



BLOCKCHAIN PRINCIPALS

CA Expo Prague 2018

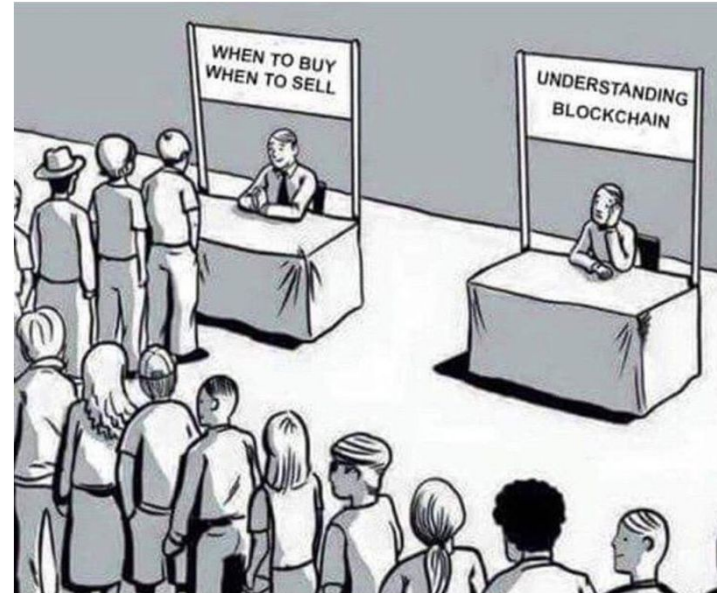
Lukáš KOLÍSKO

Principal Software Engineer @ CA Technologies
Blockchain R&D

24th April 2018



YOU MIGHT HAVE HEARD ABOUT **BLOCKCHAIN**



History



- **Satoshi Nakamoto** published a white-paper called **”Bitcoin: A Peer to Peer Electronic Cash System.”**
- Motivated by the 2008 global financial crisis, he proposed the **concept of a secure, decentralized system that solves the “double spend” problem of digital currency.**
- This solution later served as the **foundation for Bitcoin.**

