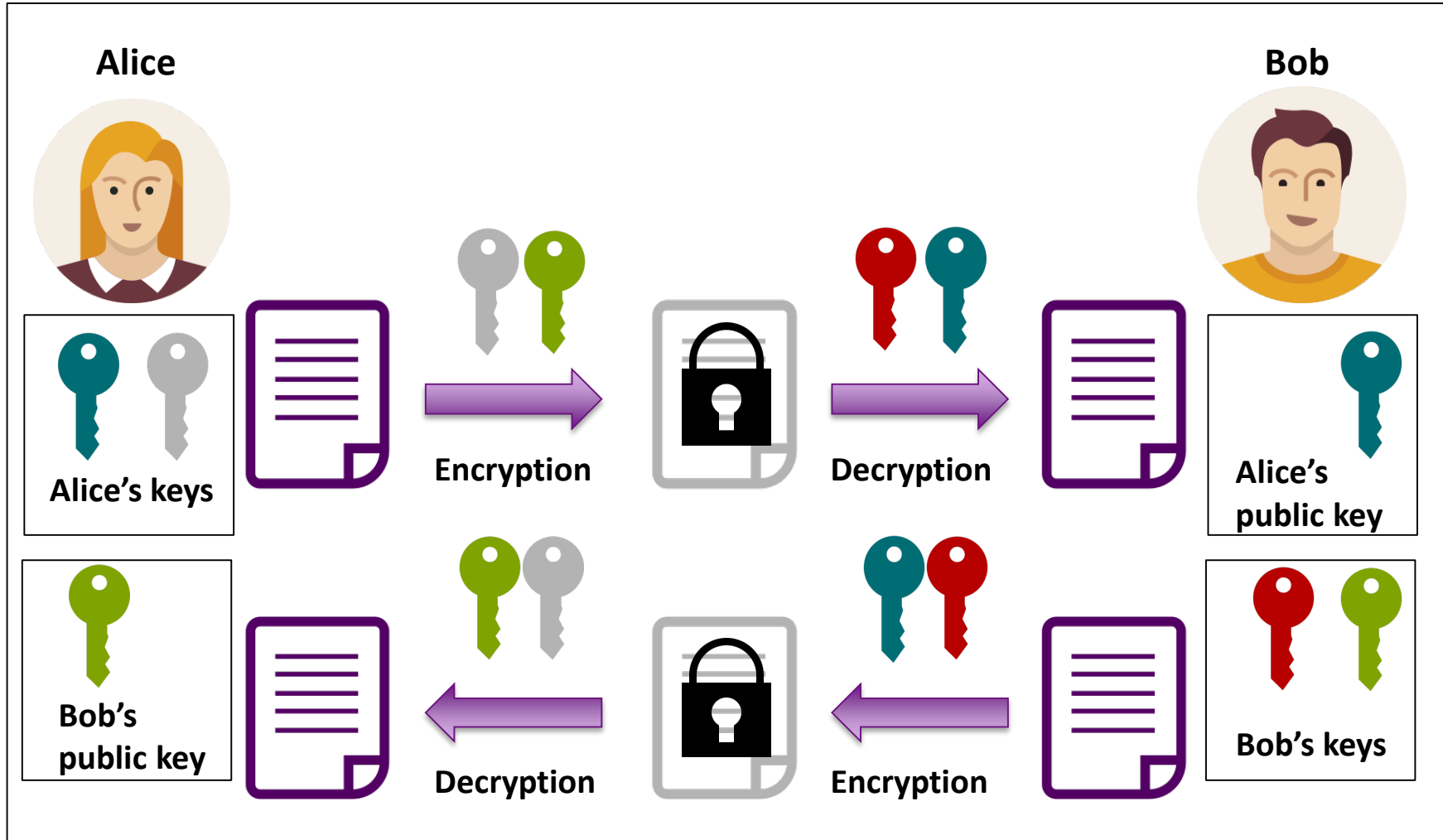


# Asymmetric key encryption



**Charlie can decrypt Alice's message.**

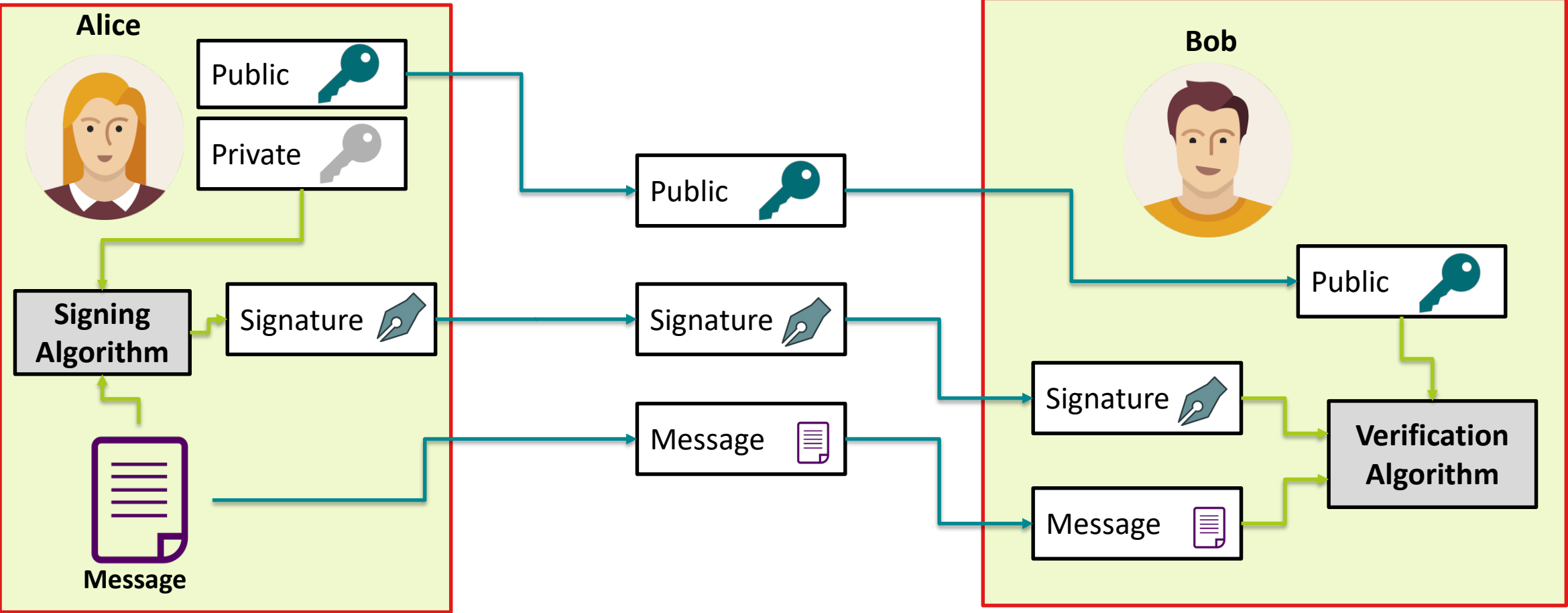
# Asymmetric key encryption



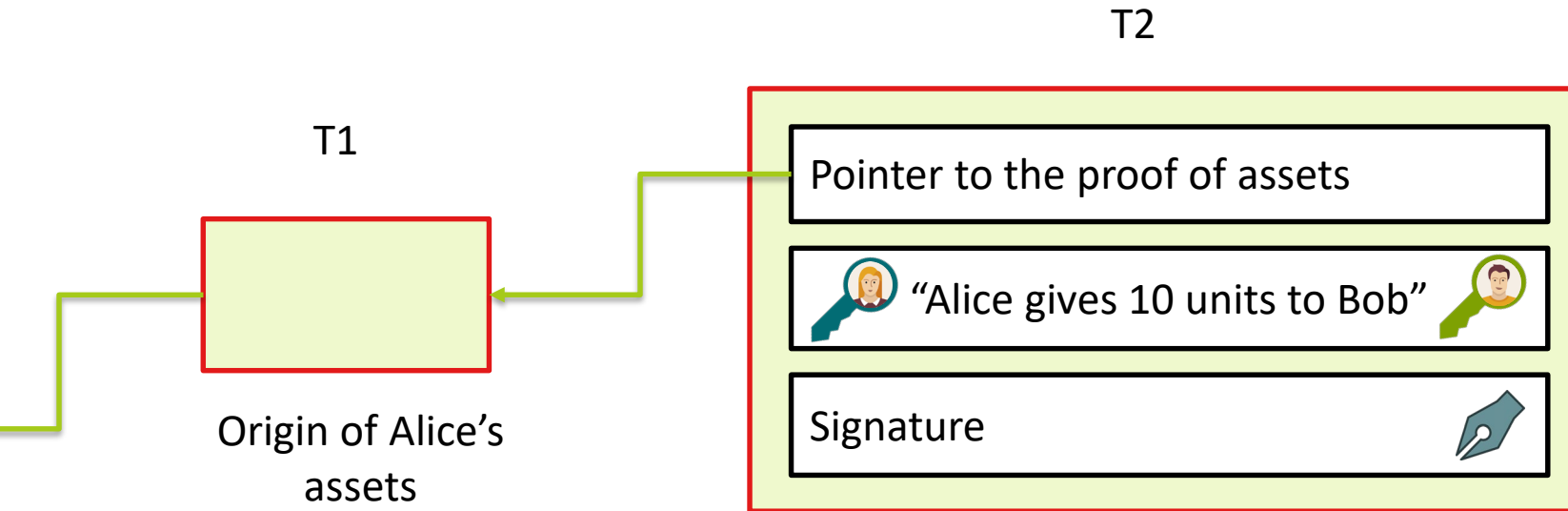
**Charlie cannot decrypt any messages.**

**Charlie cannot send messages in the name of Alice or Bob.**

# Digital signatures



# Transaction



- Anyone can verify that Alice used assets that she had.
- Anyone can verify that Bob now has the assets.
- Only Bob can use the assets since he holds the associated private key.

