Bitcoin and Cryptocurrencies

- Lecture 10: Consensus
- Professor Radjabov Mukhammad

Consensus components

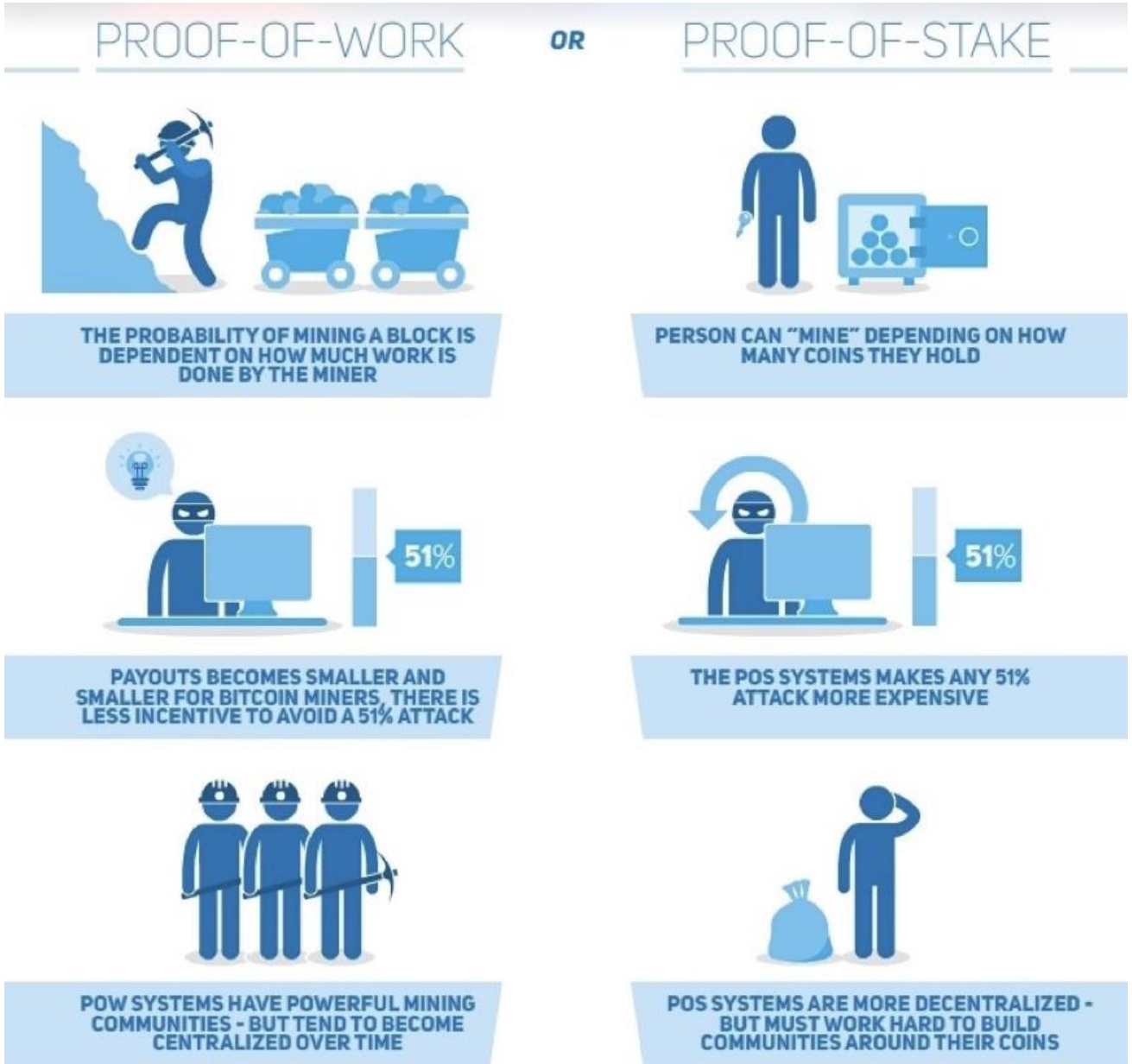
- **Principles and paradigms of distributed systems**
  - ***Byzantine fault tolerance*** (BFT): the dependability of a fault-tolerant computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component has failed.
  - The objective of BFT is to defend against failures of system components with or without symptoms that prevent other components of the system from reaching an agreement among themselves, where such an agreement is needed for the correct operation of the system.
  - One example of BFT in use is bitcoin. The bitcoin network works in parallel to generate a blockchain with proof-of-work allowing the system to overcome Byzantine failures and reach a coherent global view of the system's state.

Consensus components

- **Blockchain consensus algorithms**
  - Behind every cryptocurrency, there's a consensus algorithm. No consensus algorithm is perfect, but they each have their strengths. In the world of crypto, consensus algorithms exist to prevent double spending.

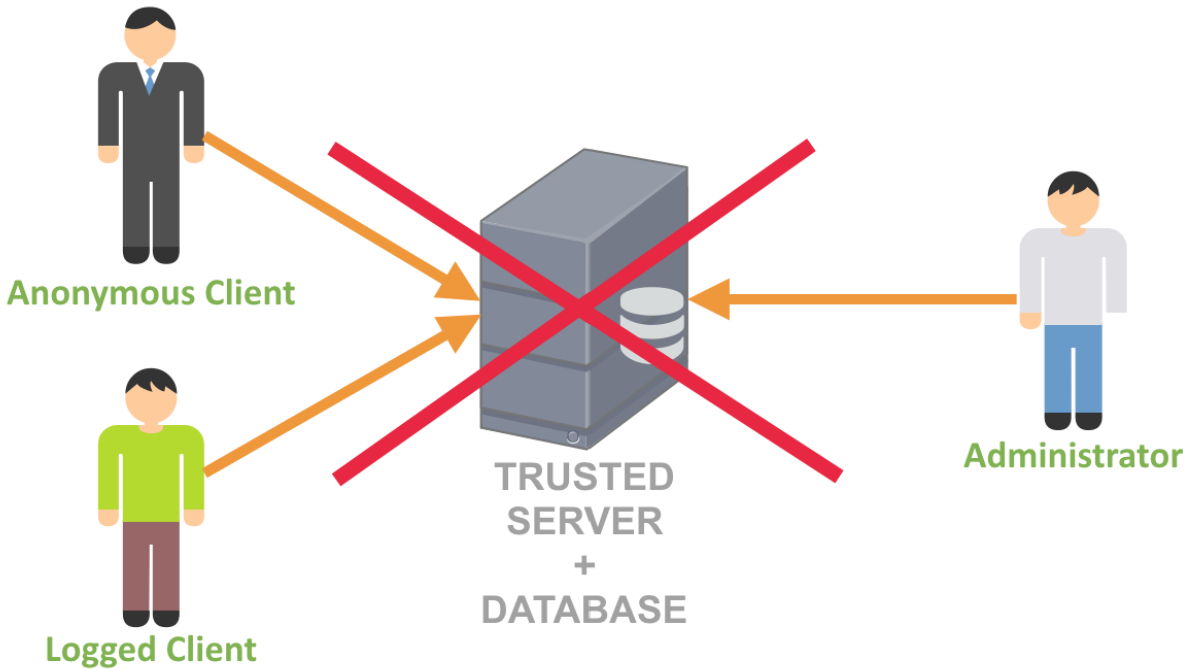
  - Proof of Work (PoW)
  - Proof of Stake (PoS)
  - Delegated Proof of Stake (DPOS)
  - Proof of Burn (PoB)
  - Practical Byzantine fault tolerant Mechanism (PBFT)
  - …

