72 Consensus from the Blockchain Consensus Encyclopedia

Consensus algorithms enable network participants to agree on the contents of a blockchain in a distributed and trust-less manner.

version 2019.3
tokens-economy.com
(c) 2019 - Cédric Walter

Attacks

- Denial of Service: overloading nodes with lots of transactions.
- 51% Attack: controlling more than 50% of nodes, can create fork longer than the main chain.
- Sybil attacks: when one node tries to represent multiple identities.
- Cryptographic attacks that break the underlying cryptography (Quantum).

The consensus algorithm plays a crucial role in maintaining the safety and efficiency of blockchain. Using the right algorithm may bring a significant increase to the performance of blockchain application.

Each consensus algorithm has its own application scenario. There is no absolute good or bad. The choice of which consensus to use for implementing the blockchain depends on the type of network and data.

For a transaction to be valid on most cryptocurrency networks, the transaction needs to collect a certain number of confirmations (often equals to an inclusion in a block of a blockchain) from the network.

The CAP Theorem

States that in case of a partition, a distributed system can only preserve either consistency or availability.

CONSISTENCY
All clients see current data regardless of update/delete

AVAILABILITY
system continue to operate even with node failures

CA
N/A
CP
AP

PARTITION TOLERANCE
the system continues to operate despite network failures

The trilemma

claims that blockchain systems can only at most have two of the following three properties

Decentralization

defined as the system being able to run in a scenario where each participant only has access to O(c) resources,

Scalability

defined as being able to process O(n) > O(c) transactions

Security

defined as being secure against attackers with up to O(n) resources

Proof of Stake

- Hybrid PBFT/Aurand — *Polkadot*
- Variable Delayed Proof Of Stake (vDPOS) — *CryptoCircuits*
- Proof of Stake Velocity — *Reddcoin*
- Proof of stake (PoS) — *Ethereum, Nxt, Waves, Tezos*
- Delegated proof-of-stake (DPoS) — *Steemit, EOS, Bitshares*
- Magi's proof-of-stake (mPoS) — *Magi*
- Leased Proof-of-Stake (LPoS) — *Nxt, Waves*
- Proof-of-Stake-Time (PoST) — *PostCoin, Vericoin*
- Leasing Proof of Stake (PoS/LPoS) — *Nxt, Waves*
- Proof of stake Boo — *Shield*
- Casper (CBC) — *Ethereum 3.0*
- High Interest Proof of Stake (HiPoS) — *EdgeCoin, GravityBits*
- Tiered Proof Of Stake (TPOS) — *XSN*
- Casper (FFG) — *Ethereum 2.0*

DAG

- Direct Acyclic Graph Tangle (DAG) — *Iota*
- Hashgraph — *Hashgraph*
- Block-lattice - Directed Acyclic Graphs (DAGs) — *Nano*

BFT-based

- Practical Byzantine Fault Tolerance — *Hyperledger Fabric*
- Federated Byzantine Agreement — *Stellar, Ripple*
- Delegated Byzantine Fault Tolerance — *neo, byteBall*
- Byzantine Fault Tolerance (BFT) — *Dispath, Ripple*
- asynchronous BFT protocol — *HoneyBadgerBFT*
- Modified Federated Byzantine Agreement (mFBA) — *BOS*
- Ouroboros — *Cardano*

Hybrid models

- Proof-of-Activity — *Decred, Espers, Coinbureau*
- Proof-of-authority (PoA) — *Ethereum on azure*
- Proof Of Activity — *Mix PoW+PoS*
- Proof Of Care (PoC) — *Tamaguchi*
- Limited Confidence Proof-of-Activity (LCPoA) — *izzz.io, BitCoen*
- High Interest Proof of Stake — *EdgeCoin*
- Proof of Processed Payments (PoPP)

Proof of Burn

- Proof of Processed Payments (PoPP) — *BOS*
- Proof of Burn (PoB) — *SlimCoin, TGCoin*
- Proof of Time — *Chronologic*
- Proof of Disintegration (PoD) — *B3Coin*

Proof of Work

- Proof of Meaningful Work (PoMW) — *vrenelium*
- Semi-Synchronous Proof of Work (SSPoW) — *Purple*
- Delayed Proof of Work (dPoW) — *Komodo*
- Proof-of-work time (PoWT) — *Vericoin, Verium*
- Proof of Edit Distance — *Block Collider*
- ePoW: equitable chance and energy-saving. Distance — *Hdac*
- Proof of Work (PoW) — *Bitcoin, Ethereum*

Proof of Capacity/Space

- Proof of Process — *Stratum*
- Proof of capacity (PoC) — *Spacemint, permacoin, burstcoin*
- Proof-of-Signature (PoSign) — *XBY*
- Proof of Retrievability (POR) — *Permacoin*
- Proof of Location — *Foam, Platin*
- Proof of Reputation (PoR) — *Gochain*
- Proof-of-Proof (PoP) — *Veriblock*
- Proof of History — *Solana*
- Proof of Existence — *HeroNode, Dragobchain,Poex.io*
- Proof of Research (DPoR) — *Gridcoin*
- Proof-of-Weight (PoWeight) — *Algorand, Filecoin, Chia*
- Proof of Zero (PoZ) — *Zcrypt*
- Proof of Importance — *NEM*
- Proof of Care (PoC) — *Quantstamp, Tomocoin*
- Raft — *Quorum*
- Proof of Value (PoV) — *LTBCoin*
- Proof-of-Presence (PoP) — *HEAT*
- Proof of Believability — *IOST*
- Proof of Ownership
- Proof of Quality (PoQ) — *LTBCoin*
- Proof-of-space (PoC) — *Spacemint, chia, burstcoin*

Legends

Stakeholders are those having coins or smart contracts on the blockchain. Only they can participate. Those with high stakes are chosen to validate new blocks.

Each participant on the network can participate in the block generation. In order to confirm the transaction and enter a block into the blockchain, a miner has to provide an answer, or proof, to a specific computational challenge.

Proof-of-space, also called Proof-of-capacity, is a means of showing that one has a legitimate interest in a service by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.

Participants should show proof that they burned someething (coin, time,...) - e.g for a coin that they are sent to a verifiably unspendable address.

Most of the time a combination of existing consensus algorithm, e.g PoW+PoS but not always...

Byzantine Fault Tolerance is the characteristic which defines a system that tolerates the class of failures that belong to the Byzantine Generals' Problem. ... and work as long as the number of traitors do not exceed one third of the generals.

In order to send a new transaction, you need to validate two previous transactions you're received. The two-for-one, pay-it-forward consensus strengthens the validity of transactions the more transactions are added to the Tangle.