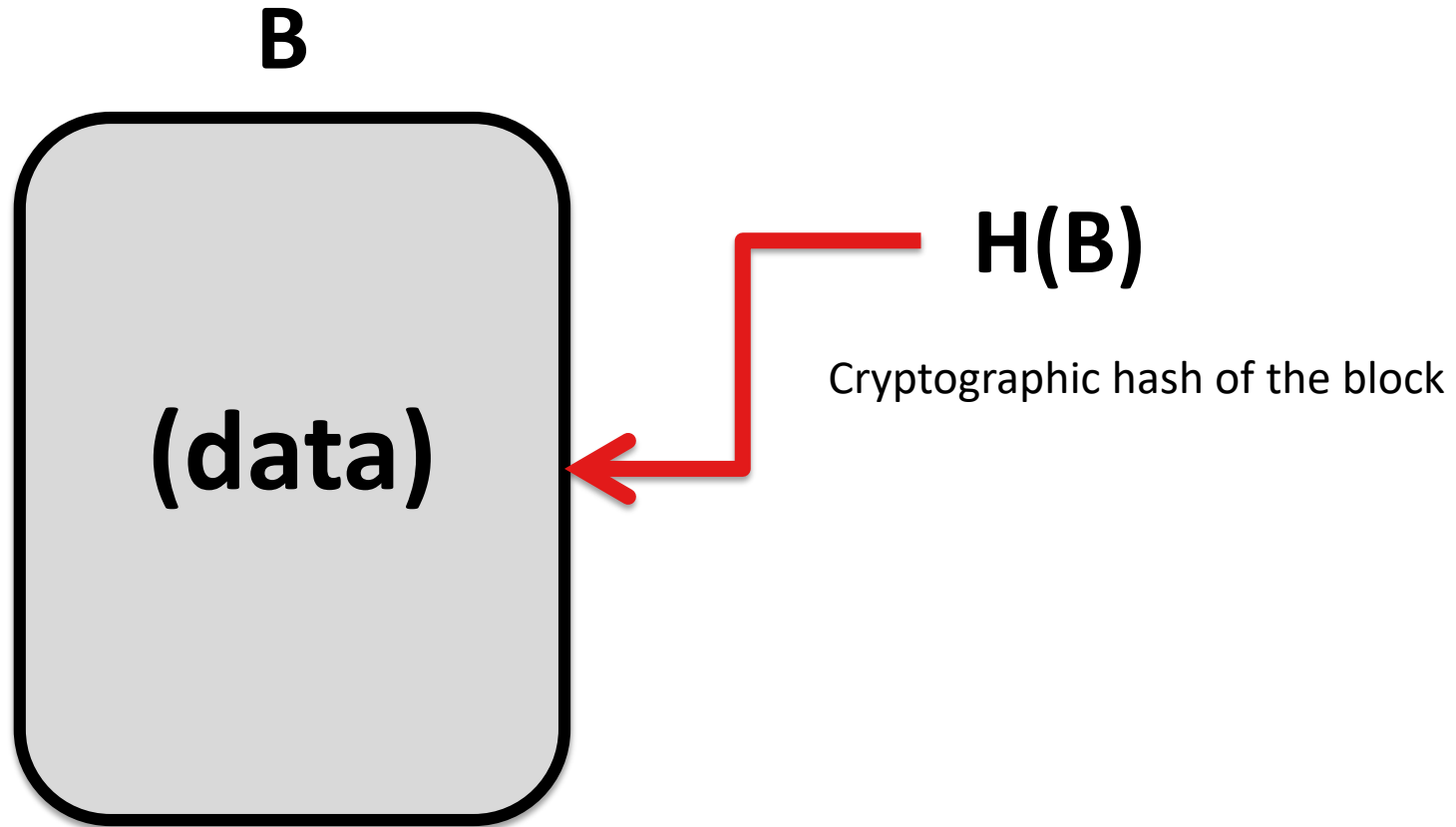


# DEMO: Bitcoin transactions

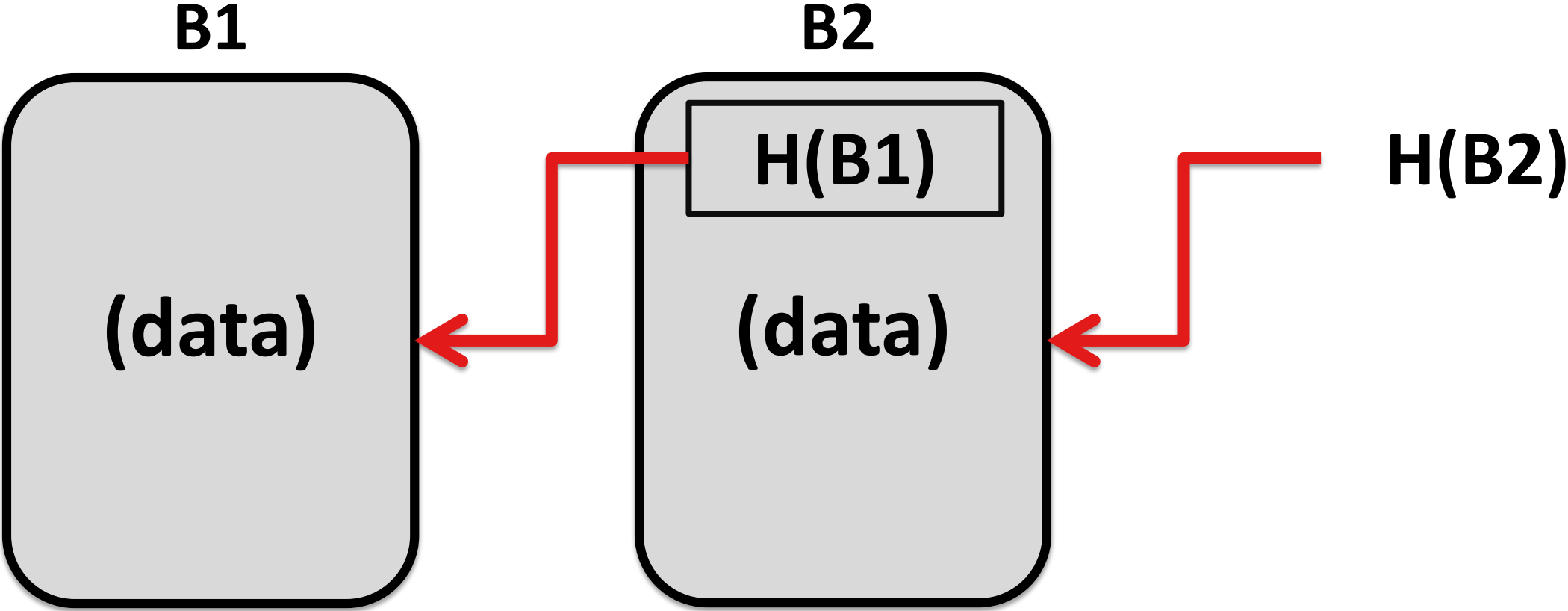


<https://www.blockchain.com/explorer>

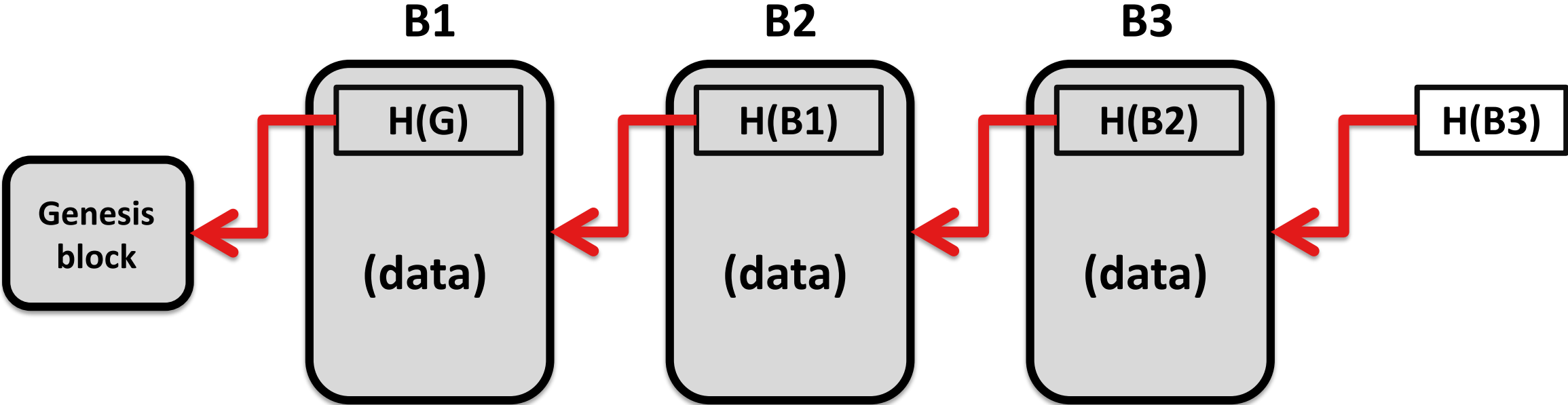
# Hash pointer



# Block of data with a hash pointer



# Blockchain



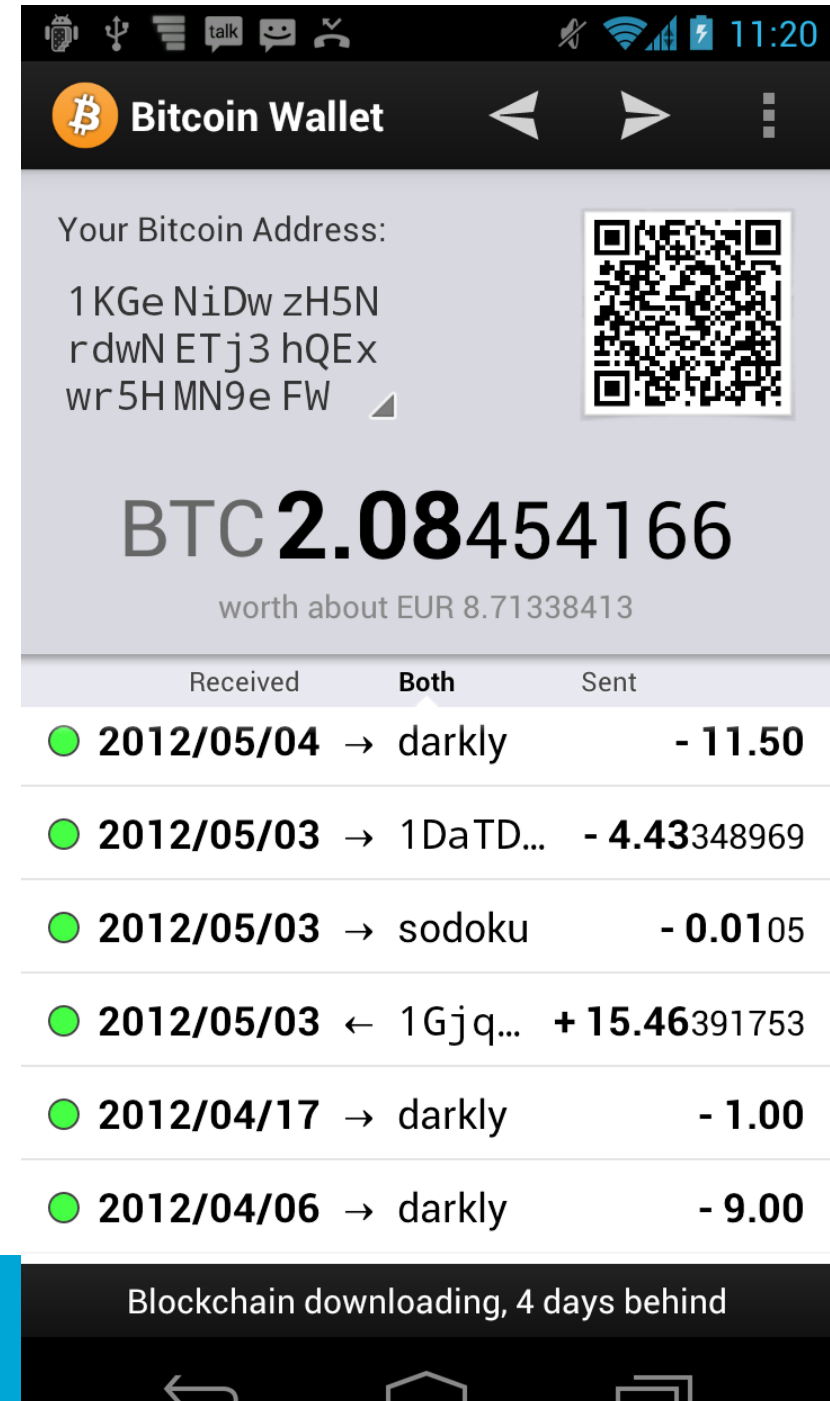
Consecutive blocks form the blockchain

# Blockchain 1.0

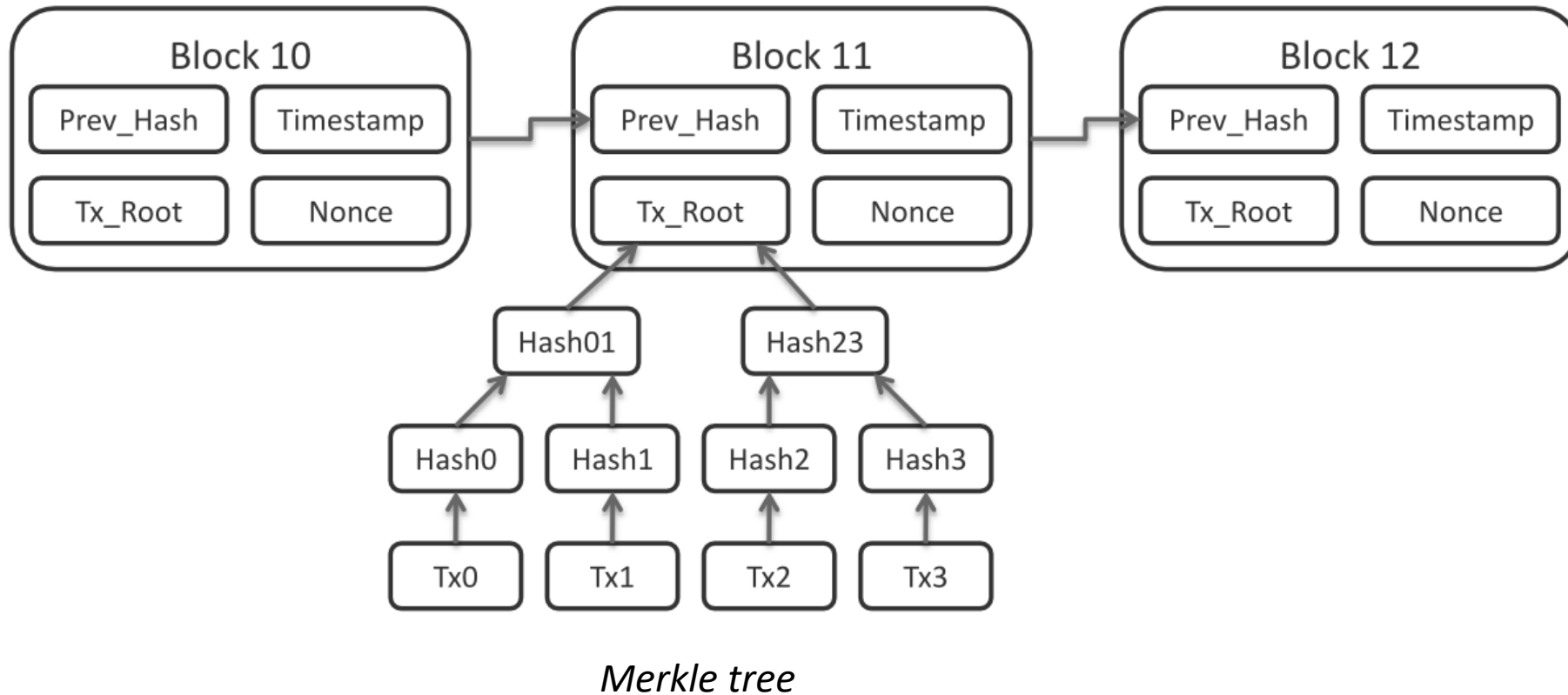


# Bitcoin

- Proposed in 2007 by Satoshi Nakamoto (pseudonym)
- No central authority issuing coins
- Your public key is your wallet address
- With the private key, you can sign transactions