Consensus components



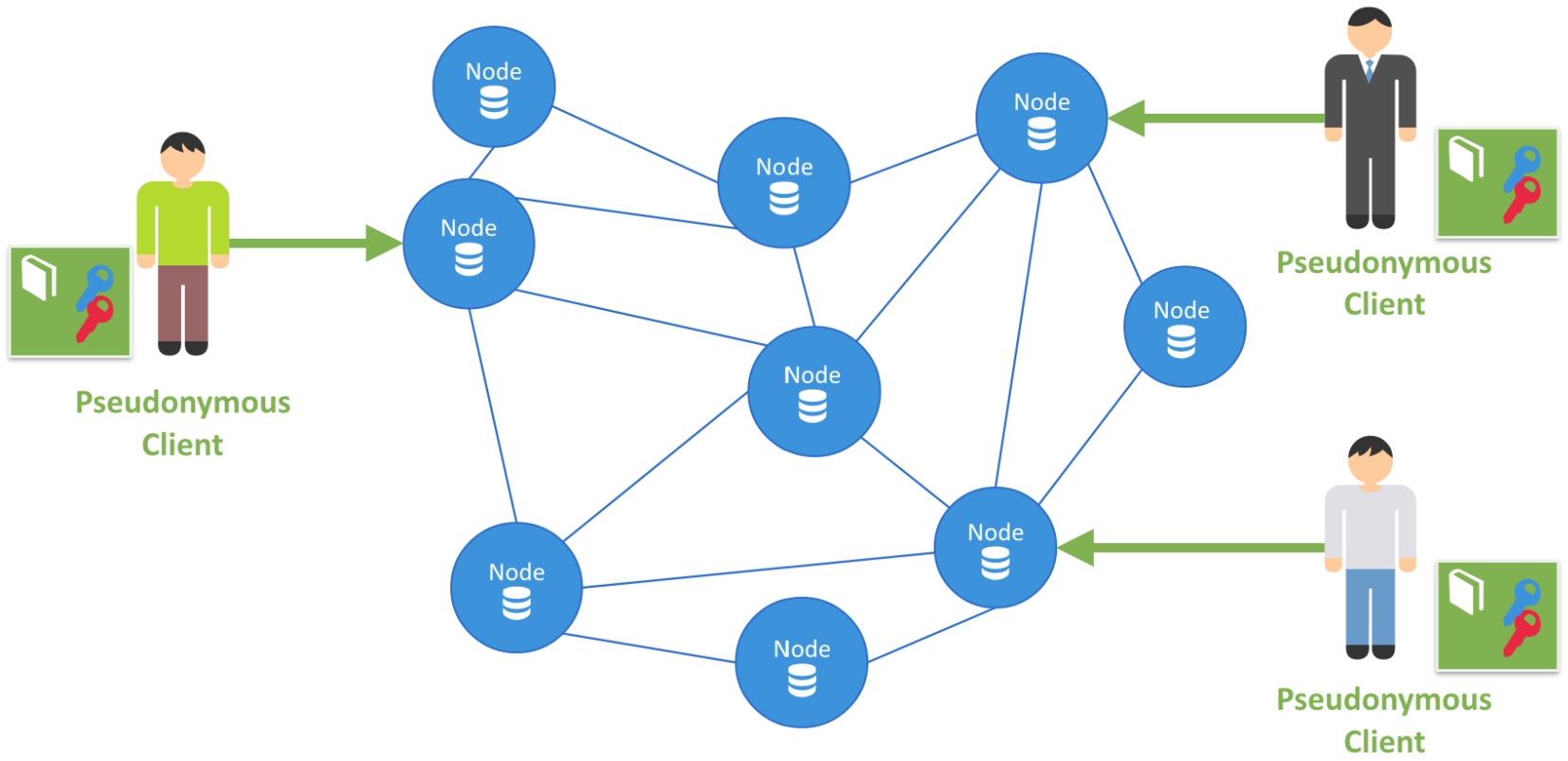
Consensus components

- **Blockchain structure**
  - No more client/server architecture with name roles



