CONSENSUS IN BLOCKCHAIN

So What is actually consensus?

We know the blockchain is distributed database so lets assume we have 5 Nodes

All 5 Nodes have the copy of blockchain and all the copies have the same state.

What will be the procedure if we have a new Block how it will be added?

You have a block which will be added by one of the five nodes above mentioned in the chain.

Lets assume Node4 will be added the new block in its own blockchain and through some protocol it will be added by all blockchain.

**Now Here is the Problem What if Node4 is malicious?**

**Now How will you sure all the Nodes will come to consensus and they will have same copy of it ?**

Here are some consensus algorithms which determine the new block will added

There are many c**onsensus algorithms**

1. Proof of work(POW)

Bitcoin uses POW to achieve the consensus

**So what is actually POW?**

POW means all the nodes do have some computational power and the have to solve the puzzle and who will solve the puzzle first that Node will add the new block in blockchain.

Then they will receive award in shape like bitcoin.

But in POW we have to sure that before adding the data in block it should do computation and spent some computation power so we trust them

1. POS (Proof of Stack)

Here question comes why we need the POS when we have the POW?

In POW we have to do a lot of computational work and it needs a lot of resource to do that but in POS we do not need this computational work.

In POS we need to actually add the stake like node a spend the 5 bitcoin then it will create a stack and the nodes who will have more stake will actually win the puzzle and get the reward of new block added.

3)PoET(proof of elapsed Time) built by INTEL

4)POD(Proof of Deposit)

5)POC(Proof of Capacity)

IN POC who have large storage will win the block reward

So at the end in consensus we actually agreed in one particular state in whole network