Blockchain Council™

Types of Consensus Algorithms

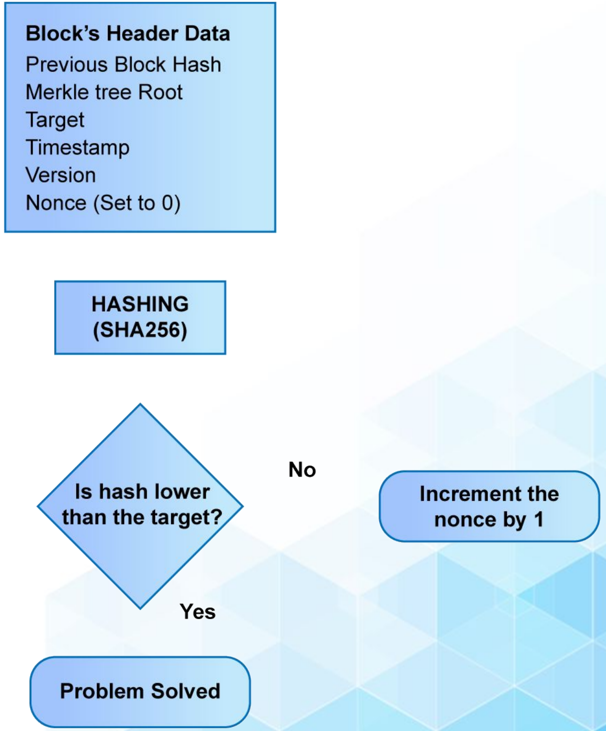
Proof-of-Work (PoW)

In Proof-of-Work, miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm.

Miner did spend a lot of time and resources to solve the problem.

When a block is 'solved’, the transactions contained are considered Confirmed.

Miners receive a reward when they solve the complex mathematical problem.



Proof-of-Work (PoW)

Transaction is validated after mining.

Valid data includes:

- Block header hash is less than the target.
- Block size is within acceptable limits.
- Block timestamp is less than two hours in the future.
- The first transaction is a coinbase transaction.
- The coinbase transaction has a valid reward.
- Valid transactions within the blocks.
- If the block is valid, the other miners will update their own copy of the blockchain with the new block.

Proof-of-Stake (PoS)

Proof-of-Stake is a different way to validate transactions and achieve distributed consensus.

Unlike the Proof-of-Work, Proof-of-Stake chooses the creator of a new block in a deterministic way, depending on its wealth, also defined as stake.

No block reward.

Also, all the digital currencies are previously created in the beginning, and their number never changes that is PoS system; there is no block reward.

Miners take the transaction fees, that is why PoS system miners are called forgers, instead.

Delegated-Proof-of-Stake (DPoS)

People in a particular cryptocurrency community vote for witnesses to secure their computer network.

People's vote strength is determined by how many tokens they hold.

People who have more tokens will influence the network more than people who have very few tokens.

If a witness starts acting strange or stops doing a quality job securing the network, people in the community can remove their votes, essentially firing the bad actor.

Delegates are elected in a manner similar to witnesses.

Proof-of-Importance (PoI)

In proof-of-importance, every account on the blockchain is assigned an importance score.

The score will influence how individual users can “harvest” the blockchain. One could say harvesting on the blockchain is almost the same as what miners do on the Bitcoin blockchain.

The objective is to add people’s transactions to the blockchain, in exchange for a small financial reward.

To be eligible for the “importance calculation,” users need to have at least some currency in their balance.

Proof-of-Elapsed Time (PoET)

Proof-of-Elapsed-Time (PoET) is designed to improve proof-of-work consensus and provide an alternative for permissioned blockchain networks.

It removes the need for the mining-intensive process and replaces with a randomized timer system for network participants.

PoET consensus can be broken down into two phases:

- Joining the network and verification
- Elapsed time, randomized lottery selection process.

Practical Byzantine Fault Tolerance (pBFT)

In the late 1990s, Practical Byzantine Fault Tolerance (pBFT) consensus algorithm was developed by Barbara Liskov and Miguel Castro.

pBFT protects against Byzantine faults and looks for optimization of aspects of Byzantine Fault Tolerance.

In pBFT, each 'general' manages an internal state which is an ongoing information status.

A consensus decision is made based on the total number of decisions submitted by all the generals.

pBFT was designed to operate efficiently in asynchronous (no upper bound on when response to request is received) systems.

It forces a low overhead on the performance of the replicated service.

Delegated Byzantine Fault Tolerance (dBFT)

Delegated Byzantine Fault Tolerance or dBFT is a consensus mechanism introduced by a cryptocurrency called NEO.

dBFT method is closer to PoS rather than PoW, by utilizing a voting system to choose delegates and speaker.

Citizens that are NEO tokens holders or ordinary nodes, Delegates are the bookkeeping nodes with specific requirements, and Speaker is the randomly chosen delegates.

The dBFT 's voting mechanism provides for large-scale participation, close to the consensus of the Delegated Proof-of-Stake. This means that by a referendum, the holder of a NEO token will help a particular 'bookkeeper'.

Absolute finality is one of the strongest points of using the dBFT mechanism. A block can not be bifurcated until final validation, so the transaction cannot be revoked or rolled back.

Simplified Byzantine Fault Tolerance (sBFT)

The Simplified Byzantine Fault Tolerant (SBFT) consensus algorithm implements an adopted version of the Practical Byzantine Fault Tolerant algorithm.

The basic idea involves a single validator who bundles proposed transactions and forms a new block.

The Consensus is achieved as a result of a minimum number of other nodes in the network ratifying the new block.

Nodes are clustered with increasing authority in delegations. The 1st node is called the lead, the 2nd node is the second in command, and so on.

A particular delegation with pre-determined 'Open' and 'Close' timestamps holds each new block and this information is exchanged with every other node in the delegation.

Each node uses its internal time to determine whether those actions are to be performed and has detailed guidelines on how to behave.