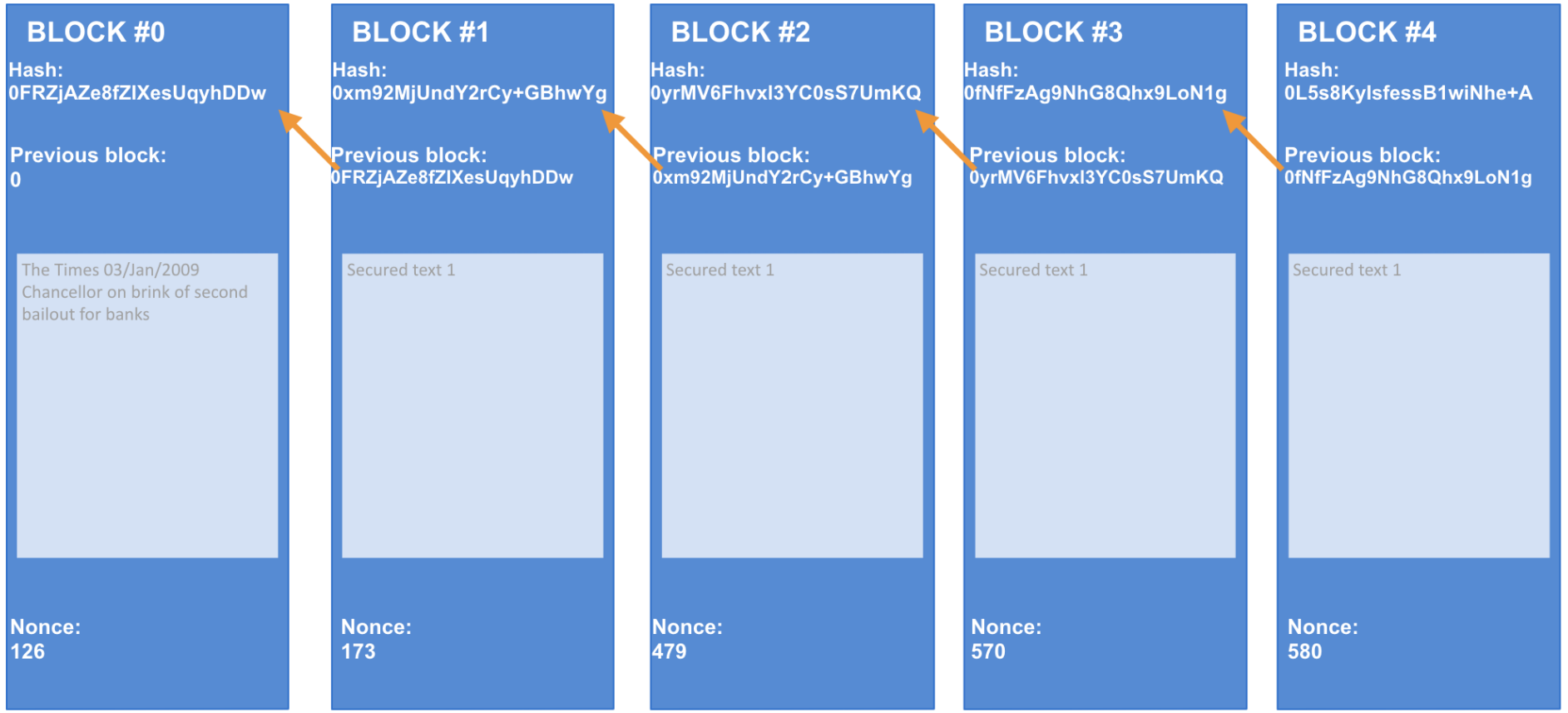
Consensus components

- **Blockchain structure**
  - Peer-to-peer Architecture with pseudonymous client bearing key pairs. Each node as a database copy.



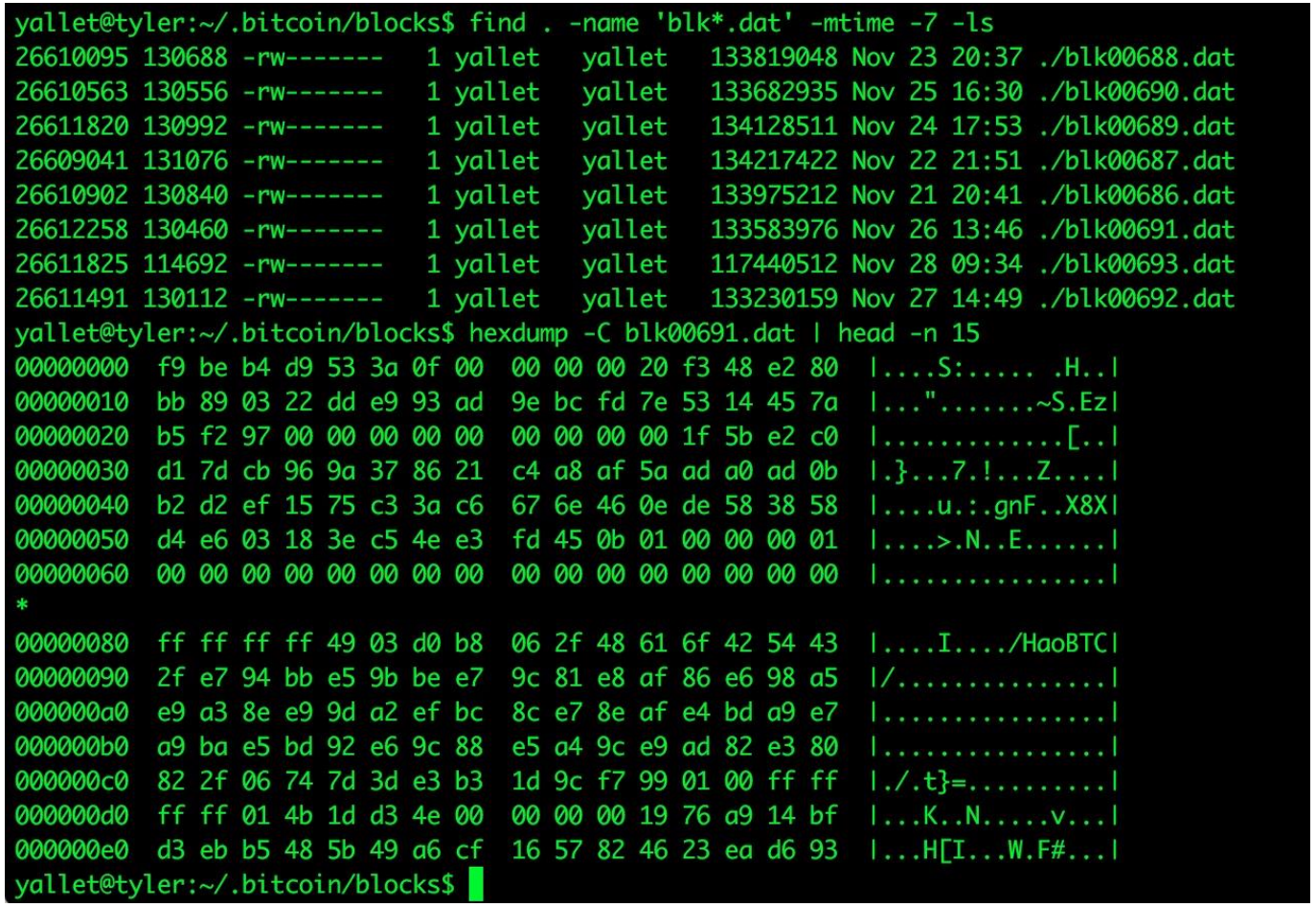
Consensus components

- **Blockchain structure**
  - Data structure:



Consensus components

- **Blockchain structure**
  - Blocks of data:



Consensus components

- **Types of blockchain**
  - There mainly three types of Blockchains that have emerged after Bitcoin introduced Blockchain to the world.
  - ✓ Public Blockchain:

no one in charge, anyone can participate in reading/writing/auditing the blockchain (i.e. Bitcoin, Litecoin, etc.)