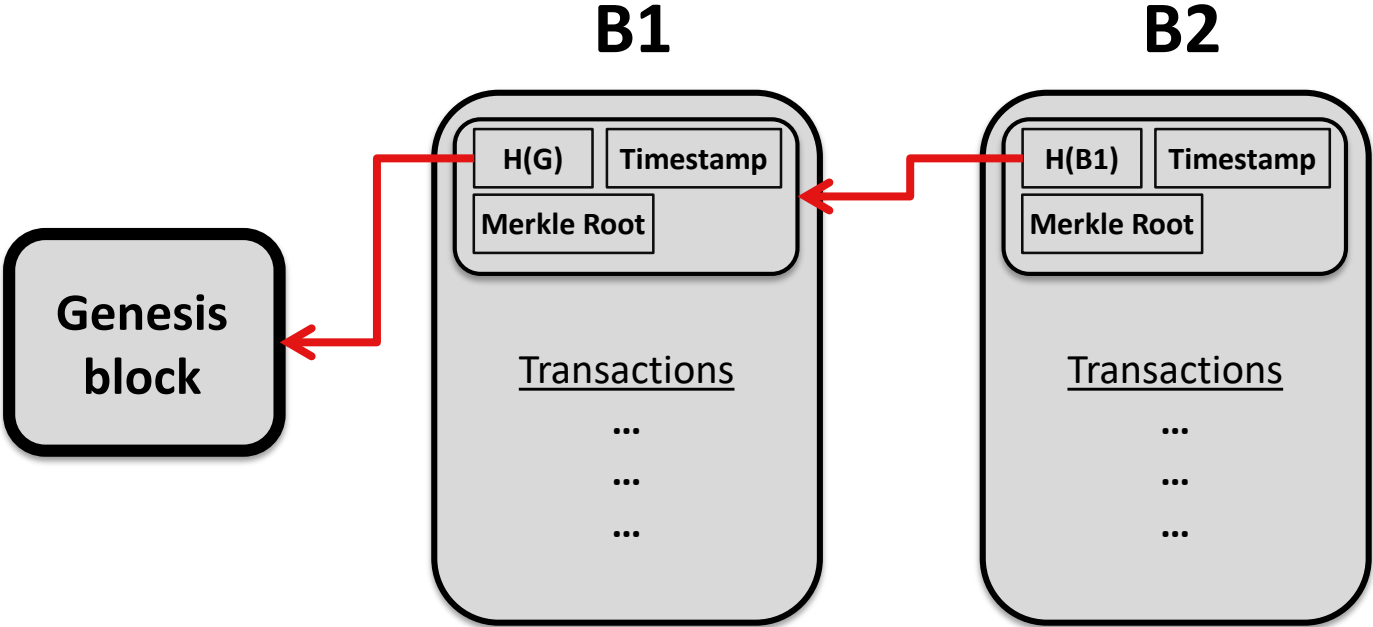


# Transactions are stored in blocks



# Consensus

- Target: Single, shared ledger of transactions



New Transactions

**T1**

**T2**

**T3**

...

...

**T100**

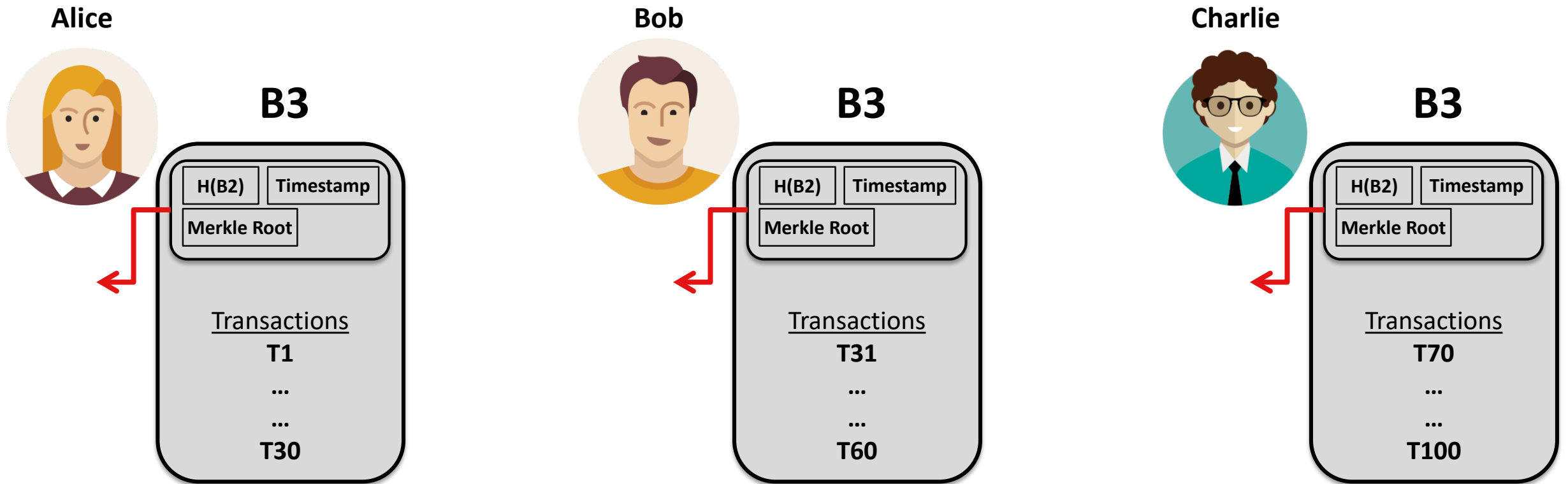
...

Which transactions will the next block (B3) contain?

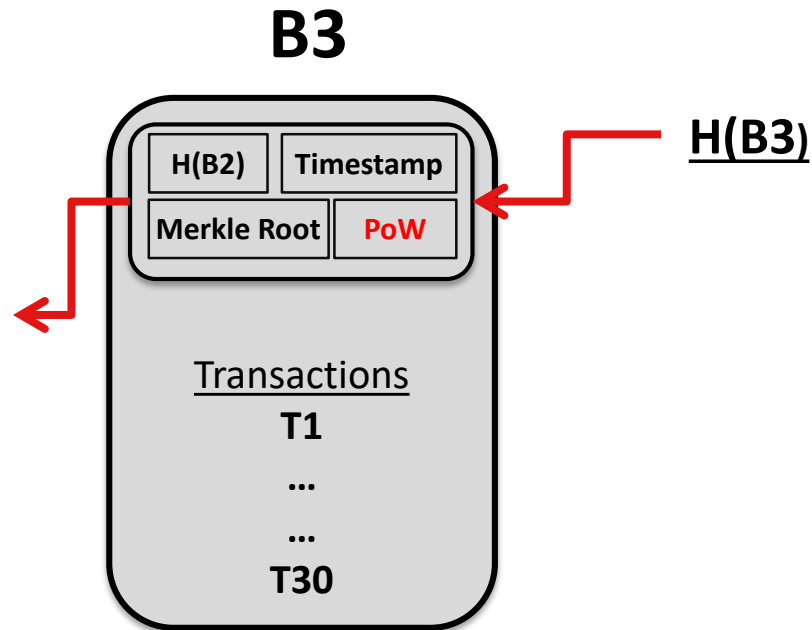


# One single blockchain

- Target: Single, shared ledger of transactions



# Proof of Work: Puzzle-solving



## Puzzle:

- Find a value for PoW such that the first X bits of  $H(B3)$  will be zero.
- Because of the features of the hashing algorithm, there is not an easy way to do this.
- The one who finds the value proves that she put a lot of effort on it.

# Consensus by Proof-of-Work

- **Derive trust through mathematical properties**
- Performed by so-called **miners**
- Solving an arithmetic puzzle
  - Goal: find  $H(x) < d$  where:
    - $H$  is a hash function
    - $x$  is (the description of) a block in the blockchain
    - $d$  is the difficulty parameter

# Bitcoin blocks

- Bitcoin has fixed block sizes of 1MB
- A block is expected to be found in 10 minutes.
  - If not, adjust the difficulty accordingly.
  - The more miners compete, the more difficult the problem is.
- Higher block size -> more transaction throughput
  - But leads to faster growth of blockchain and resource usage

# DEMO: Bitcoin blocks

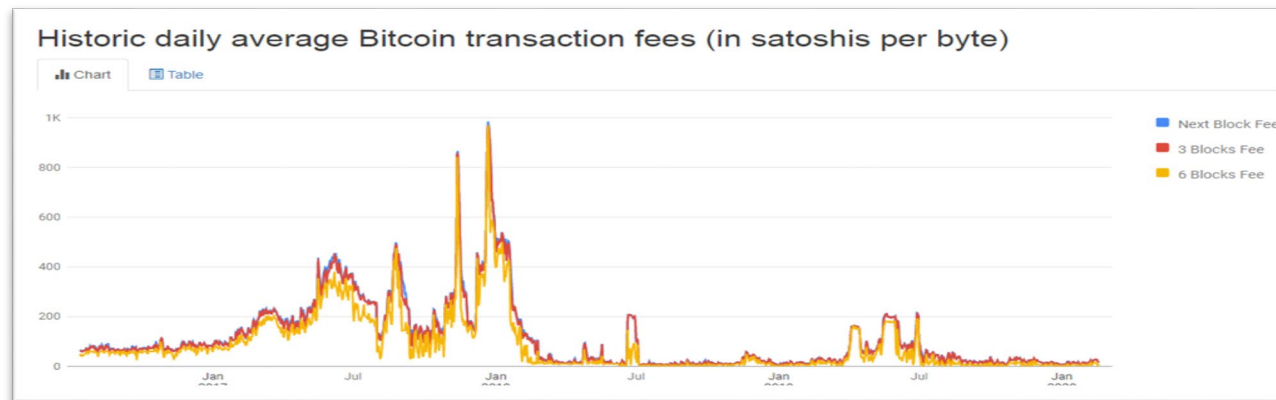


<https://www.blockchain.com/explorer>

# Consensus by Proof-of-Work

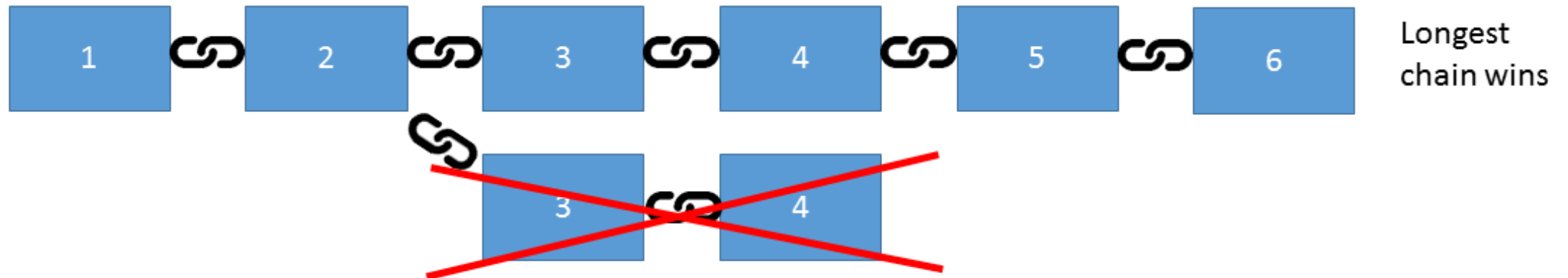
The first miner to find such a “magical” hash is rewarded with:

1. The block reward (halves every 210,000 blocks, the coin reward decreased from 12.5 to 6.25 coins on 12 May 2020. It will decrease from 6.25 to 3.125 coins on 06 May 2024) (<https://www.bitcoinblockhalf.com>)
2. Sum of transaction fees in the block (<https://billfodl.com/pages/bitcoinfees>)
  - To get your transaction processed quickly you have to outbid other users

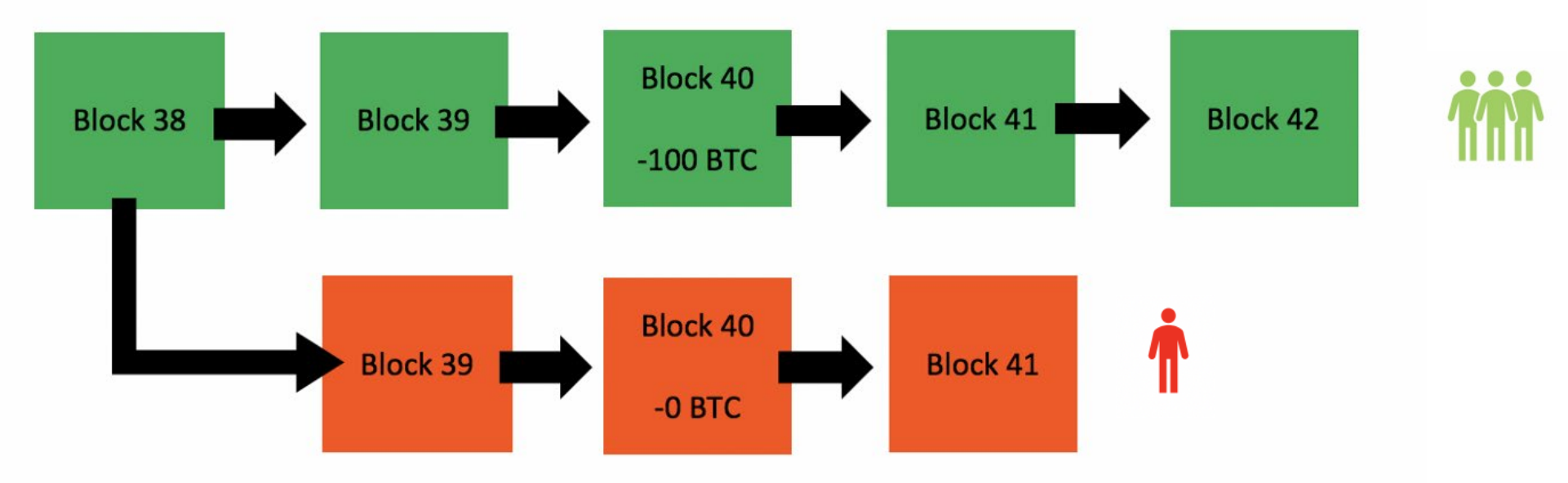


# Simultaneous mining

- What if two miners find the same block at (roughly) the same time?
- Now, different miners will build upon different blocks
- Selection rule by miners: **longest chains wins**

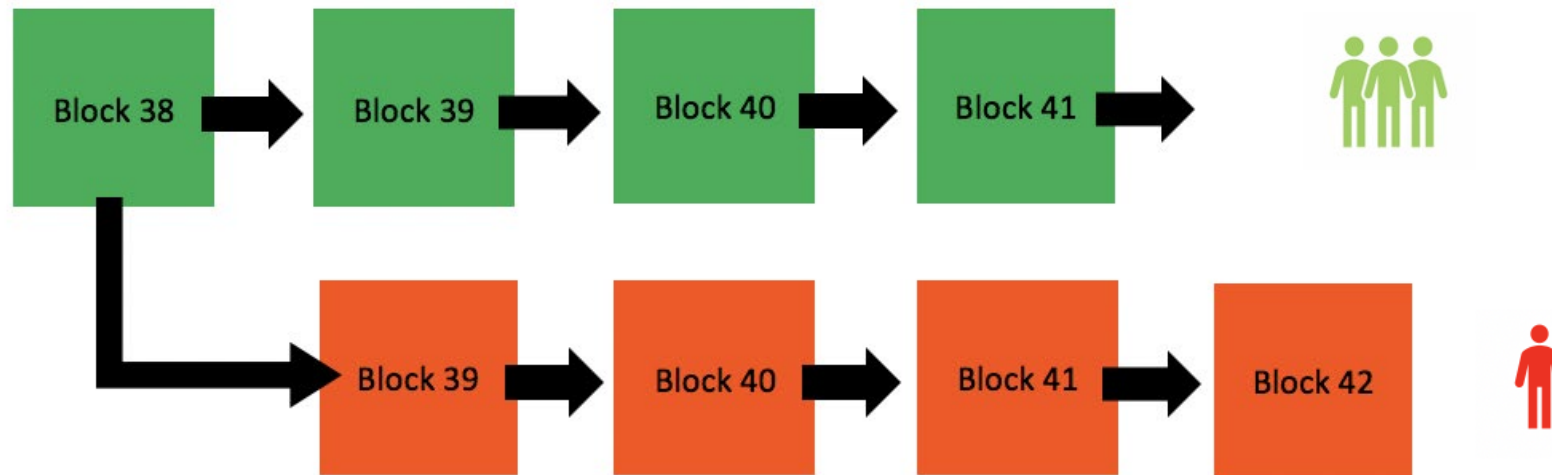


# Double-spending attack

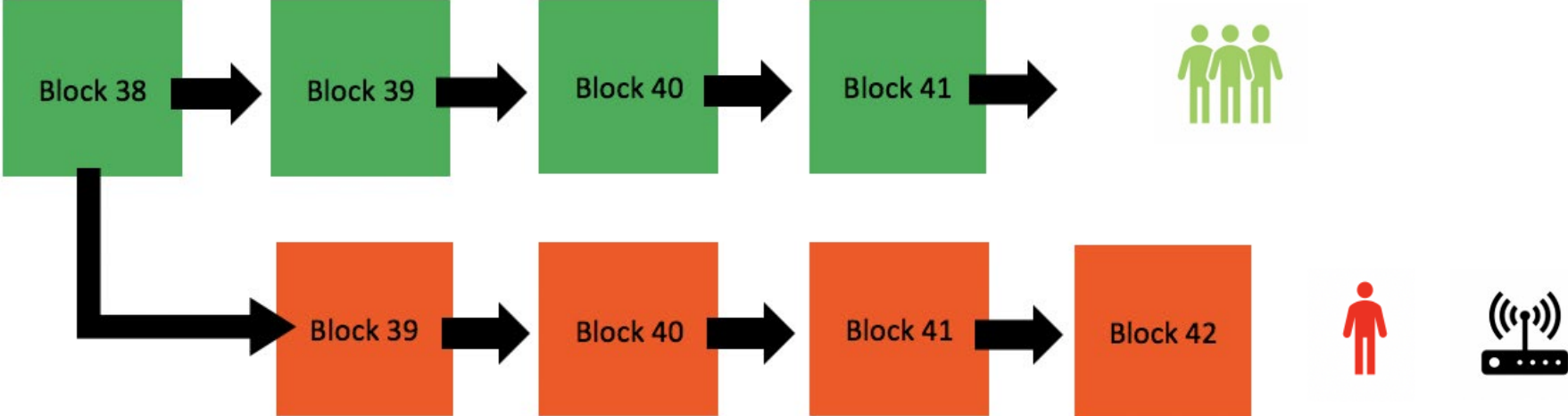




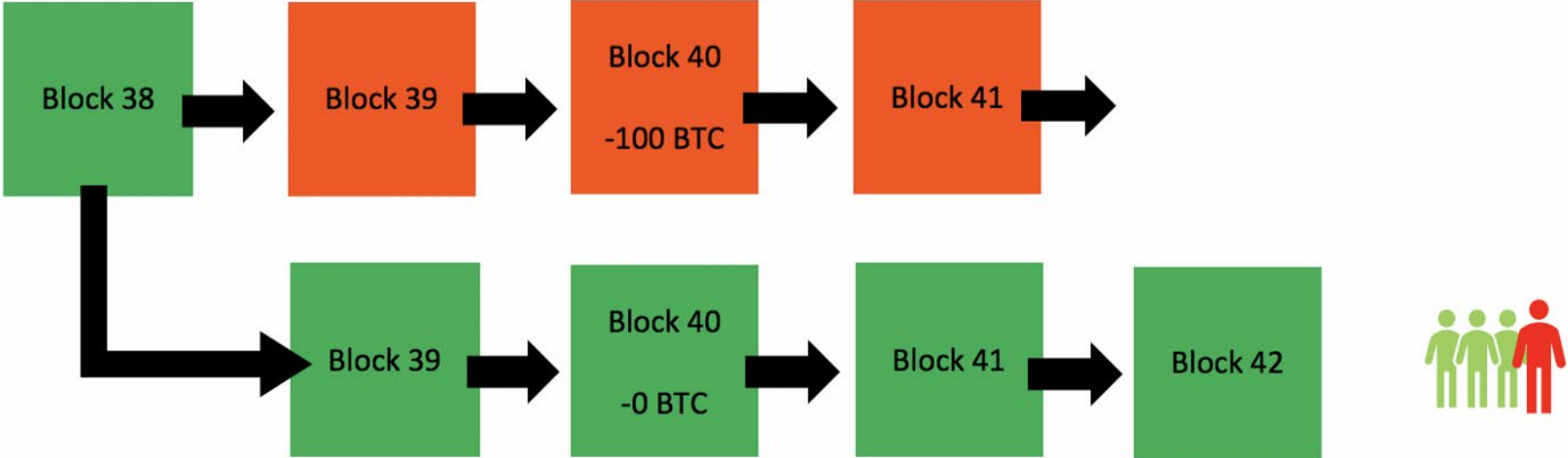
# Double-spending attack



# Double-spending attack



# Double-spending attack



# Double-spending attack

- An attacker needs a majority of mining power
- This requires an extensive investment in resources
- Also called the 51% attack
- Sometimes happens on immature coins
  - For some coins, it is easy to get a majority of mining power

# Altcoins

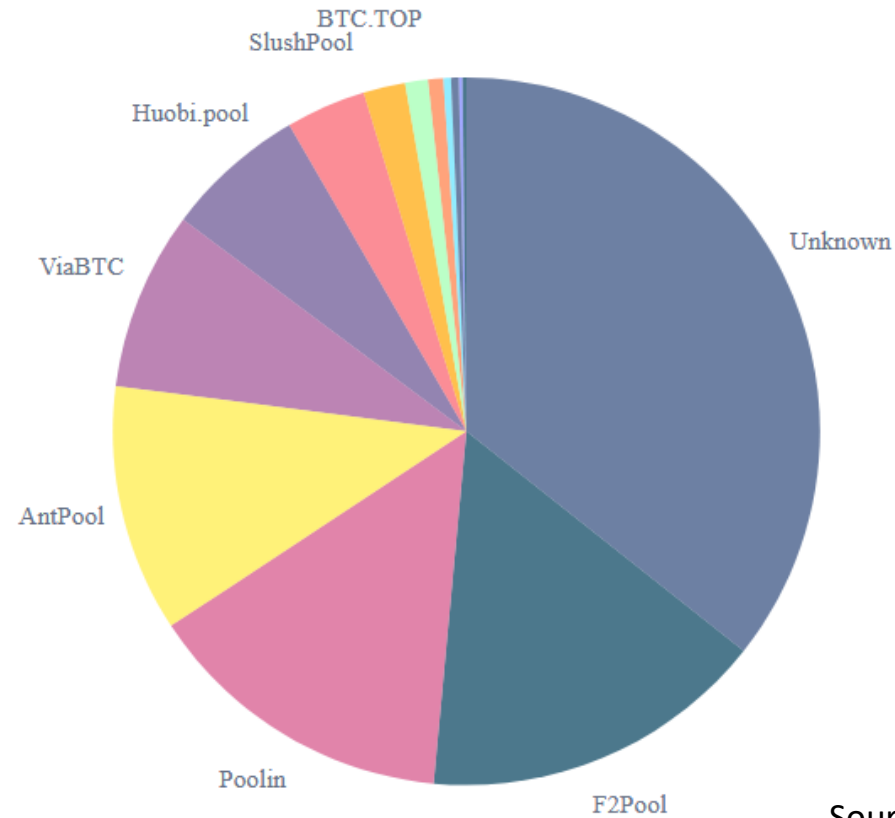
- Bitcoin-derived alternative coins
- Often use different parameters
  - Hashing algorithm
  - Block size
  - Mining difficulty
  - Block rewards