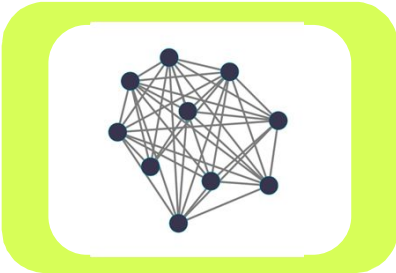
... and 10 years later



BLOCKCHAIN COMPONENTS



**DISTRIBUTED
LEDGER**



**BLOCKCHAIN
NETWORK**



**SMART
CONTRACTS**

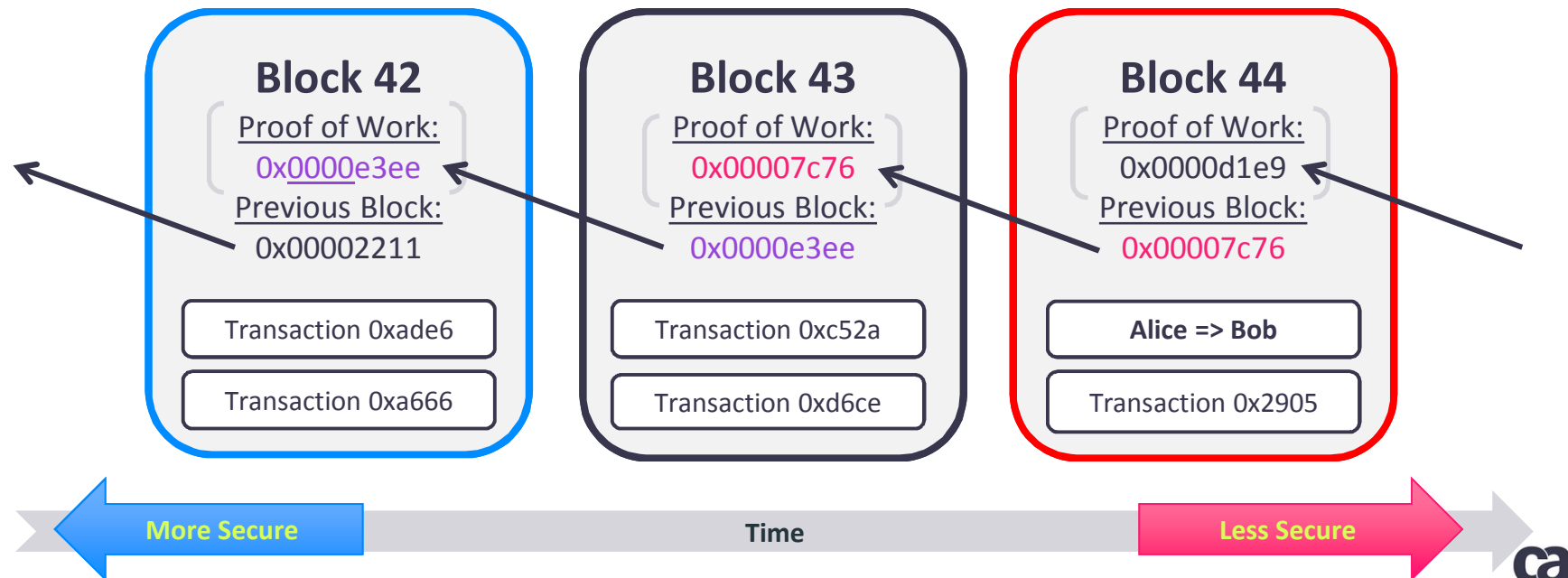


CONSENSUS

Distributed Ledger



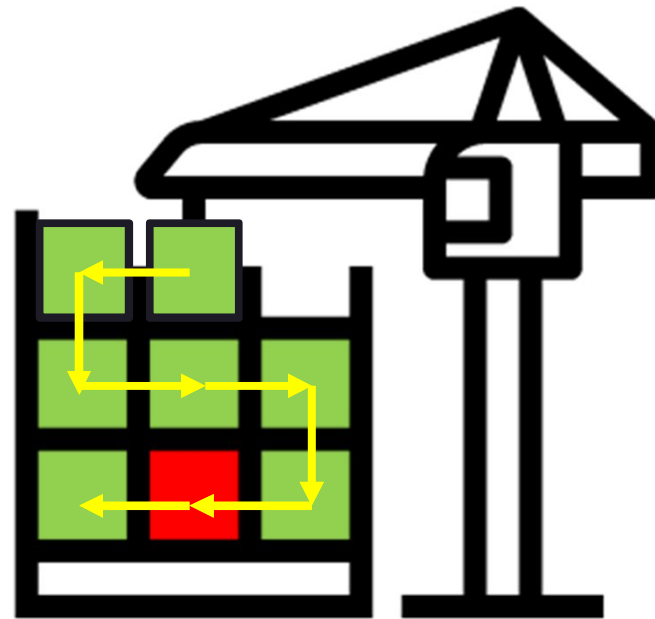
A ledger is a type of **database** that is **consensually shared and synchronized** among members of a network.