  - ✓ Private Blockchain:

a private property of an individual or an organization, there is one in charge of important things such as read/write or whom to selectively give access to read or vice versa (i.e. Bankchain)

  - ✓ Consortium or Federated Blockchain:

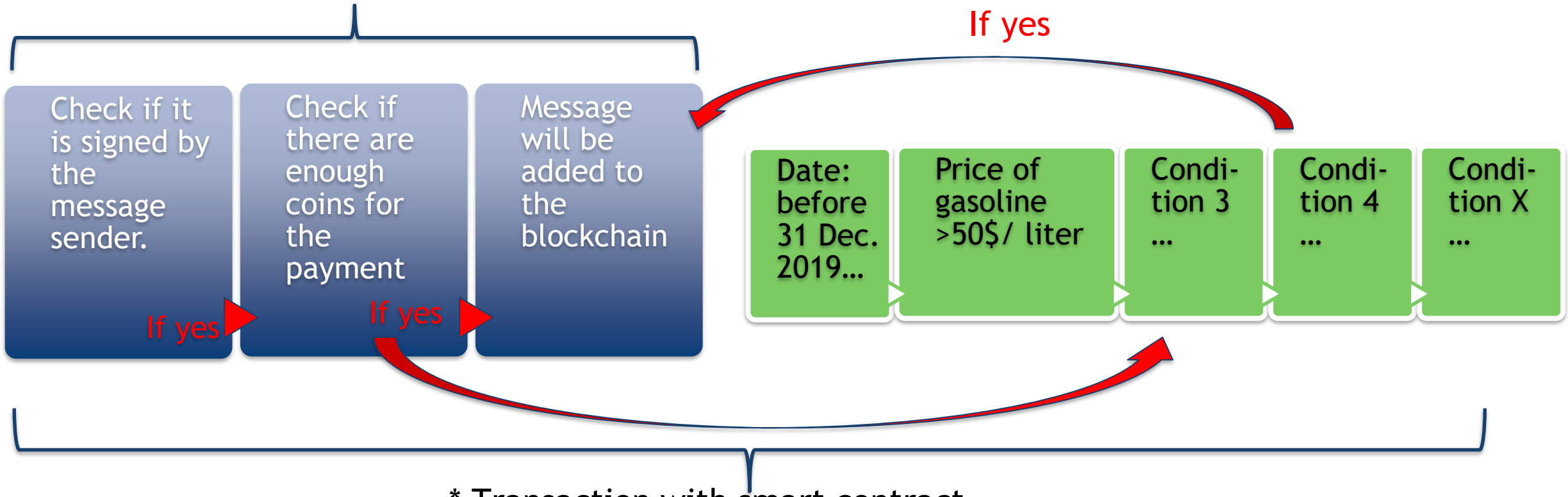
More than one in charge. A group of companies or representative individuals come together and make decisions for the best benefit of the whole network (i.e. r3, EWF)

Smart Contract Theory and architecture

- **Smart Contract Theory**
  - A computer protocol designed digitally facilitate, verify, or enforce the negotiation or performance of a contract.
  - It allows the performance of credible transactions without the third parties.
  - The transactions are traceable and irreversible.