# Mining pools

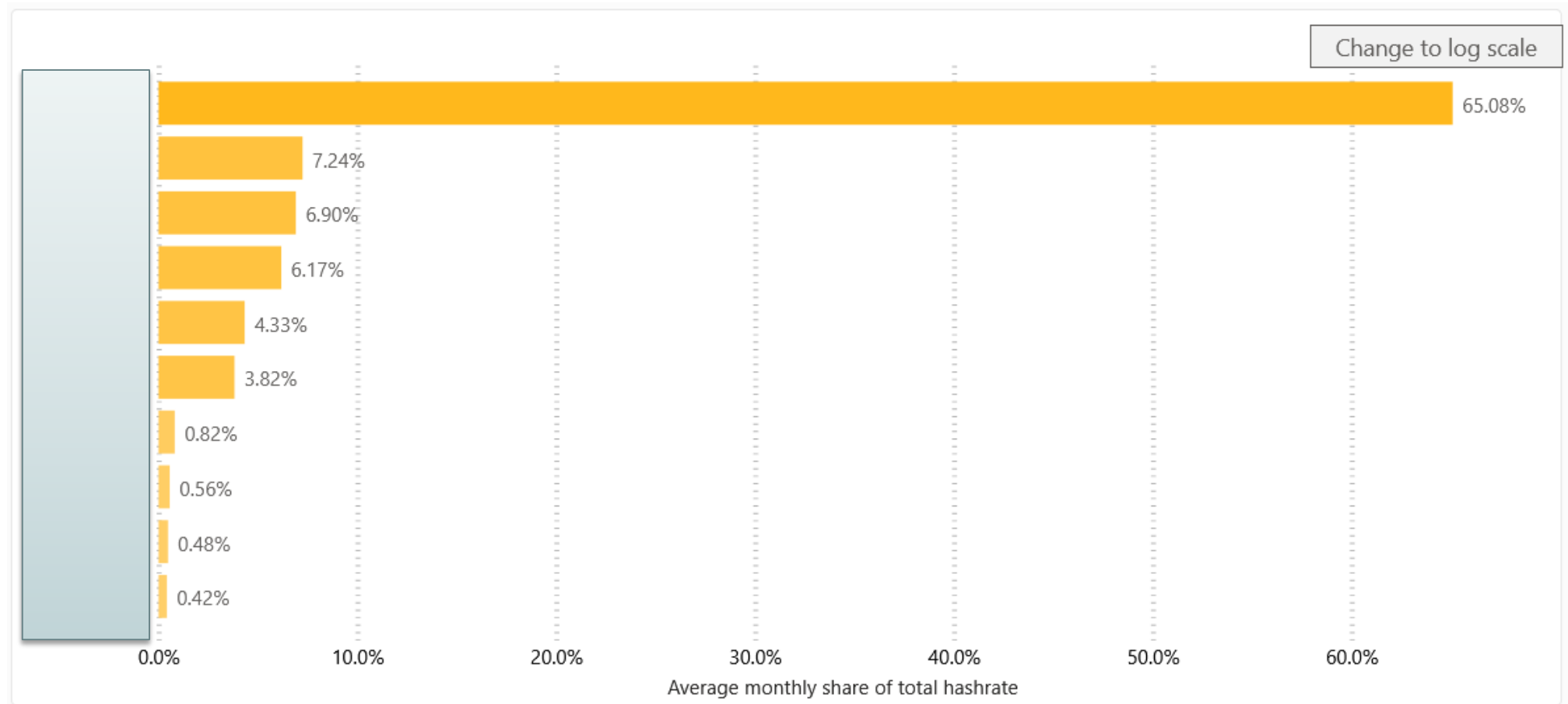
## Hashrate Distribution

An estimation of hashrate distribution amongst the largest mining pools.



Source: <https://www.blockchain.com/pools>

# Mining pools



Source: <https://www.blockchain.com/pools>

# Bitcoin Issues

- Scalability
  - Transaction throughput is bounded by block addition rate
  - > 1000 tx/sec throughput required to replace the Visa payment system
- Storage requirements
  - Blockchain is large; over 328 GB (Last year it was around 292 GB)  
(<https://www.blockchain.com/charts/blocks-size>)
- Unsure future
  - What happens when the block reward becomes low?
- Electricity usage



# Total World Production & Consumption

## Total electricity production



25 082 TWh



Bitcoin represents

**0.48 %**

## Total electricity consumption



20 863 TWh



Bitcoin accounts for

**0.55 %**

Source: <https://cbeci.org/cbeci/comparisons>, [International Energy Agency](#) report, 2016 est.

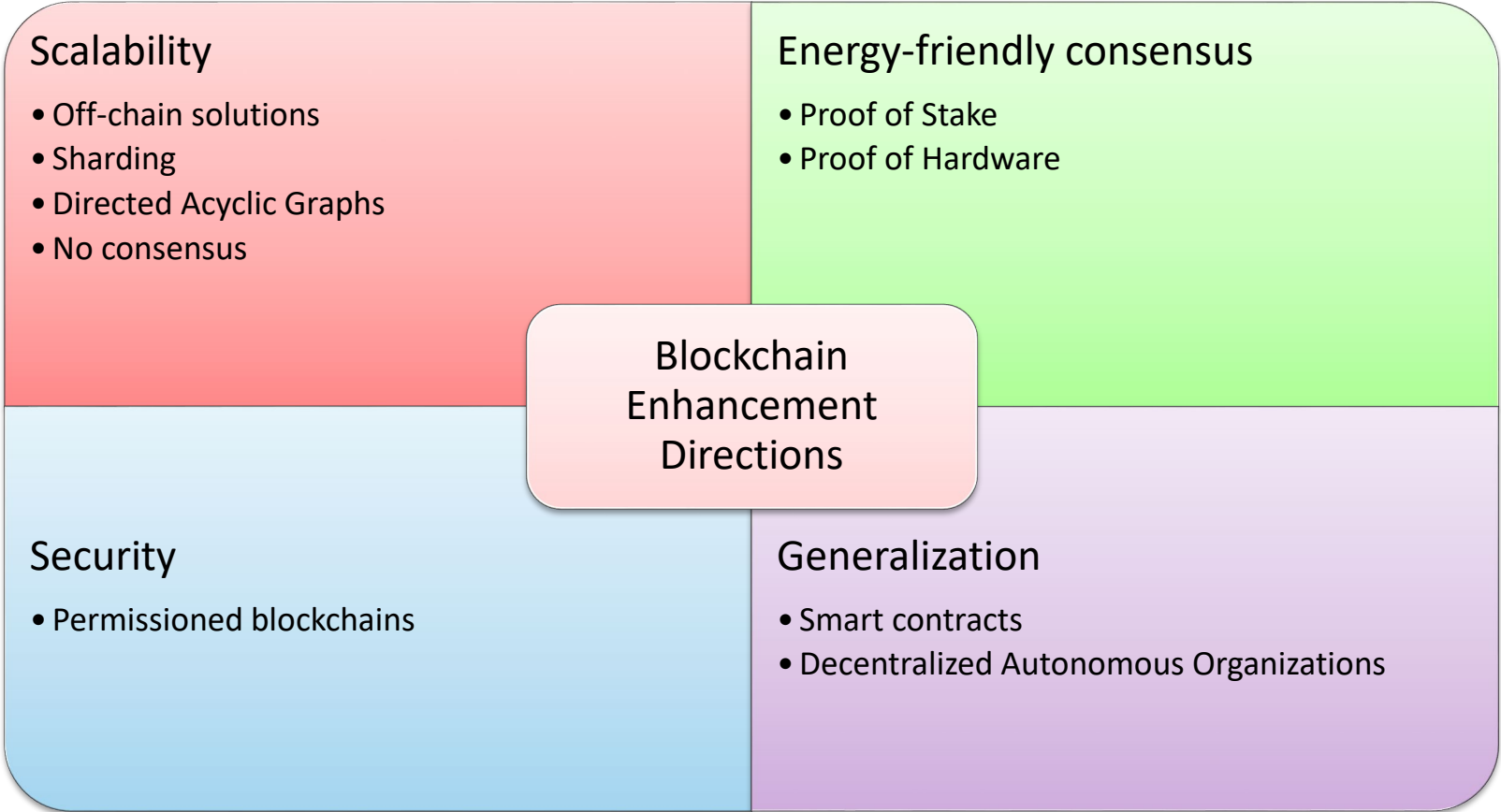
# Energy Consumption

## Country Ranking



Source: <https://cbeci.org/cbeci/comparisons>, [U.S. Energy Information Administration](https://www.eia.gov) country data, 2019 est. (or most recent available year)

# Enhancement



# Blockchain 2.0



ethereum

# Ethereum

- Founded in 2014
- Nodes in the network execute **smart contracts**
  - Executed within the Ethereum Virtual Machine
  - Written in the Solidity scripting language
- Gas, the “fuel” of the network
  - Every computing step that transforms the state consumes some gas

# Example of a smart contract

```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

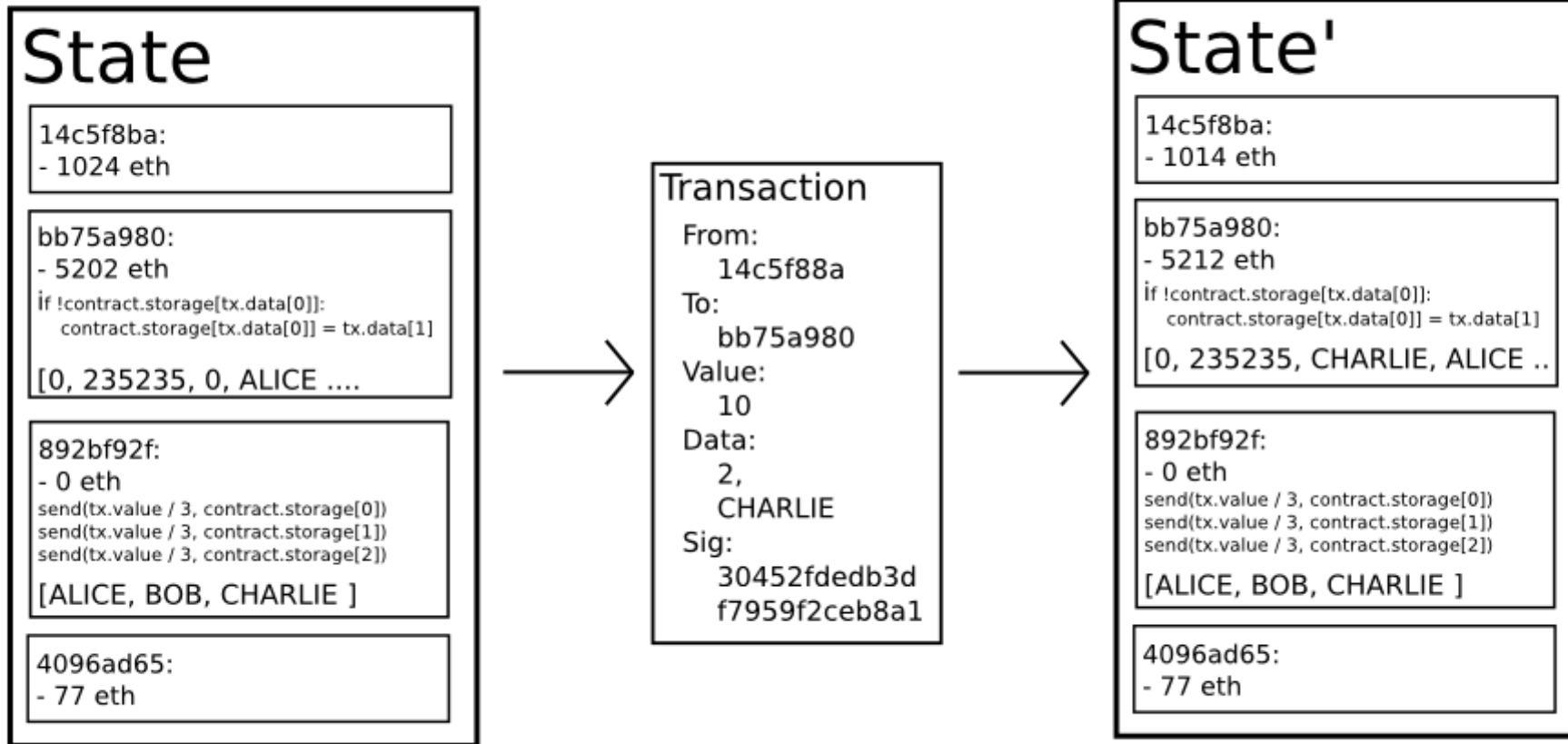
    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
    ) {
        balanceOf[msg.sender] = initialSupply;           // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        if (balanceOf[msg.sender] < _value) throw;       // Check if the sender has enough
        if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
        balanceOf[msg.sender] -= _value;                 // Subtract from the sender
        balanceOf[_to] += _value;                         // Add the same to the recipient
    }
}
```

