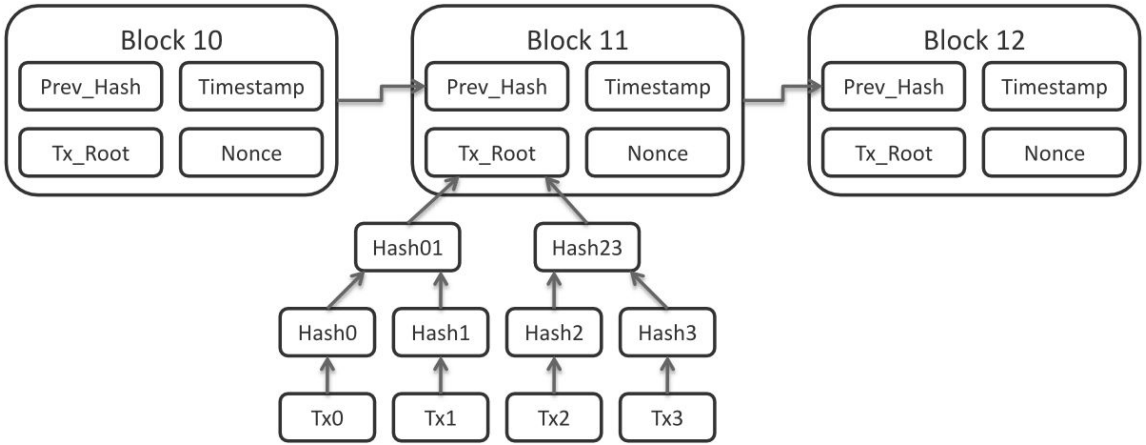
Overview on Blockchain and Cryptocurrencies

Dmytro Piatkivskyi

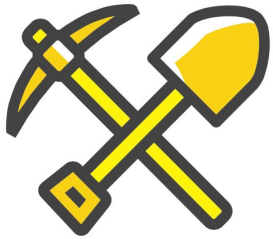
Blockchain

Is a **database** which is:

- De-centralised
- Hardened against tampering



Mining

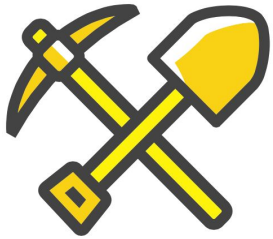


Block hash: 00000008a3a41b85b....

