Unit 3

Index

Consensus

It is a procedure to reach a common agreement on a distributed decentralised environment.

The reason for using a consensus algorithm is as follows:

- **Agreement**- every correct individual agrees on the same value
- **Termination** - when the algorithm ends, all valid individuals decide on a value
- **Validity** - If all individuals propose the same value, all correct individuals decide on that value.
- **Fault tolerant** - the network should work in presence of faults
- **Integrity** - Every correct individual has at most one value.

Proof Of Work

This was proposed way before the white paper.

It works on the principle that the solution us hard to find but easy to verify. Each node needs to solve a math problem to find the solution i.e. propose the transaction. The math problem is finding the hash value based on the previous block's hash and the hash value of the input message. The solution will be less than the difficulty of the blockchain i.e. size less than size of difficulty.

The proposed value is called a nonce. This is then verified throughout the chain. The nonce should then be validated by a majority usually 51% but can change based on the chain.

Advantages	Disadvantages
Tested from a long time so is known to be reliable.	Slow and gets more costly as more people join.
More guaranteed. We know there will be no rollback.	51% risk
It is trustless. No one can block your transaction from processing.	Can indirectly lead to centralization. The people with the most resources can pool together.

Proof of Stake