

## **Consensus Algorithms:**

We know that Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency. There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified. This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network.

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

---

The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

Now, we will discuss various consensus algorithms and how they work.

### **Proof of Work (PoW):**

This consensus algorithm is used to select a miner for the next block generation. Bitcoin uses this PoW consensus algorithm. The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution. This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block. For more details on PoW, please read Proof of Work (PoW) Consensus

### **Practical Byzantine Fault Tolerance (PBFT):**

Please refer to the existing article on practical Byzantine Fault Tolerance (pBFT).

### **Proof of Stake (PoS):**

This is the most common alternative to PoW. Ethereum has shifted from PoW to PoS consensus. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stake. After that, all the validators will start

validating the blocks. Validators will validate blocks by placing a bet on it if they discover a block which they think can be added to the chain. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets and their stake increase accordingly.

In the end, a validator is chosen to generate a new block based on their economic stake in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.

### **Proof of Burn (PoB):**

With PoB, instead of investing into expensive hardware equipment, validators 'burn' coins by sending them to an address from where they are irretrievable. By committing the coins to an unreachable address, validators earn a privilege to mine on the system based on a random selection process. Thus, burning coins here means that validators have a long-term commitment in exchange for their short-term loss. Depending on how the PoB is implemented, miners may burn the native currency of the Blockchain application or the currency of an alternative chain, such as bitcoin. While PoB is an interesting alternative to PoW, the protocol still wastes resources needlessly. And it is also questioned that mining power simply goes to those who are willing to burn more money.

### **Proof of Capacity:**

In the Proof of Capacity consensus, validators are supposed to invest their hard drive space instead of investing in expensive hardware or burning coins. The more hard drive space validators have, the better are their chances of getting selected for mining the next block and earning the block reward.

### **Proof of Elapsed Time:**

PoET is one of the fairest consensus algorithms which chooses the next block using fair means only. It is widely used in permissioned Blockchain networks. In this algorithm, every validator on the network gets a fair chance to create their own block. All the nodes do so by waiting for random amount of time, adding a proof of their wait in the block. The created blocks are broadcasted to the network for others consideration. The winner is the validator which has least timer value in the proof part. The block from the winning validator node gets appended to the Blockchain. There are additional checks in the algorithm to stop nodes from always winning the election, stop nodes from generating a lowest timer value.

There also exist other consensus algorithms like Proof of Activity, Proof of Weight, Proof of Importance, Leased Proof of Stake, etc. It is therefore important to wisely choose one as per the business network requirement because Blockchain networks cannot function properly without the consensus algorithms to verify each and every transaction that is being committed.