Number of 0s in front defines difficulty

Mining rate = Mining power / Difficulty

Mining



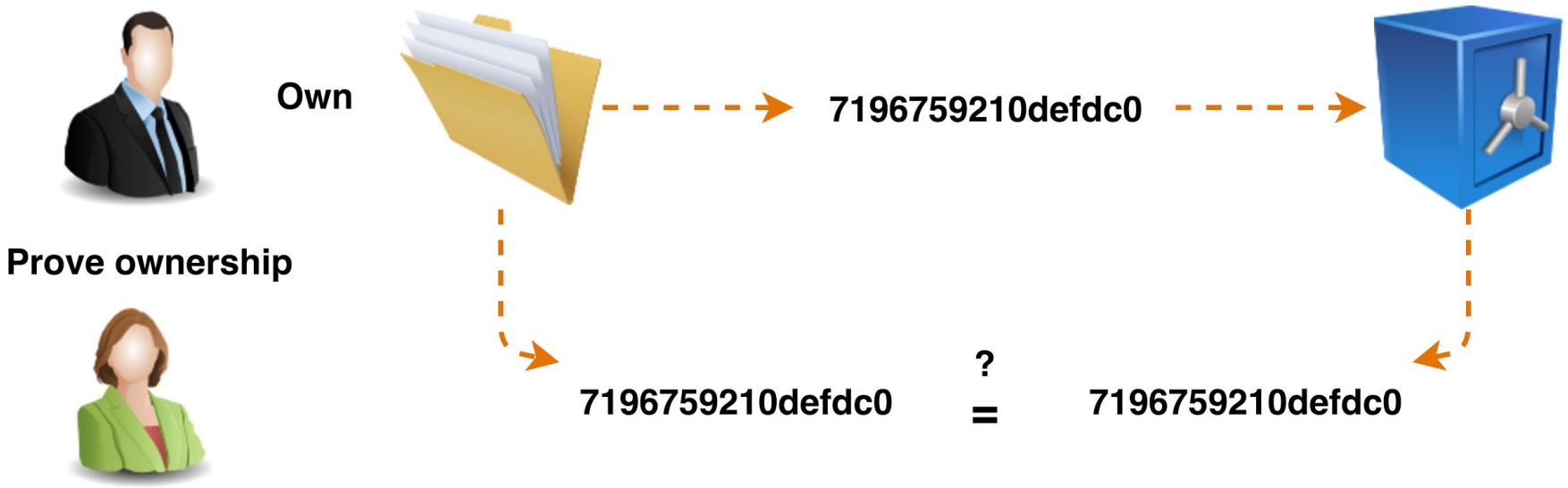
Everyone votes

For correctness and compliance

Blockchain is an enforcement platform with no regulation

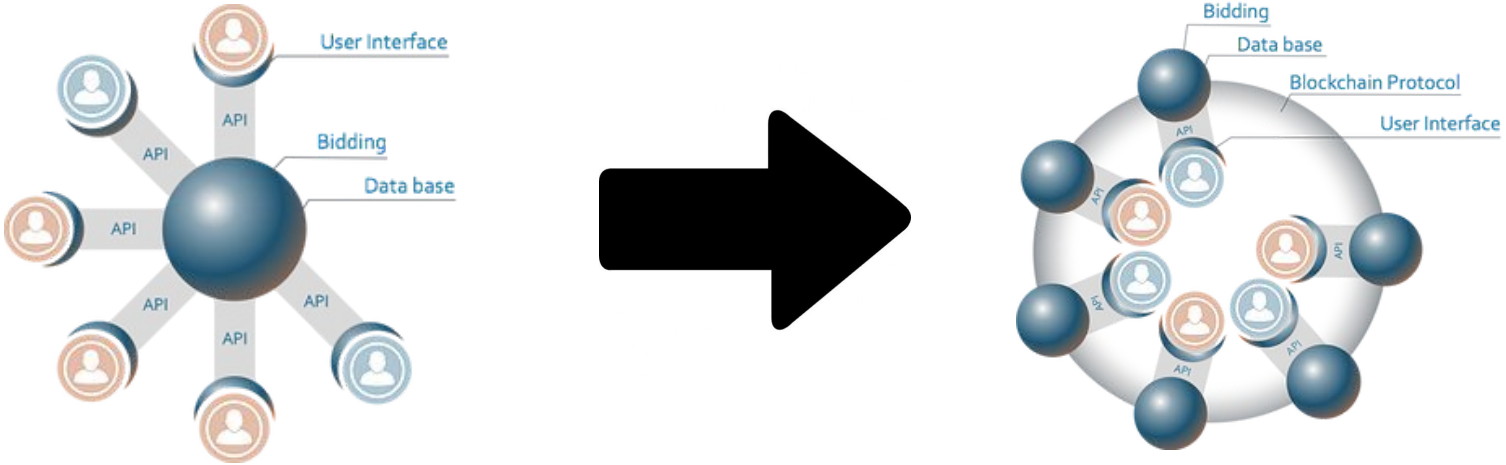
Eliminates the need of trusted third party

Proof of ownership



De-centralised e-auction 3.0

- No trusted party - no corruption
- Peer-to-peer interaction (peer is a service provider)
- Bids are encrypted before the decision is made
- An algorithm makes decisions

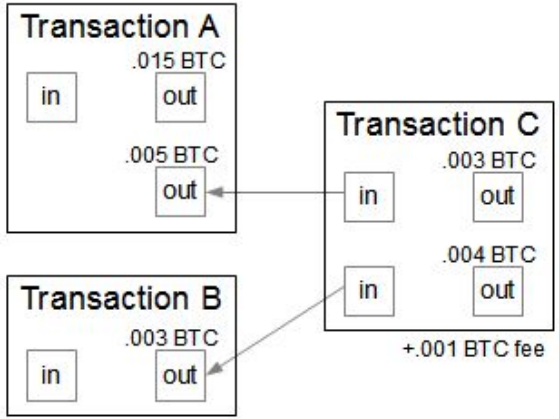


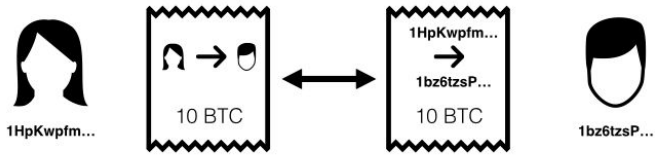
Bitcoin

- Fast money transfers
- No borders
- Very low fees
- Anonymity
- Non-regulated
- Build-in programming language => smart contract

