Consensus Algorithms

Thomas Sermpinis - AUTh

Consensus

- Agreement among a number of processes (or agents) for a single data value.
- Some of the processes may fail
  - Fundamental problem in distributed computing
- Consensus protocols must be fault tolerant or resilient
- Most cryptocurrencies use consensus algorithms
- None of them is perfect
- Each of them has its strengths and its characteristics
- Used in order to prevent double spending

When several nodes (usually most nodes on the network) all have the same blocks in their locally-validated best blockchain.

Proof-of-Work (PoW)

Proof-of-Work (PoW)

- First blockchain consensus algorithm
- Miners solve mathematical problems in order to create blocks
- “The longest chain wins”
- Most miners work on the same chain - this chain will be the longest and most trustworthy
- Massive power consumption - power “hungry” and expensive hardware as a prerequisite.

Advantages:

- It works!!!!

Disadvantages:

- Slow
- Inefficient solution (Huge energy needs)

Implementations; Bitcoin, Ethereum (for now), Litecoin and others

Proof-of-Stake (PoS)

- No miners, just *minters*
- **“Betting”** their currency units on the block that will be valid
- Forks are solved by voting to support a chain by the minters using their currency
- If the chain that a minter has voted is the wrong one, she will lose her “stake” in the correct chain
- Forks may be more common with PoS, which may harm the credibility of the currency

Advantages:

- Energy efficient
- More expensive to attack (in some cases)

Disadvantages:

- *“Nothing at Stake”*

Implementations; Ethereum (soon), Decred, Peercoin

Delegated Proof-of-Stake (DPoS)

- Vote to elect delegates that will do the validation on their behalf
- The delegates are shuffled periodically
- Designated time slots for each delegate
- In case of missed blocks, or invalid transaction publishing, delegates get replaced by voting new ones.
- Miners collaborate instead of competing

Advantages:

- Cheap transactions
- Energy efficient

Disadvantages:

- Partially Centralized

Implementations; EOS, Steemit and others

Proof-of-Authority (PoA)

- Centralized
- Validation by network approved accounts
  - Much like “admins” of a system
- The authority that shares the correct blockchain with other nodes in the network
- Optimized for private networks
- High performance
- Not suitable for public blockchains

Advantages:

- High performance
- Scalable

Disadvantages:

- Centralized

Implementations; Ethereum Kovan testnet, POA.Network

Proof-of-Weight (PoWeight)

- Based on Algorand consensus model
- Similar to PoS but based on other weights instead of percentage of currency units
- Filecoin and Proof-of-Spacetime as an example
    - Weighted on how much IPFS data you are storing
- Proof-of-Reputation and others

Advantages:

- High customizability
- Scalable

Disadvantages:

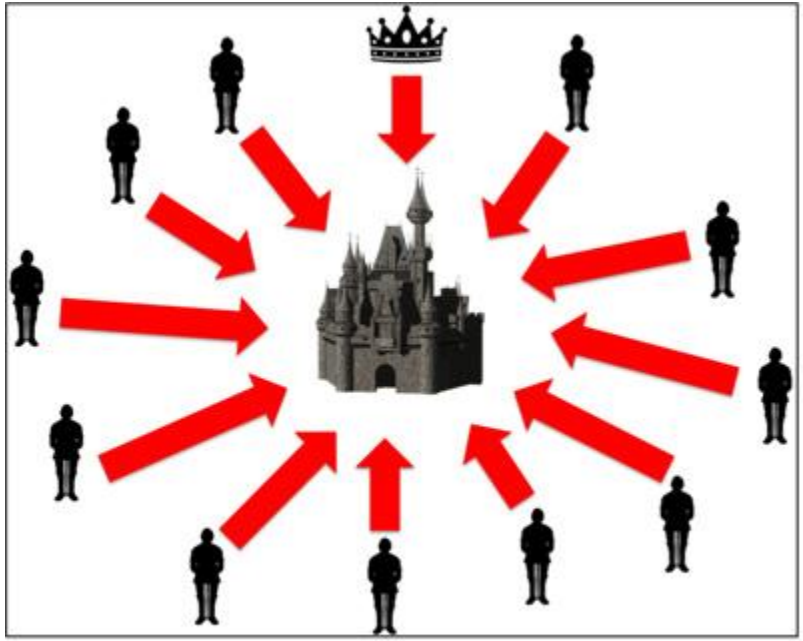
- Challenging incentivization

Implementations; Filecoin, Chia and others

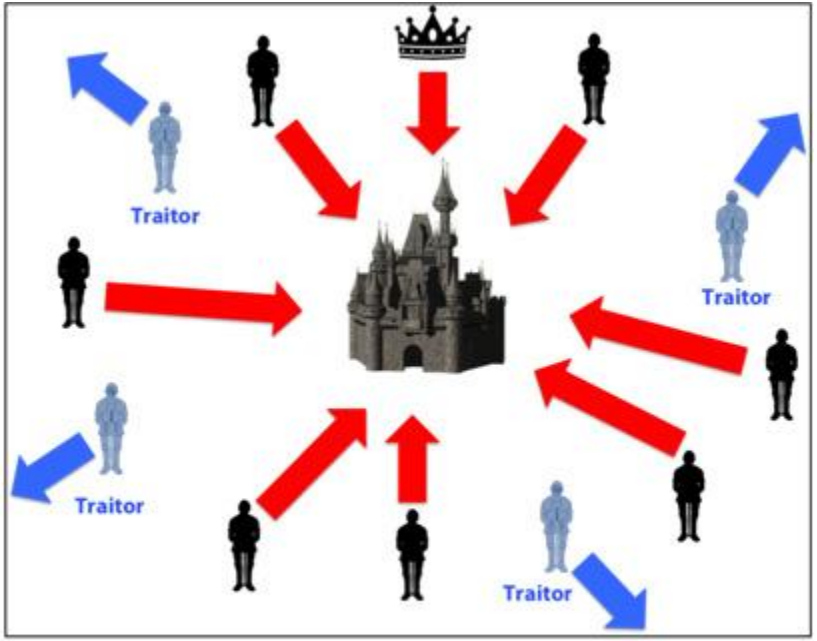
Byzantine Fault Tolerance (BFT)

Based on “Byzantine generals” problem

Byzantine Fault Tolerance (BFT)



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

Practical Byzantine Fault Tolerance (pBFT)

- Practical Byzantine state machine replication
- Tolerates Byzantine faults (malicious nodes) by assuming that there are independent node failures and manipulated messages propagated by specific, independent nodes.
- Works in asynchronous systems
- One node is the primary node - leader
- All other nodes (backup nodes) are ordered in a sequence

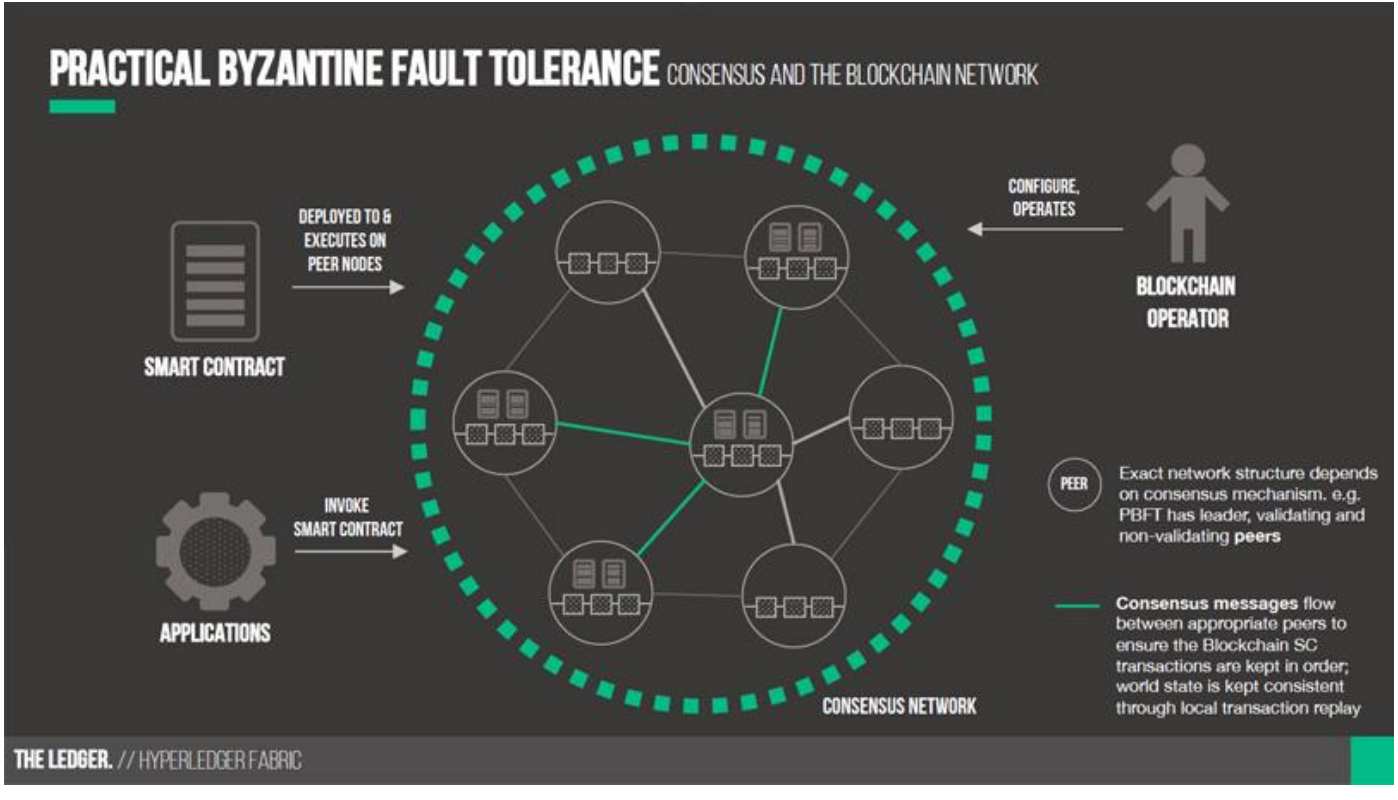
Advantages

- High transaction throughput (Considering small networks)