Distributed Ledger Immutability

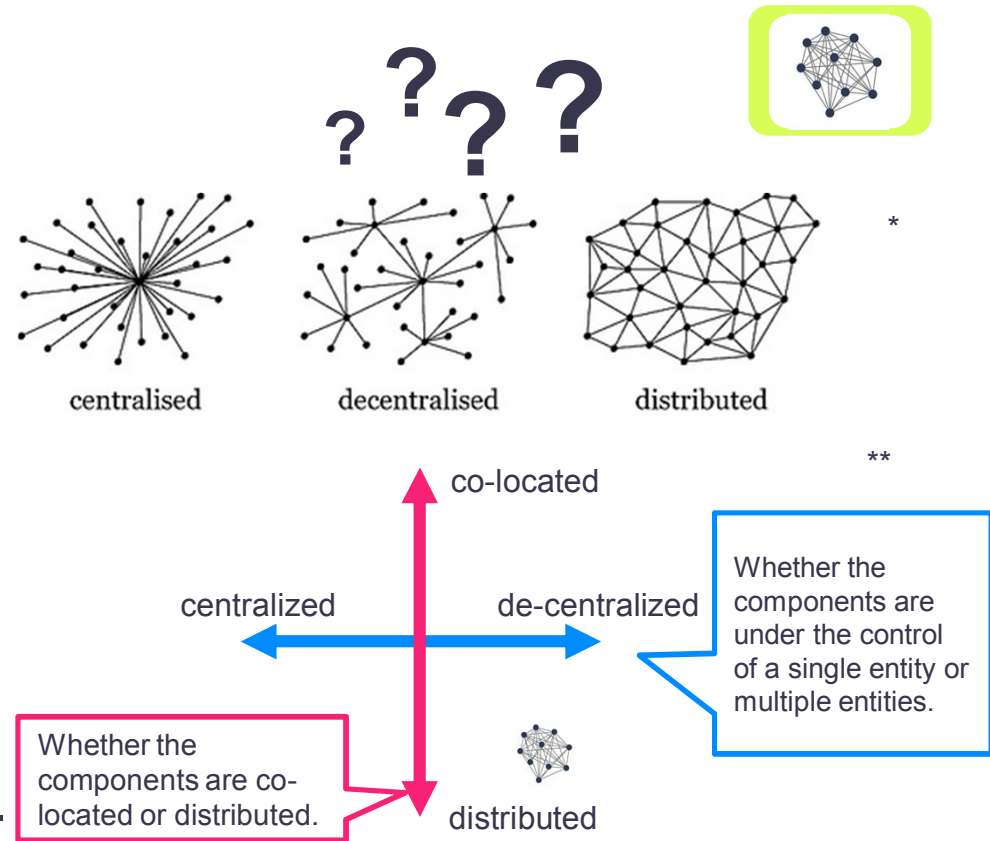


- **Proof-of-Work** ensures that an attacker cannot change transactions without **overwhelming the actual and previous computational power used to hash the blockchain** until the moment (block) attacker decided to attack the chain on.



Blockchain Network

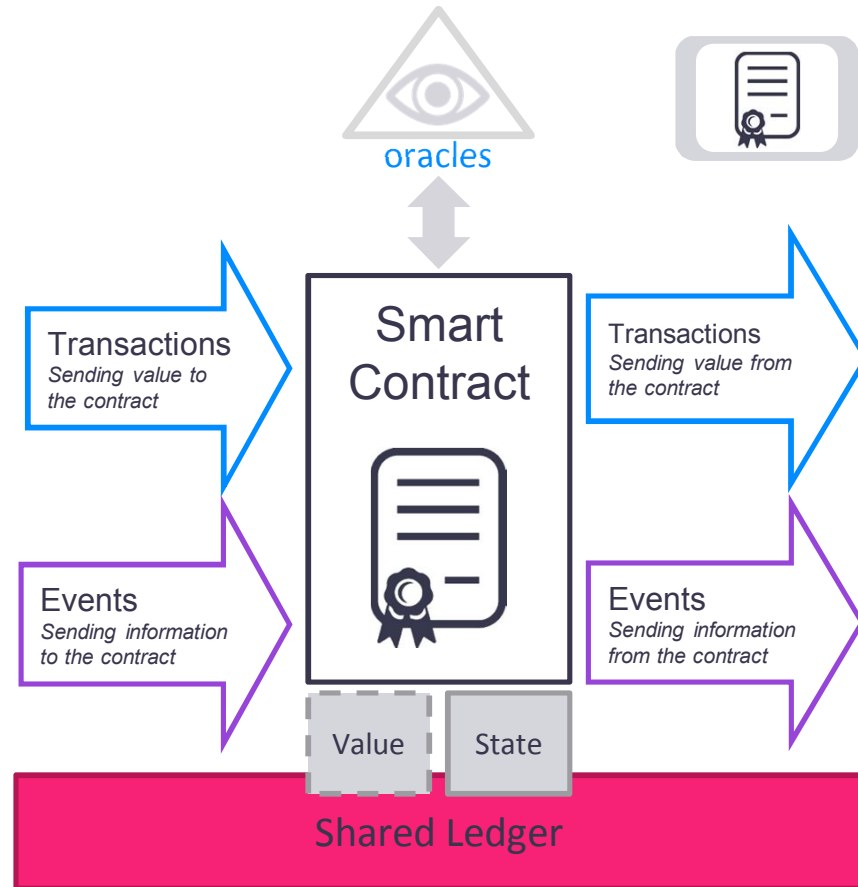
- A **distributed decentralized network** consisting of computers known as nodes
- Nodes hold a copy of the digital ledger
- Nodes can have different roles in the network
 - Full Node, Listening Node, Miner Node, Validator Node,...