Smart Contract Theory and architecture

- **Smart Contract architecture**

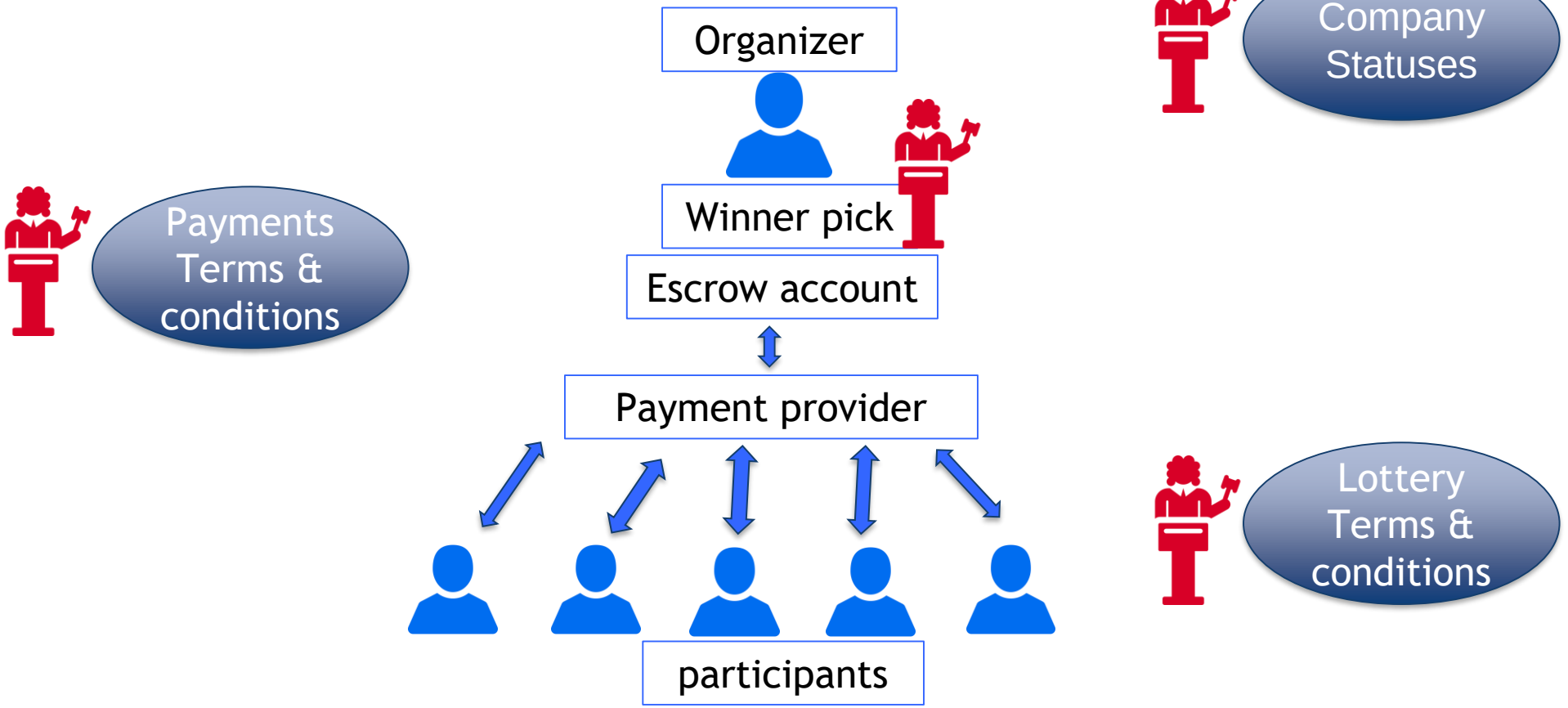


Architectures and decentralized autonomous systems

- **DAO** (Decentralized Autonomous Organization)
  - An organization represented by rules encoded as a computer program, which is transparent, controlled by shareholders and not influenced by a central government.
  - It's notionally like the example for getting funds for a small conference, except that it includes much more. Members buy shares in the DAO and can vote on things according to the number of shares they have. The dreamers have the idea they'll replace Democracy and run entire countries this way.
  - The DAO was the largest crowdfunding in history, having raised over $150m from more than 11,000 enthusiastic members. (ICO)
  - A DAO’s financial transaction record and program rules are maintained on a blockchain.