# Ethereum accounts

- Externally owned accounts (EOAs)
  - No code attached to this account
- Contract accounts
  - Code execution triggered by transactions
- Transactions are created from EOAs

# Ethereum transactions





# Ethereum scalability

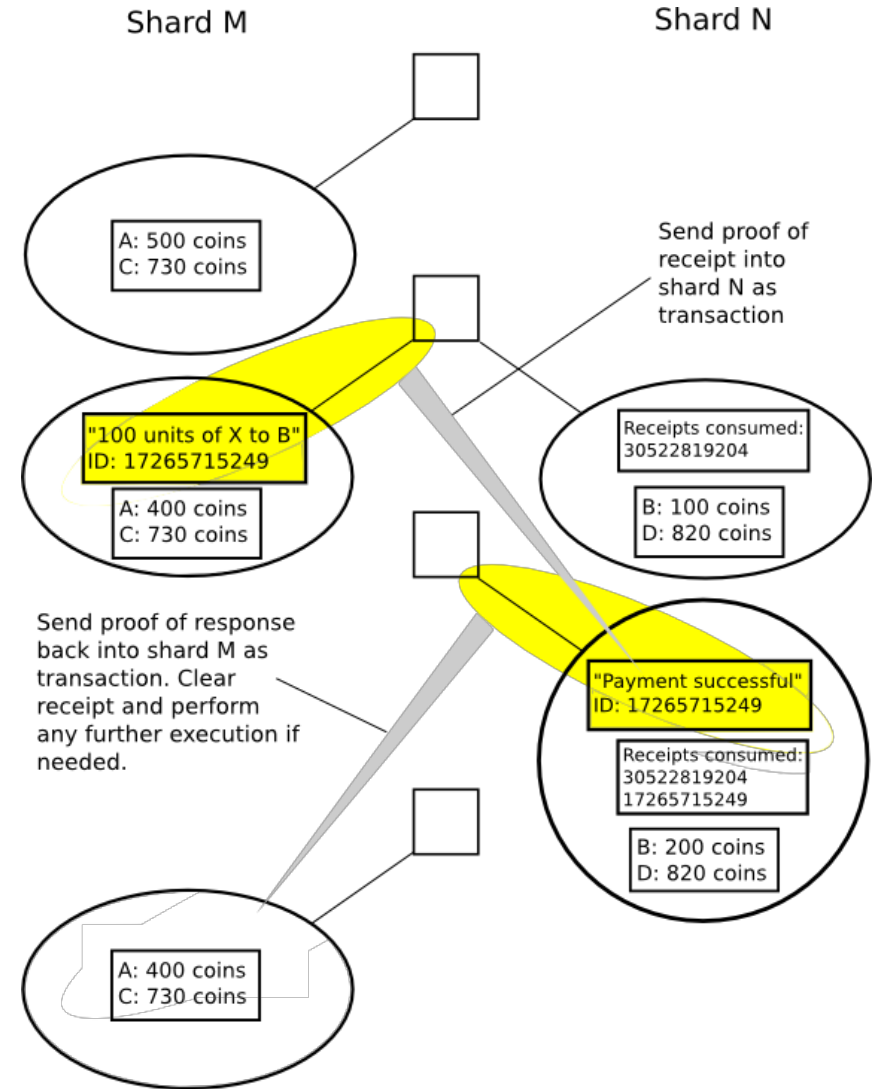
- One block mined around every 12 seconds
- When a block is mined, transactions in the block are executed by all miners
- Amount of transactions in a block determined by gas limit block and transactions

# (More) Scalable consensus: Proof-of-Stake





- The creator of the next block is chosen in a pseudo-random way, depending on his share of the chain.
- Ethereum plans to move to Proof-of-Stake consensus (Casper)
- Advantage:
  - Less (mining) energy consumption
- Disadvantage:
  - Working on a double spend is "free" (nothing at stake)

# Improving scalability: sharding

- Usually: one single state
- Idea: split up the state in different shards
  - I.e. Based on address space
- Keep communication as much within shards
- Inter-shard communication is expensive



# Other Blockchain Solutions in Short

	Permissioned	Permissionless
Specific		
Generic	 <b>HYPERLEDGER</b>	 ethereum

# Hyperledger Fabric



## HYPERLEDGER

- Permissioned
- Uses **Smart Contracts**
- Configurable consensus
  - relies on a backend service (known as the ordering service) that *intermediates* the messages between senders and receivers.
  - *Backend service ensures that all receivers will see messages in same order*

# Ripple (XRP)



- Permissioned network consisting financial institutions and banks
- Consensus: XRP Ledger Consensus Protocol (evolving)
- Currently, does not have a use case, is only a speculative token.

# Ripple (XRP)



## Rocketing Ripple Puts Founders and CEO Among the World's Richest People

admin January 04, 2018

The post Rocketing Ripple Puts Founders and CEO Among the World's Richest People appeared first on CCN

The value of the cryptocurrency ecosystem has surpassed 1,000% gains. Ripple's XRP took the beginning of 2017 and is currently trading at the second-biggest cryptocurrency by market cap.

The post Rocketing Ripple Puts Founders and CEO Among the World's Richest People appeared first on CCN

The post Rocketing Ripple Puts Founders and CEO Among the World's Richest People appeared first on CCN

U.S. SECURITIES AND EXCHANGE COMMISSION

VISIONS & OFFICES | ENFORCEMENT | REGULATION | EDUCATION

### Press Release

## SEC Charges Ripple and Two Executives with Conducting \$1.3 Billion Unregistered Securities Offering

**FOR IMMEDIATE RELEASE**  
**2020-338**

Washington D.C., Dec. 22, 2020 — The Securities and Exchange Commission announced today that it has filed an action against Ripple Labs Inc. and two of its executives, who are also significant security holders, alleging that they raised over \$1.3 billion through an unregistered, ongoing digital asset securities offering.

## Jed McCaleb Sells \$22 Million Worth of XRP, Ripple Cofounder's Stash Could Run Dry by May

Bitcoin.com | 14 February 2021 - 23:00:31



During the last few weeks, the former Ripple executive Jed McCaleb has reportedly been selling millions of XRP tokens and every sale has been monitored by the public. On Sunday, McCaleb dumped another 38 million XRP worth \$22 million after selling 95 million XRP last week worth \$56 million today. Ripple Cofounder Sells 38 million [...]

# Bitcoin-NG

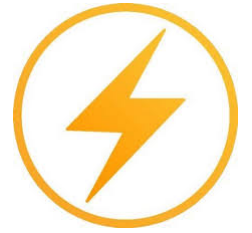
- Motivation: Bitcoin loses incentive-compatibility when attacker size  $> 29\%$
- Solution:
  - Single-chain
  - 2 types of blocks:
    - Macro blocks: Proof of Work
    - Micro blocks: Their transaction fees go to creator of macro-blocks



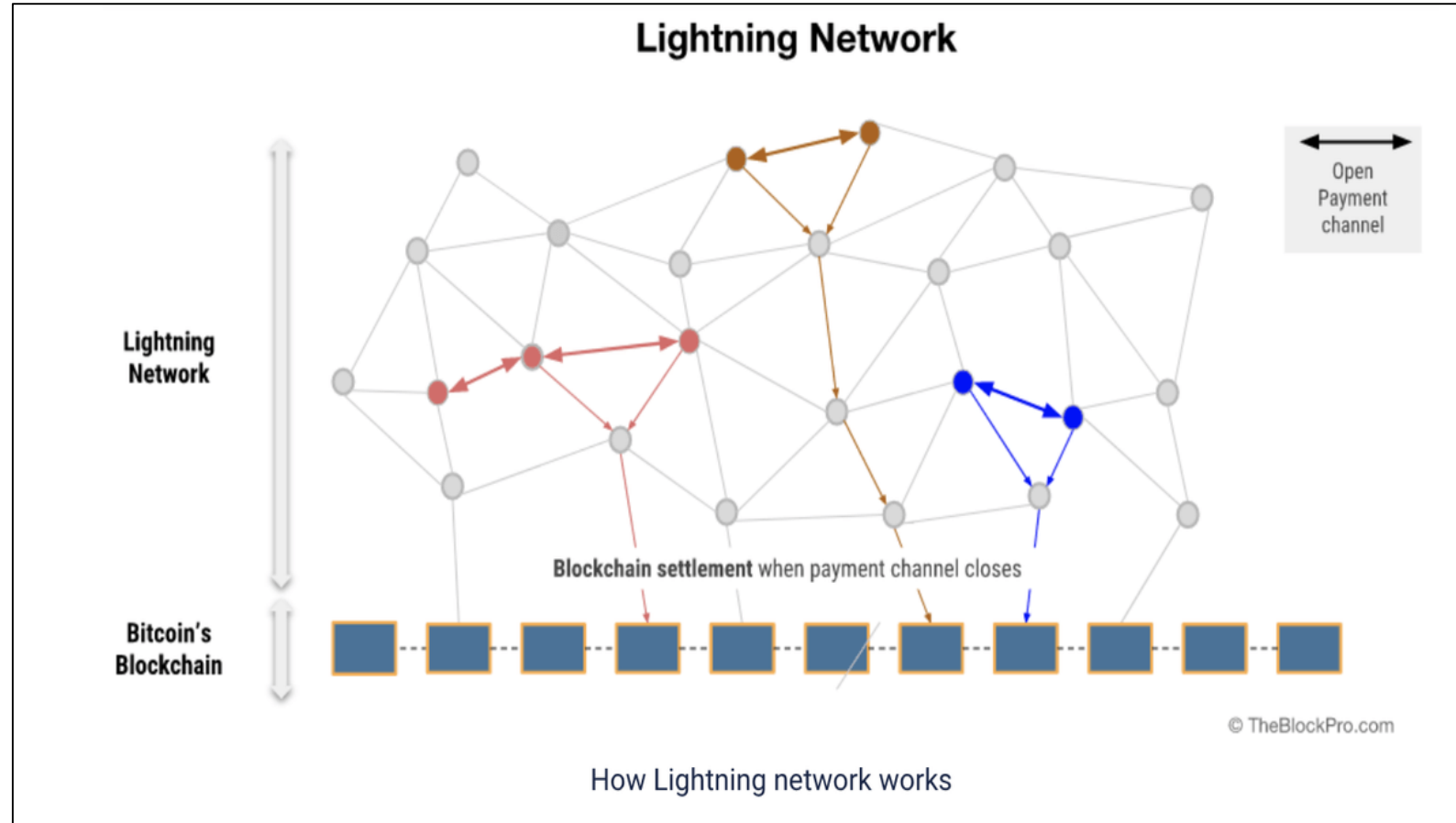
Source: <https://hackingdistributed.com/2015/10/14/bitcoin-ng/>