Bitcoin scalability

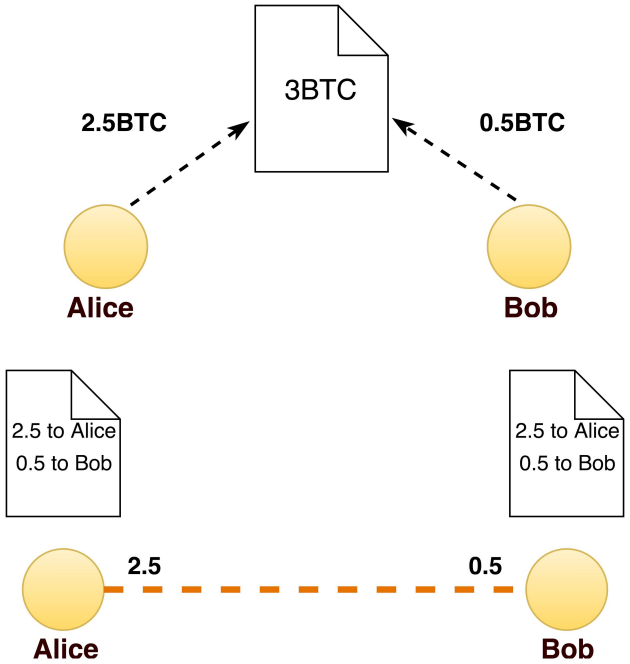
- Every transaction gets published on the blockchain
- Block size = 1Mb
- Block generation time = 10 minutes (on average)
- Throughput ≈ 7 transactions/second
- Visa peeks ≈ 47 000 transactions/second





Bidirectional channels

Channel opening



Lightning network transaction

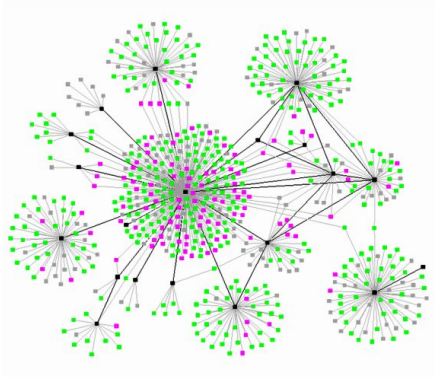
Lightning network

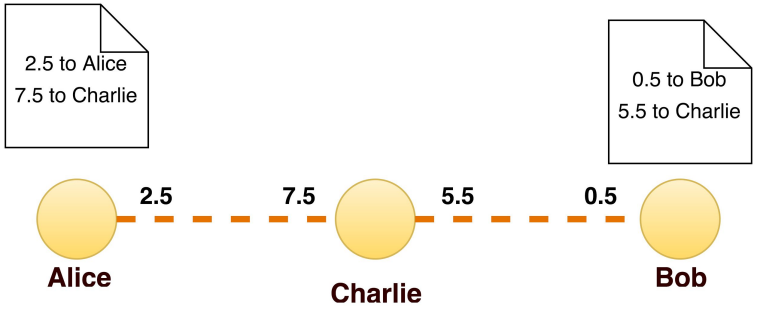
Pros:

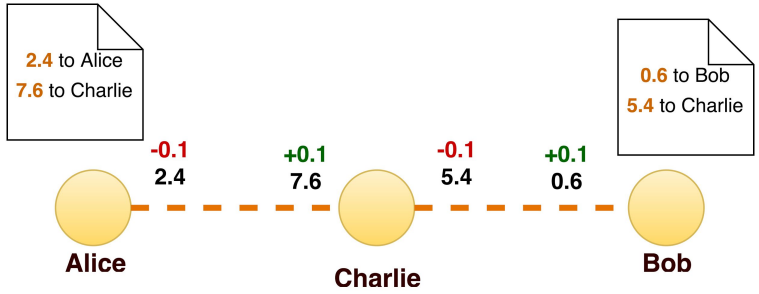
- Instantaneous payments
- Even lower fees
- Absolutely scalable
- Better anonymity

Cons:

- Money locking
- Centralisation







Anonymity of the off-chain transactions in Bitcoin

Points to consider:

- Blockchain data
- Payment processing hubs data

Main research method - Lightning network simulation:

- Topology
- Dataset
- Analysis

Thank you!