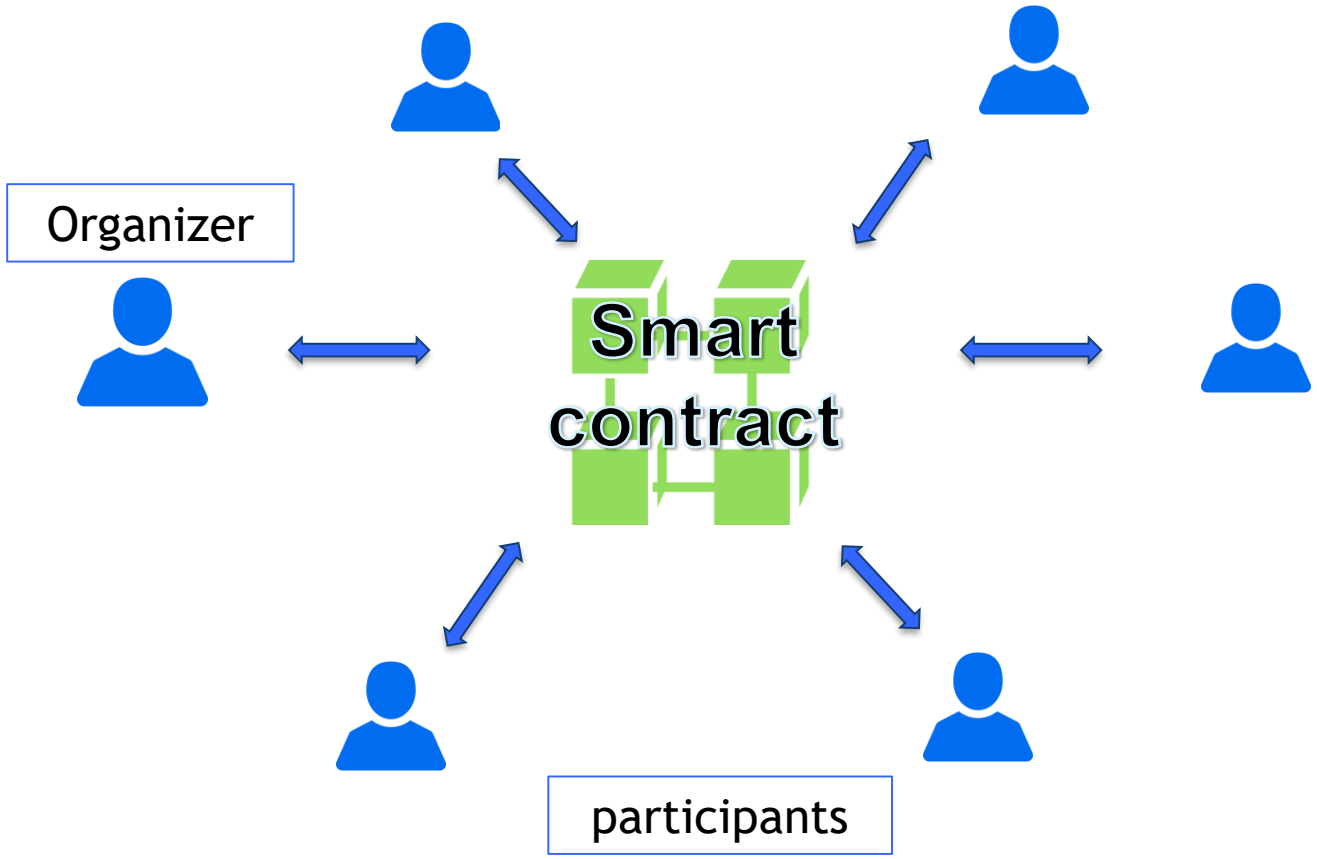
Smart contract application

- **Example 1: Lottery**
  - Lottery without smart contract



Smart contract application

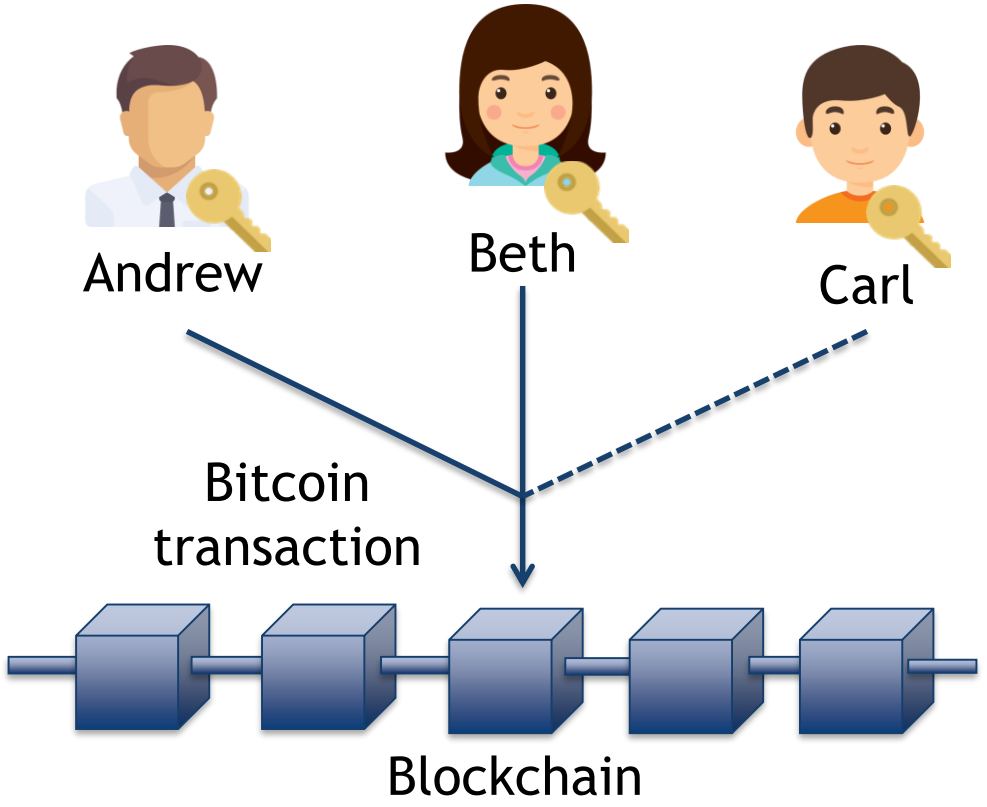
- **Example 1: Lottery**
  - Lottery with smart contract



Smart contract application

- **Example 2-1: Group wallets**
  - Enforcing at least 2 out of 3 people of a group to agree to create a valid transaction

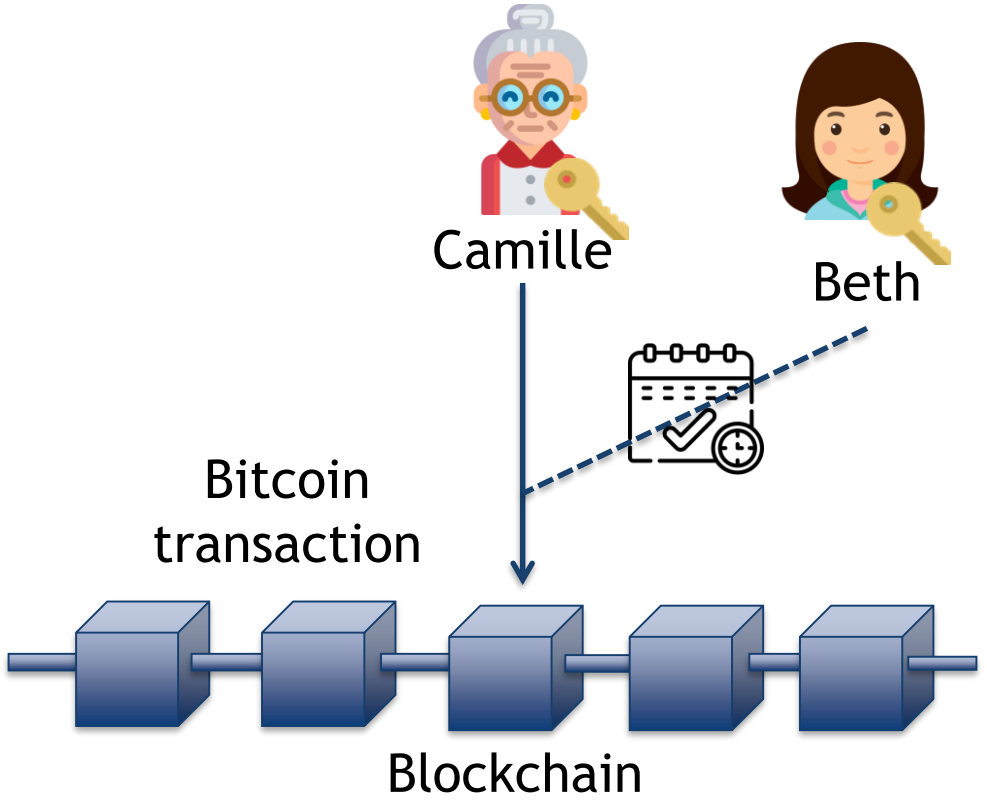
```
2 <pubKeyAndrew>
<pubKeyBeth>
<pubKeyCarl> 3
CHECKMULTISIG
```



Smart contract application

- **Example 2-2: Heritage wallets**
  - Enforcing that a transaction must be signed either by Camille OR by Beth after 5 years