Disadvantages

- Centralized / Permissioned **????**

Practical Byzantine Fault Tolerance (pBFT)



Federated Byzantine Agreement (FBA)

- Nodes does not have to be known and verified ahead of time
- Membership is open
- Nodes choose whom they trust
- System-wide quorums emerge from decisions made by individual nodes
    - Number of nodes required to reach agreement within a system
    - “Quorum slices” - subset of quorum, which can convince other nodes to agree
- In Ripple the generals (validators) are pre-selected by the Ripple foundation.
- In Stellar, anyone can be a validator so you choose which validators to trust.

Advantages

- Open Membership
- Decentralized

Byzantine Fault Tolerance (BFT)

Popular Implementations:

- Hyperledger (TODO) , Stellar, Dispatch, and Ripple

Advantages

- High throughput, low cost

Disadvantages

- Semi-trusted

Directed Acyclic Graphs (DAGs)

- No use of blockchain structure
- Mostly asynchronous
- Theoretically infinite transactions/second
- DAGs resembles a flowchart with all points headed in one direction
- Similarity with file directory structure
  - Folders, subfolders, etc
- Tree-like

Advantages:

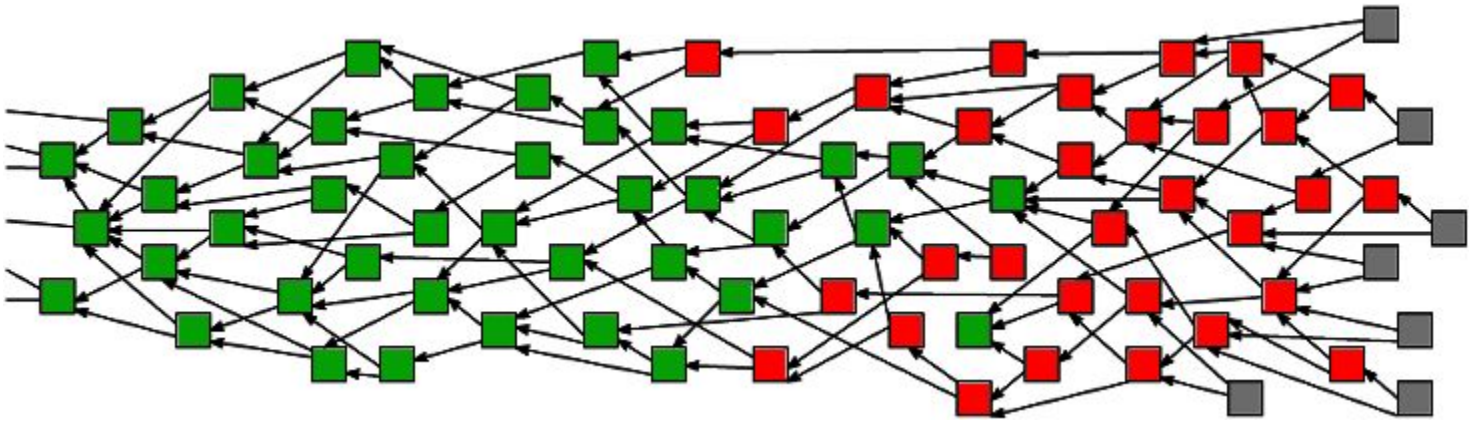
- Network scalability
- Low cost

Disadvantages:

- Depends on implementation

Implementations; Iota, Hashgraph, Raiblocks/Nano

Directed Acyclic Graphs (DAGs)



IOTA and DAG (or Tangle?)

- Assign of the same exact duties to every member
- All users are both issuers and validators
- Small amount of PoW to prevent spam
- Everyone is participating in the consensus of the network
- The more the people, the faster the network becomes
- No need for fees to “miners”
- Microtransactions execution

Advantages

- Small fees, High scalability

Disadvantages

- Proprietary cryptographic algorithm, Central point of failure due to temporary centralized element (Coordinator node - “Coo”)

Questions?

Email: sermpinis@csd.auth.gr
Web: https://cr0wsplace.com
LinkedIn: https://www.linkedin.com/in/thomas-sermpinis-0473a4b0/
Twitter: @serbinhio
YouTube: https://www.youtube.com/user/Cr0wsPlace