source: * Baran (1962) On Distributed Communication Networks, ** Windley <https://bit.ly/2pFCII9>

Smart Contracts

- “Digital counterpart to legal contracts”
- Event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger.
- Bitcoin Script, Solidity, Go, Java,...

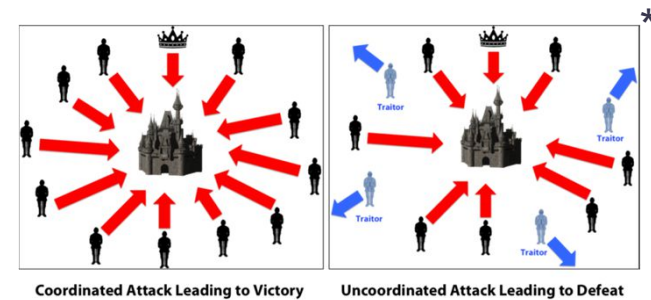


source: <https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/>

Consensus



- Network of blockchain nodes has to collectively agree on contents of the ledger => **Agreement on global state**
- Provides a **guaranteed ordering** of transactions and **validates the block of transactions**.
- Byzantine Generals Problem
- PoW, PoS, DPoS, RBFT, PoET,...

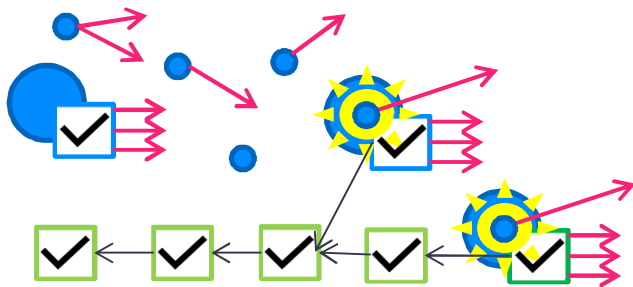


source: *) <https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c>

Consensus Types

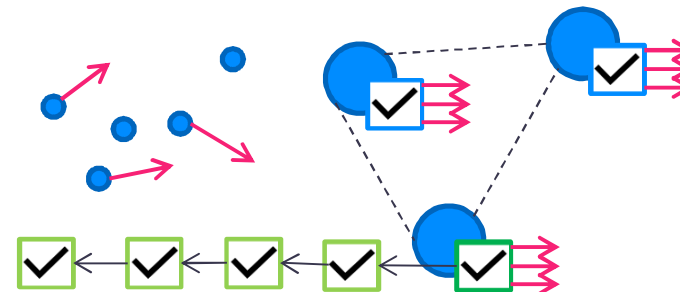
Lottery Based

- Winner of the lottery proposes a block and transmits it to the rest of the network for validation. Lead to forking when two “winners” propose a block.
- Scalability x Longer Time To Finality
- Public Blockchains
- Proof of Work, Proof of Elapsed Time, Proof of Stake