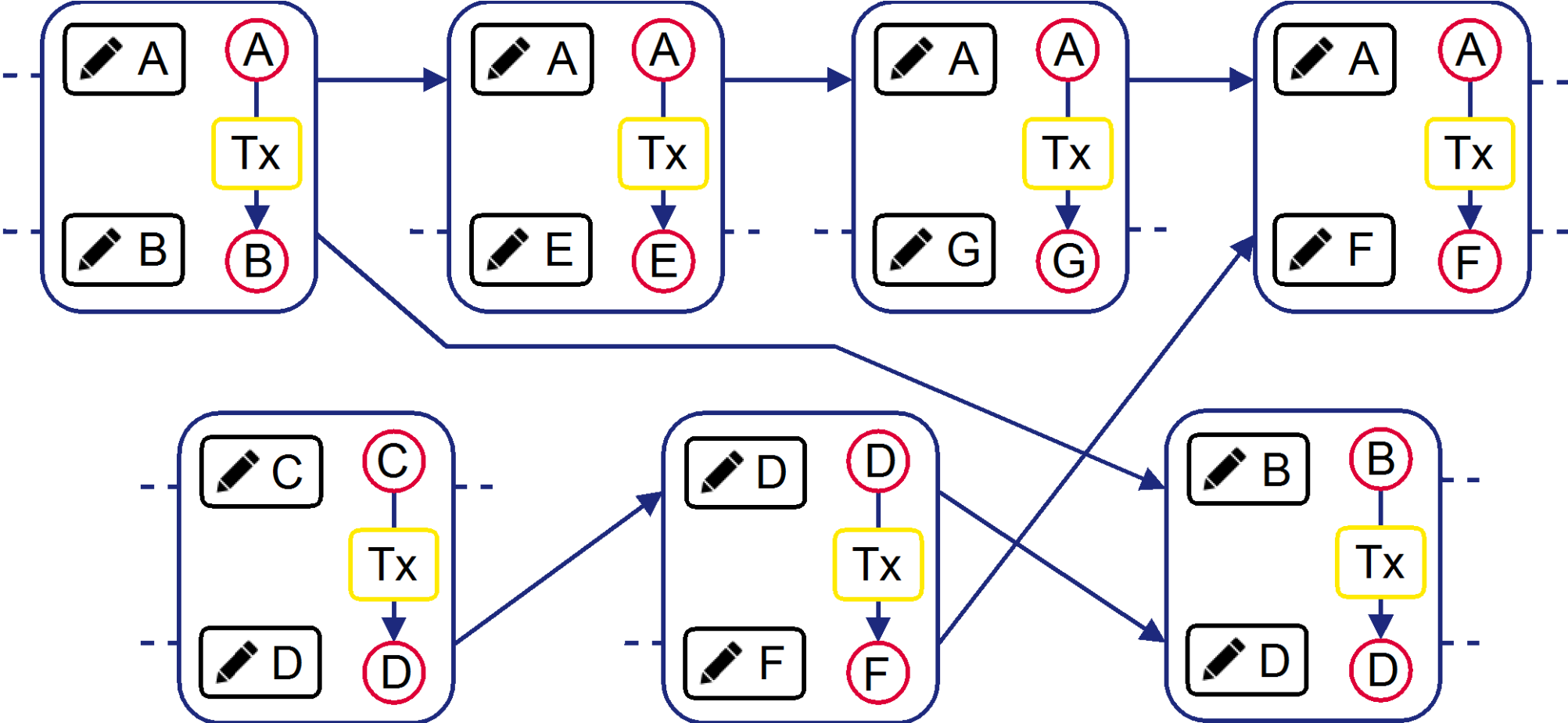
# Lightning Network



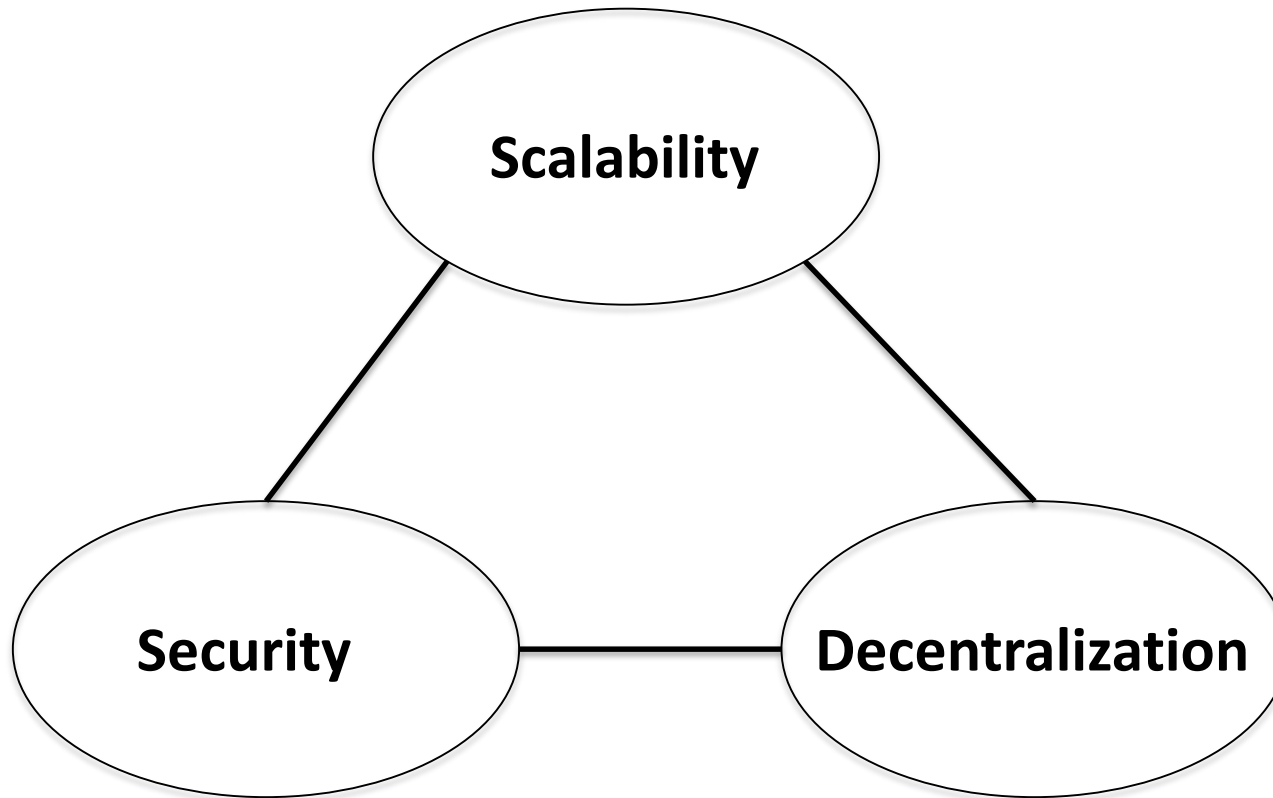
- Layer-2 payment protocol (on top of Bitcoin)
- Attacks scalability problem
- Off-chain transactions: No need to store all transactions on bitcoin



# Blockchain 3.0



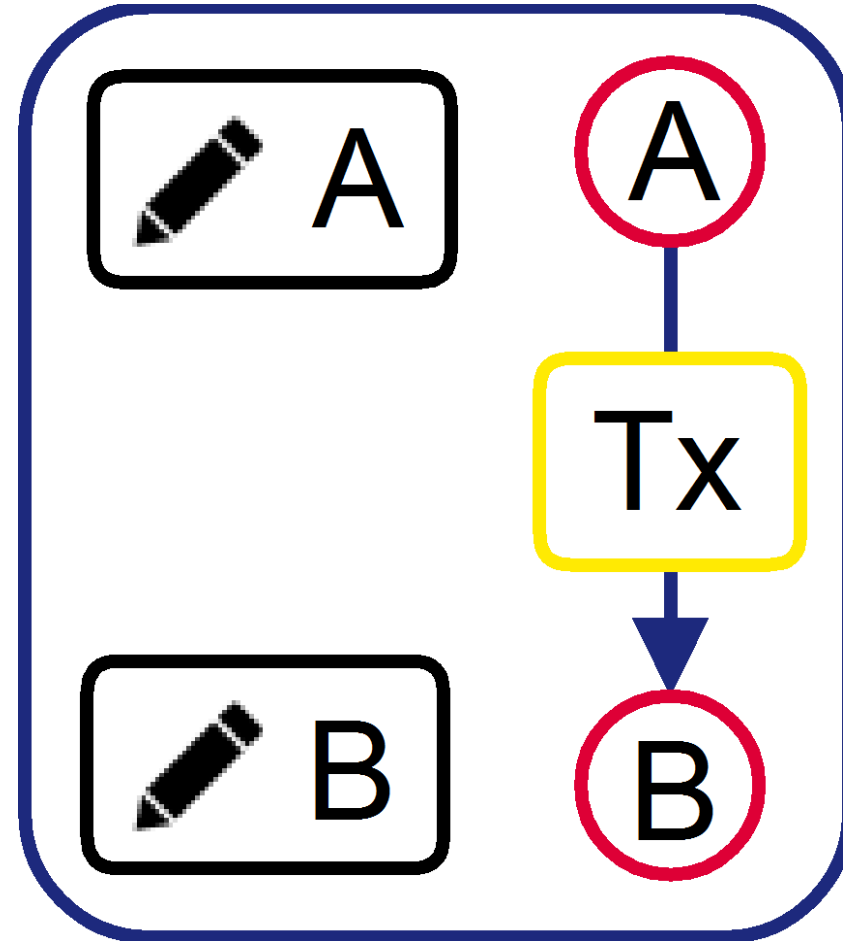
# The scalability trilemma (?)





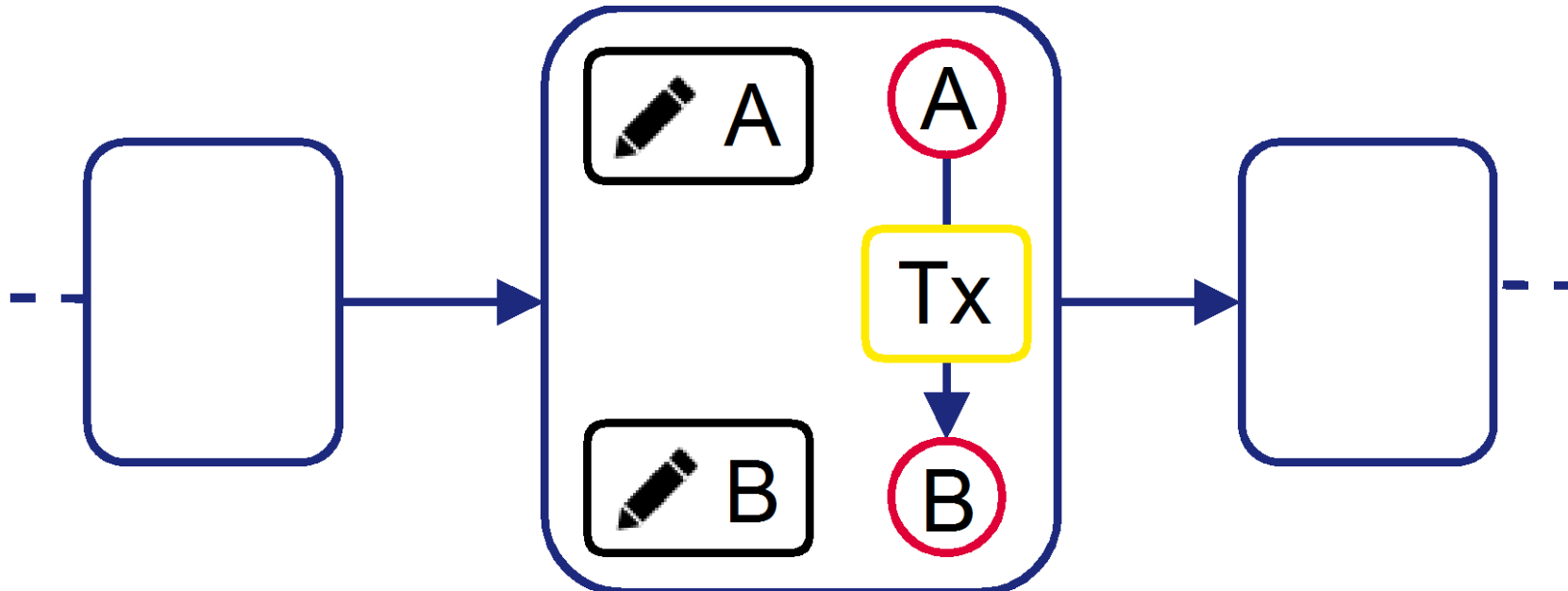
# Transaction

- Consider a transaction between two users
- Both users sign the transaction
  - Using any secure signing algorithm
  - Irrefutable participation