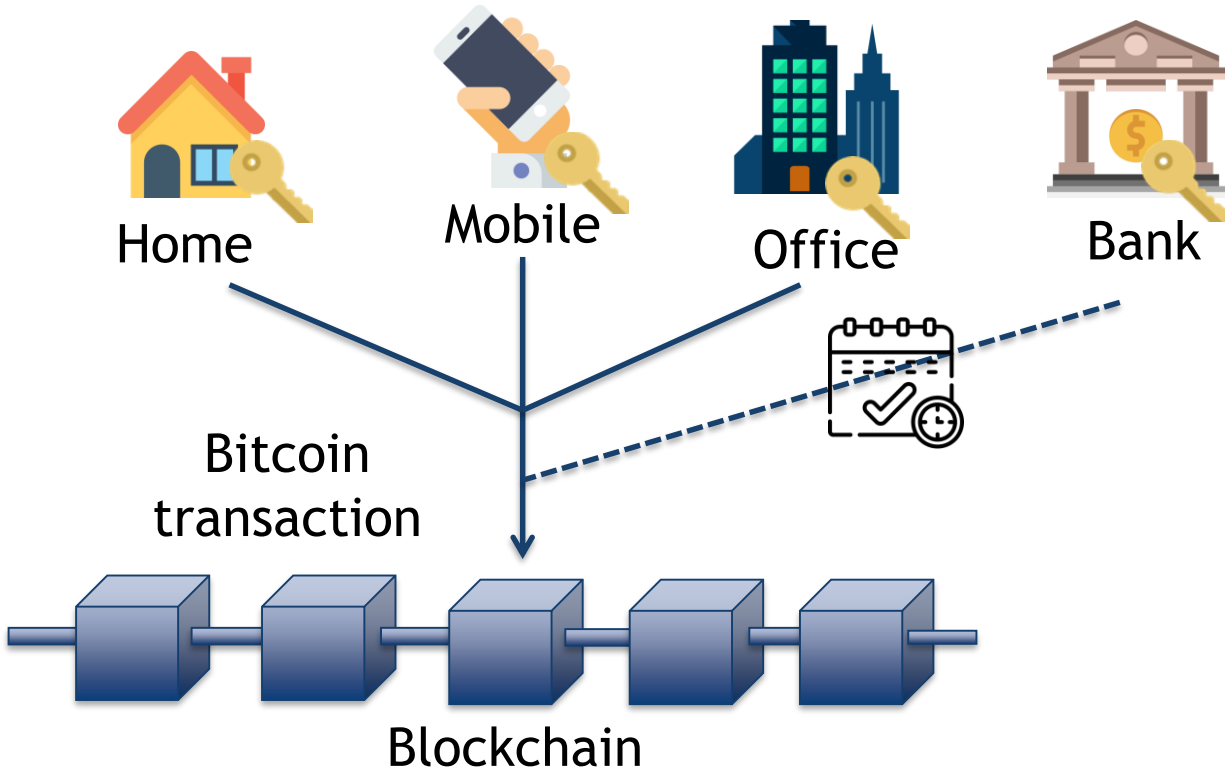
```
IF
   <pubKeyCamille>
   CHECKSIG
ELSE
   <5 y> CLTV DROP
   <pubKeyBeth>
    CHECKSIG
ENDIF
```



Smart contract application

- **Example 2-3: Secure storage**
  - Enforcing that a transaction must be signed by either 3 devices in different locations OR a recovery key deposited in the bank after 8 months

```
IF
      3 <pubKeyHome>
       <pubKeyMobile>
       <pubKeyOffice> OP_3
       CHECKMULTISIG
ELSE
      <8 m> CLTV DROP
      <pubKeyBank>
      CHECKSIG
ENDIF
```



Existing blockchain applications, related structures and architectures

- **ERC-20**
  - Proposed on November 19, 2015 by Fabian Vogelsteller.
  - A technical standard used for smart contracts on the Ethereum blockchain for implementing tokens. (ERC: Ethereum Request for Comment, 20: the number that was assigned to this request.)
  - It defines a common list of rules that an Ethereum token has to implement, allowing developers to program how new tokens will function within the Ethereum ecosystem. These rules include how the tokens are transferred between addresses and how data within each token is accessed.
  - + 142,200 ERC-20 token contracts (as of November 19, 2018): EOS, Bancor, Qash, etc…

Existing blockchain applications, related structures and architectures

- **ERC-721: a class of unique tokens**
  - A free, open standard that describes how to build non-fungible or unique tokens on the Ethereum blockchain. While most tokens are fungible (every token is the same as every other token, i.e.ERC-20), ERC-721 tokens are all unique.
  - It defines a minimum interface a smart contract must implement to allow unique tokens to be managed, owned and traded.
- **ERC-725: Ethereum Identity Standard**
  - A proposed standard for blockchain-based identity which lives on the Ethereum blockchain.
  - It describes proxy smart contracts that can be controlled by multiple keys and other smart contracts, it can describe humans, groups, objects and machines.
  - Users should be able to own and manage their identity instead of ceding ownership of identity to centralized organizations.

Creating a currency from scratch

- Motivation
  - Distrust of financial institutions
  - Transaction costs
- Primary concerns
  - Transaction security
  - Double spends

Distrust of financial institutions

- Any noncash transaction requires a trusted third-party administrator—commonly a bank or financial service provider.
- The system forces participants to trust financial institutions that are not always trustworthy.

Transaction costs

- Traditional payments are revocable, even on irrevocable services.
- Financial institutions act as an arbitrator between counterparties in disputed claims.
- Arbitration costs are passed on to consumers.

Transaction security

- Two levels of verification
  - Source is legitimate
  - Coins are legitimate
- Public/private key verification ensures the legitimacy

Double spends

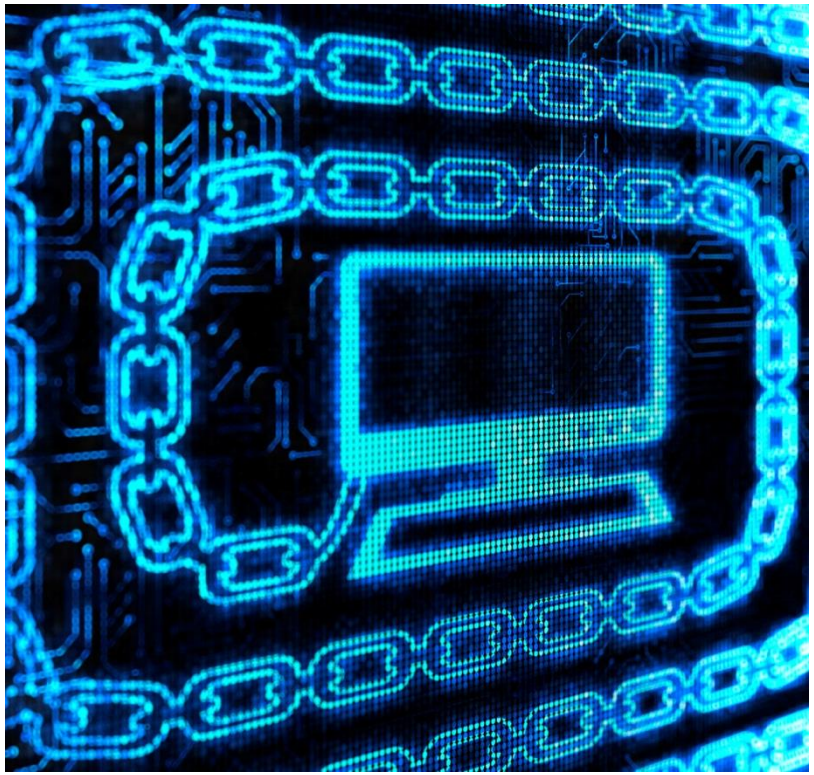
- If the money is just digital codes, why not copy and paste to make more money?
  - Timestamps
  - Hashes
  - Block chain

Double spends

- Timestamp
  - Each transaction is packaged and publically recorded in the order it was carried out.
- Hash
  - The time-stamped group of transactions are given a unique algorithmically derived number

Double spends

- Block chain
  - Transactions are recorded in a community-built record of all transactions that acts as a proof-of-work.
  - Computers connected to the network accept the longest chain as accurate.