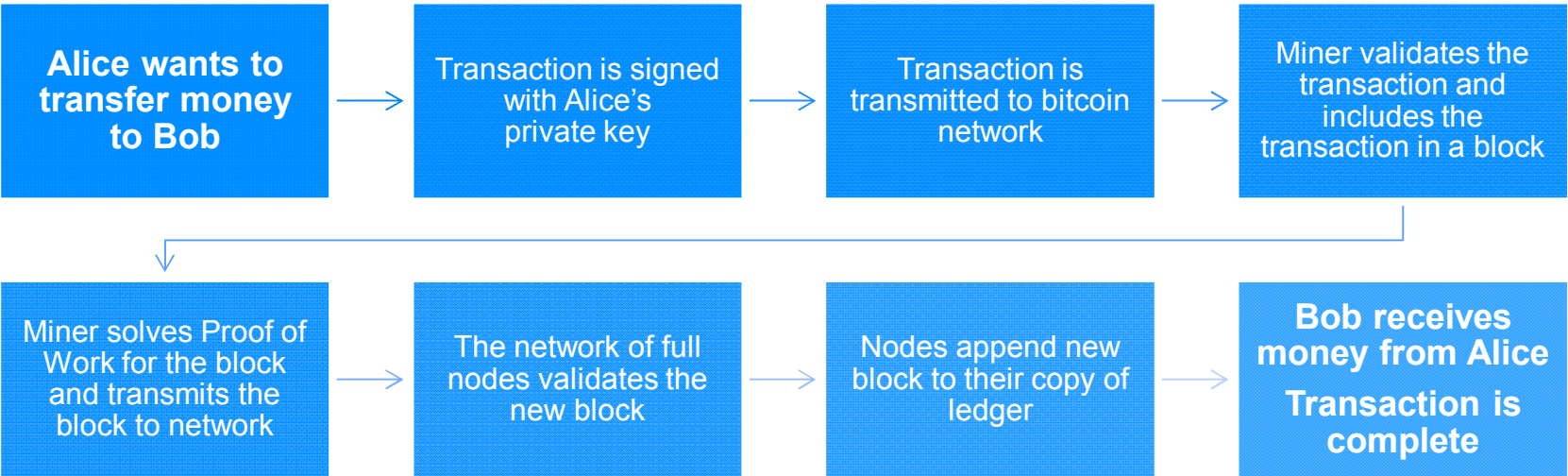
Voting Based

- When a majority of nodes validates a transaction or block, consensus exists and finality occurs.
- Low Latency Finality x Scalability-Speed
- Private Permissioned Blockchains
- Paxos, Byzantine Fault Tolerance Algorithms - Redundant Byzantine Fault Tolerance, BFT-SMaRt



source: <https://www.slideshare.net/ITU/blockchain-cryptography-and-consensus>

How Bitcoin Blockchain Works



Value of Blockchain Technology

Concepts of blockchain technology allow removing the need for central sources of truth via distributing the trust to the blockchain network using formally proven principles.



Thank You.



Lukáš KOLÍSKO
Principal Software Engineer
Lukas.Kolisko@Ca.Com



BACKUP SLIDES



Public, Private and Permissioned Blockchains



 Anonymity of the validators



Permissionless Public

Proof of Work	
Scalability	Good
Speed	Poor
Finality	Prob.Poor
Token	Needed

Proof of Stake	
Scalability	Good
Speed	Good
Finality	Prob.Good
Token	Needed




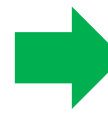
Permissionless
Permissioned
Public

Permissionless Public or Consortium

Federated BFT	
Scalability	Good
Speed	Good
Finality	Immediate
Token	No Need

BFT	
Scalability	Medium
Speed	Good
Finality	Immediate
Token	No Need

Permissioned
Private


 Trust to a validator
 

sources: <https://bit.ly/2GlecNV>, <https://bit.ly/2lb7oDn>