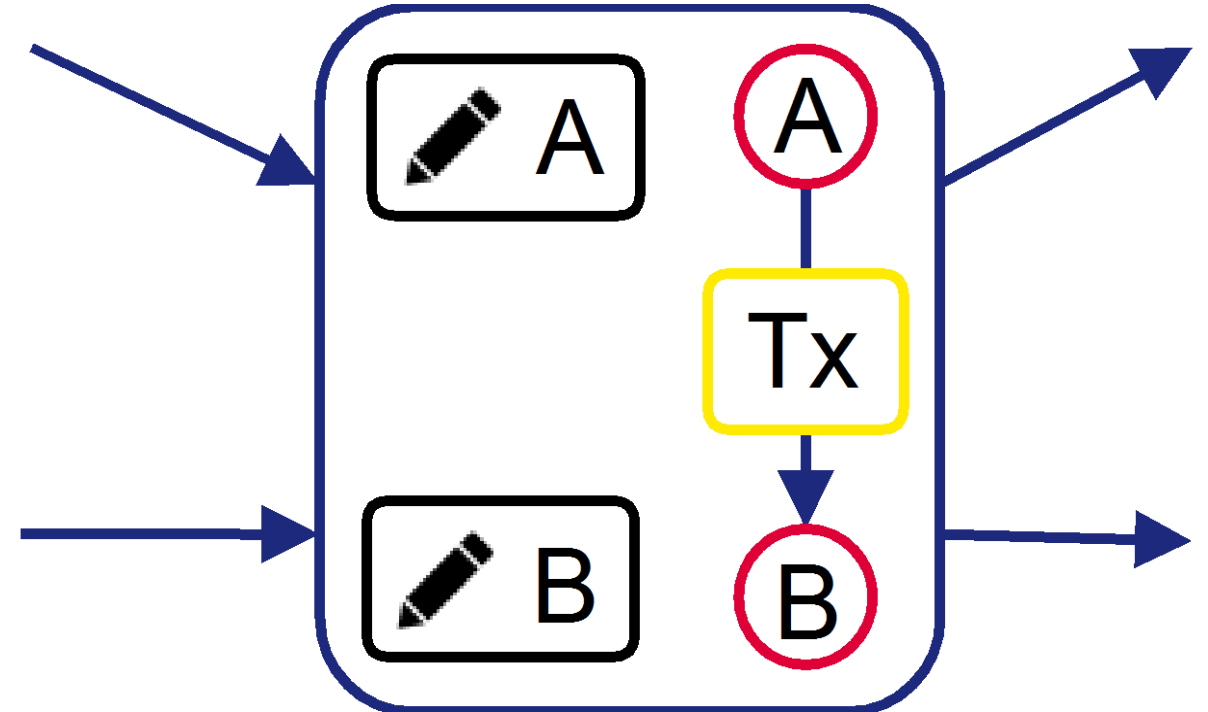
# Transaction Chaining

- We can chain these transactions together
- Each users keeps track of his own transaction history

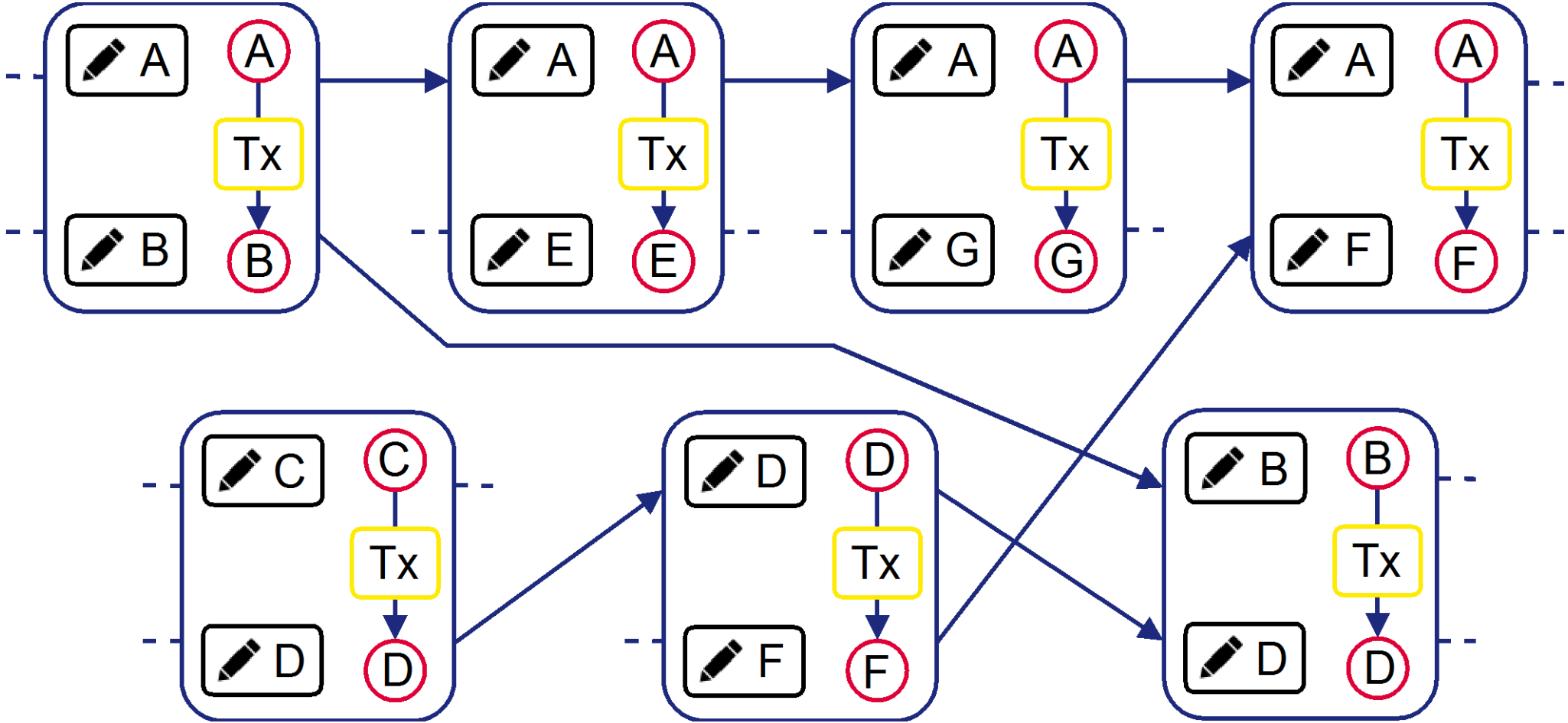


# Improving Security

- We add an additional pointer to each block
  - Points towards the previous block in the chain of the transaction counterparty



# Entangled Chains





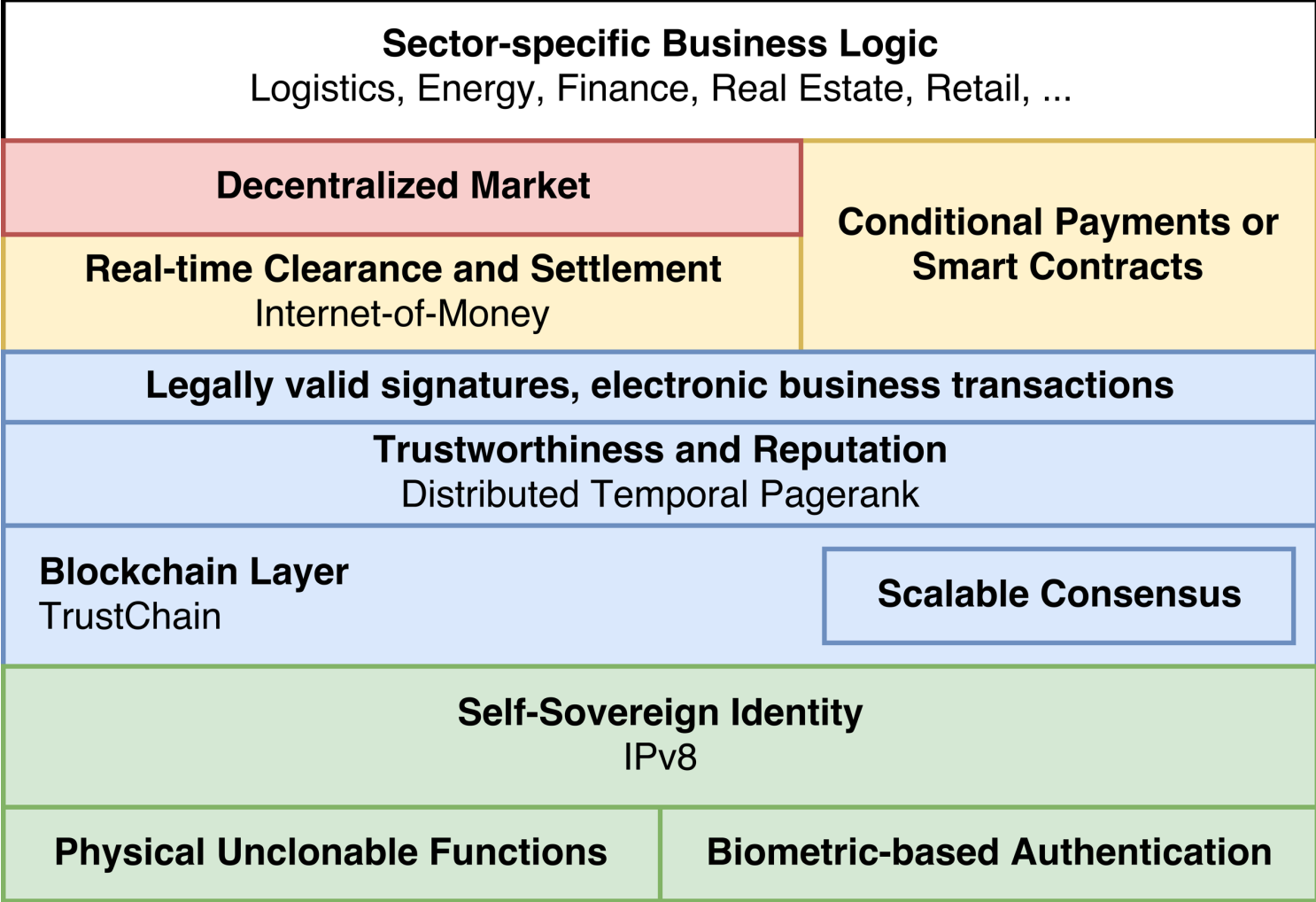
# TrustChain properties

- Entanglement makes it hard to tamper with the chain
- Scalable
  - Transactions are not dependent on other users in the network
- Lower storage requirements
  - We only need to store our own chain and (parts of) the chains of transaction partners

# What can we do with TrustChain?

- Build a digital identity (ongoing project with Dutch government)
  - Real-time money routing with *real* IBAN accounts
  - Large-scale Bandwidth accounting
  - Build a scalable decentralized exchange
  - ... ?
- 
- **No cryptocurrencies required, just accounting!**

# Delft Technology Portfolio



# Tribler

- Our academic, experimental playground
- Peer-to-peer file sharing software
- 1.8 million downloads
- Anonymous downloading and seeding
  - Tor-like overlay network
- Video-on-Demand



<https://tribler.org>

# Future

- Blockchain managed to decentralize currency
- Why not to

decentralize everything?

- Properties? Companies?

# Decentralized Autonomous Organization

- An organization represented by computer-programmed rules
- The rules upon which the company functions are enforced digitally
- Emerged with the generalization of application domain: Smart contracts
- The program is controlled by all shareholders
- No central government
- Transaction records and program rules are stored in blockchain

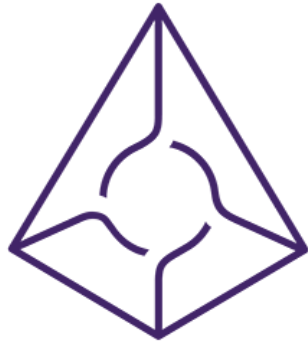


Source: <https://blog.codecentric.de/en/2017/09/decentralized-autonomous-organization-blockchain/>

# Decentralized Autonomous Organization

- Self-organization
- Feedbacks from shareholders
- Meritocratic: Your position in organization is based on the value you contributed
- Contribution is measured with tokens (reputation)
- Diversity of perspectives

# DAO Examples



AUGUR

a decentralized prediction market



**Aragon**

open-source software project for the creation and management of decentralized organizations

(plug and play company setup)



A social media platform.  
You get money for creating content.