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



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

N/A

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

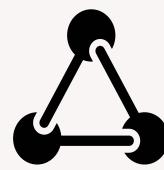
AVAILABILITY

system continue

with node failures

to operate even

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



Security **Scalability**

defined as being secure defined as being able to against attackers with process O(n) > O(c)up to O(n) resources transactions

Hybrid PBFT/Aurand Polkadot

Proof of stake (PoS) thereum, Nxt, Waves, Tezos

Delegated

proof-of-stake (DPoS) Steemit, EOS, Bitshares

Direct Acyclic

Graph Tangle (DAG)

DAG

asynchronous

BFT protocol

(mFBA) _{BOS}

High Interest

Proof of Stake

EdgeCoin

HoneyBadgerBFT

Modified Federated

Byzantine Agreement

Hybrid models

Block-lattice - Directed

Acyclic Graphs (DAGs)

Hashgraph

Practical Byzantine

Fault Tolerance

Byzantine Fault

Tolerance (BFT)

Dispath, Ripple

Ouroboros

Cardano

Proof-of-Activity

Decred, Espers, Coinbureau

Proof Of Care (PoC)

Hyperledger Fabric

Federated Byzantine

Agreement Stellar, Ripple

Delegated

Byzantine

Fault Tolerance neo, byteBall

BFT-based

Hashgraph

Proof-of-Stake-Time (PoST) PostCoin, Vericoin

Proof of stake Boo Shield

Casper (CBC) Ethereum 3.0 **High Interest Proof**

of Stake (HiPoS) EdgeCoin, GravityBits Distance

Tiered Proof Of Stake (TPOS)

Casper (FFG) Ethereum 2.0

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

Proof Of Activity

Proof of Processed Payments (PoPP)

Proof-of-Activity (LCPoA) izzz.io, BitCoen

Proof of Burn

Proof of Time

(PoD)

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



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 vou're received. The two-for-one, pay-it-forward consensus strengthens the validity of transactions the more transactions are added to the Tangle.

Magi's proof-of-stake (mPoS) Magi

Proof of Stake

Leased Proof-of-Stake (LPoS) Nxt. Waves

Leasing Proof of Stake (PoS/LPoS) Nxt, Waves

Proof-of-work time (PoWT)

ePoW: equitable chance and energy-saving.

Variable Delayed

Proof Of Stake (vDPOS)

Proof of Stake

VelocityReddcoin

CryptoCircuits

Proof of Edit Distance

Block Collider

Delayed Proof of

Work (dPoW)

Proof of Work (PoW) Proof of Work

Proof of Process

Proof of Meaningful

Work (PoMW)

Semi-Synchronous

Proof of Work (SSPoW)

Proof of Retrievability (POR) Proof-of-Signature (PoSign)

Proof of Location

Proof of Reputation (PoR)

Proof-of-Proof (PoP) Veriblock

Proof of History

Proof of Existence HeroNode, Dragobchain,Poex.io

Proof of capacity (PoC)

Permacoin

Spacemint, permacoin, burstcoin

Proof of Research (DPoR)

Gridcoin

Proof-of-Weight (PoWeight) Algorand, Filecoin, Chia

Proof of Zero (PoZ) Zcrypt

Proof of Importance Proof of

Capacity/Space

Proof of Care (PoC) Quantstamp, Tomocoin

Raft

Proof of Value (PoV) **LTBCoin**

Proof-of-Presence (PoP)

Proof of Believability

Proof of Ownership

Proof of Quality (PoQ)

Proof-of-space (PoC) Spacemint, chia, burstcoin

Proof-of-authority (PoA) Ethereum on azure

Proof of Processed

Payments (PoPP)

Mix PoW+PoS

Limited Confidence

Proof of Burn (PoB) SlimCoin, TGCoir

Chronologic

Proof of Disintegration