Where do bitcoins come from?

- They’re mined, silly.
- High-powered computers solve complicated math problems.
- Each time a problem is solved, the finder is paid a bounty.

Mining bitcoins

- Miners solve complicated algorithms to find a solution called a hash.
- Finding a hash creates a block that is used to process transactions.
- Each new block is added to the block chain.

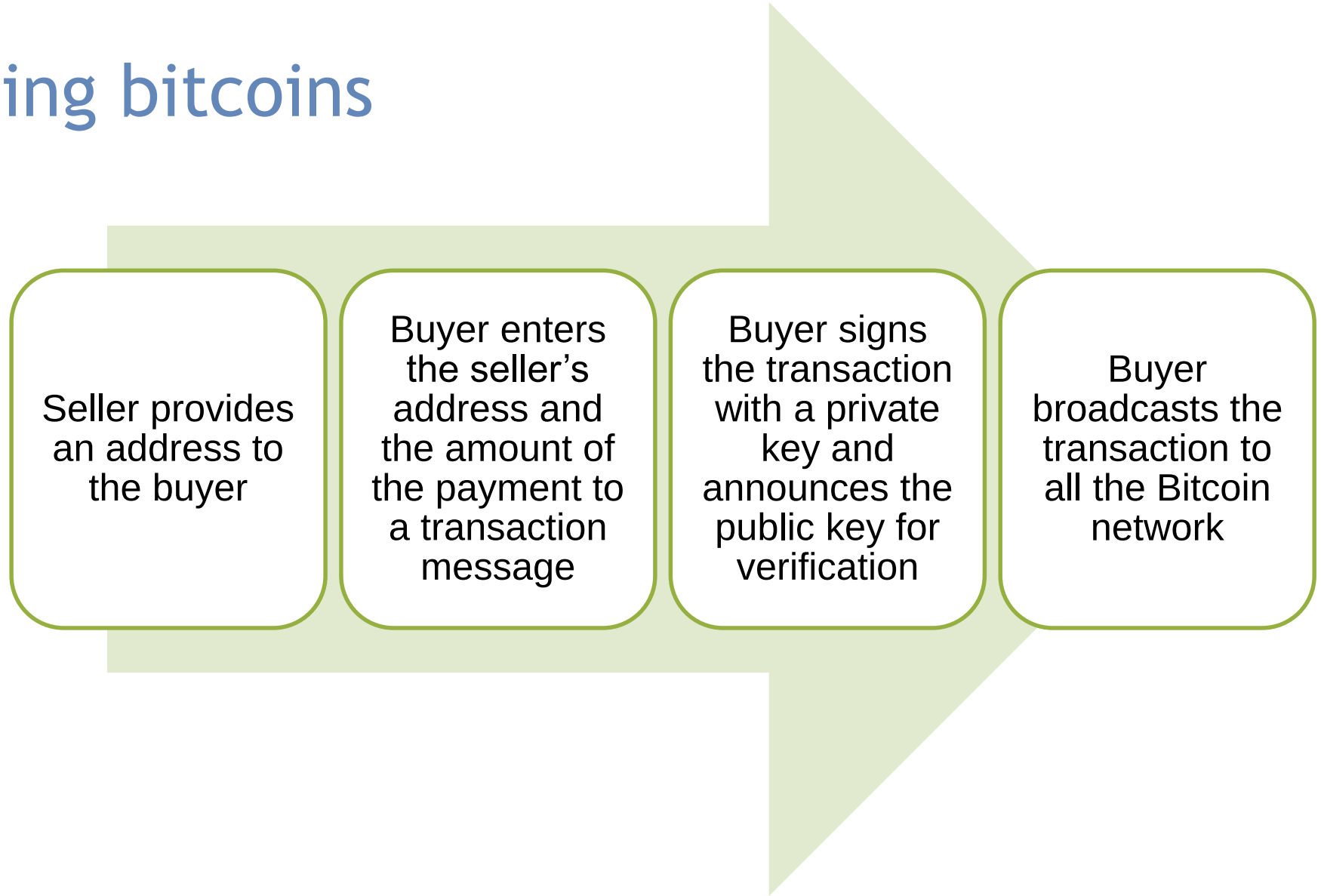
Mining bitcoins

- Until there are 21 million bitcoins, miners are paid for finding a hash in new coin.
- After 21 million, miners will charge transaction fees for creating a new block.
- The amount paid per hash goes down by half about every 4 years.

Owning bitcoins

- Users create accounts called wallets.
- Wallets are secured using passwords and contain the private keys used for transferring bitcoins.

Spending bitcoins



Bitcoin security

- Computers accept the longest block chain, which inhibits hacking.
  - Hackers would have to create a longer chain of fraudulent information faster than the combined effort of all other computers.
- Public/private cryptography means individual bitcoins are secured when not being transacted.

Reference

- The Bitcoin Standard: The Decentralized Alternative to Central Banking – Illustrated, April 24, 2018 by Saifedean Ammous
- The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- Blockchain Bubble or Revolution: The Future of Bitcoin, Blockchains, and Cryptocurrencies – June 12, 2019 by Neel Mehta (Author), Aditya Agashe (Author), Parth Detroja (Author)
- Cryptocurrency Investing For Dummies – March 6, 2019 by Kiana Danial
- Cryptocurrency Mining For Dummies– Illustrated, December 5, 2019 by Peter Kent
- Cryptocurrency Mining: A Complete Beginners Guide to Mining Cryptocurrencies, Including Bitcoin, Litecoin, Ethereum, Altcoin, Monero, and Others – February 21, 2018 by Crypto Tech Academy (Author)