Consensus protocol

Consensus protocol is the process by which a network of nodes confirms the record of previously verified Txs and by which it verifies new txs.

PROBLEMS WITH PROOF OF WORK PROTOCOL :

1. In BTC, no user is implicitly trusted to verifyTxs.All users follow an algorithm that verifies transactions by committing software and hardware resources to solve a problem by brute force.The miner who solves the cryptographic puzzle first, is rewarded.

2. Anyone can operate in BTC, across the globe.This has led to black market trading since the consensus protocol is energy consuming ,the majority of users operate in countries with cheap electricity, leading to network centralisation and possibility of collusion, thereby making the network vulnerable to changes in policy of electricity subsidies.

Both of these has led to increased interest in private blockchains.In private blockchains, the control is customised to a specific set of users as to who can verify or submit or read the transactions.

Private blockchain can allow who is allowed to operate a node as well as how nodes are connected. Nodes with more connections receive info faster. Nodes may be required to maintain certain number of connections to be considered active. A node that transmits incorrect information or that restricts the transmission of information can be identified in order to maintain the integrity of the system.
How to treat uncommunicative to intermittently active nodes? Even if nodes go offline, the network must be structured to function without them and be able to quickly bring these nodes back to speed if they return.

DIFFERENT CONSENSUS PROTOCOLS

1.**Proof of Work:**

- Ensures that the next block in a blockchain is the one and only version of truth .
- Miners compete to add the next block in the chain by racing to solve a cryptographic puzzle.
- The first to solve gets a reward of 12.5 BTC and transaction fee.
- This reward halves every 4 years.

Cons:

1. Requires huge amount of computational energy, resulting in centralisation of mining in areas of world where the electricity is cheap.

2. Doesn’t scale well as the transaction confirmation itself takes about 10-60 minutes.

2.**Proof of Stake:**

- No coin creation concept exists here.
- All the coins exist from the beginning.
- Instead of investing in expensive computer equipment, here, a ‘**validator**’,also called stake holder, invests in the coins of the system and are paid strictly in terms of the transaction fees.
- Your chance of being picked to create next block is strictly proportional to the stake you hold(number of coins in the system you own).A validator with 30 coins is 3 times more likely to get a chance to create a block than a validator with 10 coins.
- After creation of block by validator, the block to be added to the chain, has to be signed by various signers in the system.

Nothing at stake problem:

What is to discourage a validator from creating 2 blocks and claiming 2 sets of transaction fees?What is to discourage a signer to double sign both of those blocks?
A participant with nothing to lose has no reason not to behave badly.This is nothing at stake problem.

Eg:
1. Tendermint - Every node has to sign until a majority vote is reached, while in other systems a group of signers is randomly chosen.

2. Peer-coin, NXT, black coin uses proof of stake.
Note: Ethereum uses Proof of work but is planning to move to proof of stake.

2 variations of Proof of stake exist.

(i)Leased Proof of stake
(ii)Delegated Proof of stake

LEASED PROOF OF STAKE:
In classic POS, accounts with small balances are unlikely to stake a block, just like small miners with low hash rate are unlikely to mine a block in bitcoin system.
The accounts with low balances would never get a chance to mine a block thereby leaving the network to a limited number of users with higher account balances.
Since network security is better in decentralised system with large number of players, it is important to incentivise these small holders to take part.
LPOS achieves this by allowing holders to lease their balances to the staking nodes(accounts with low balances).
Leased coins then increase the weight of the staking node, thereby increasing its chance to mine a block.Any rewards receives are shared proportionally with the leasers.
Eg: Waves

DELEGATED PROOF OF STAKE:
Coin holders use their balances to elect a list of nodes that will have the opportunity to stake blocks of new transactions and add them to the blockchain.
This engages all stakeholders with small or large balances.

Holders can also vote for changes to the network parameters for greater influence and ownership over the network.

PROOF OF ACTIVITY:

- Formulated by BTC to avoid the tragedy of the commons.
- To avoid hyperinflation , BTC will only ever produce 21million BTC.For every 4 years, BTC reward halves, thereby leading to a point of time where the BTC block reward subsidy will end and miners would receive only transaction fee.This spoils the system where people could act in self interest.So proof of activity is created as an alternative incentive structure for BTC.
- Hybrid approach which starts with proof of work, where miners racing to solve a cryptographic puzzle.
- Mined blocks don't contain any transactionut contains only miners address and the header.
- Now it switches to proof of stake.Based on the information in the header , a random group of validators are chosen.The more coins a user has, the more likely he gets to be chosen to sign the new block.
- After all the chosen signers sign, the block is added to the system.
- If any of the chosen validators are absent, the system would chose next winning block to be added to the blockchain.

CONS:
Same as that of proof of work and proof of stake.
Eg: Decred

PROOF OF BURN:

- Instead of investing in computing equipment, here you burn coins by sending them to an online vault which is not refundable, thereby earning privilege to mine in the system based on a random selection process.
- The more coins you burn the better chance you have of being selected to mine the next block.
- Over time, stake decays and again investment needs to be done to increase your odds of being selected to mine the next block.

CONS:
Similar to BTC, instead of miners in areas where electricity is cheap, here mining power goes to those who are willing to burn more money.
The protocol wastes resources needlessly.

Eg: Slimcoin

PROOF OF CAPACITY:

- Pay with hard drive space.
- The more hard drive space you have, the better your chance of mining the next block and earning the block reward.
- The algorithm generates large data sets known as plots which you store on your hard drive.The more plots you have, the better your chance of finding the next block in the chain.

CONS:
By investing in space, you buy yourself a better chance to create duplicate blocks.Again nothing at stake problem arises.

PROOF OF ELAPSED TIME:
Similar to proof of work but with less electricity.
The algorithm uses a trusted executed environment to ensure blocks get produced in a random lottery fashion, but without the required work.

PROOF OF IMPORTANCE:
Based on the idea that the productive network activity, not just the amount of coins, should also be rewarded.
Odds of staking a block are based on various factors like balance, network activity, reputation and the number of transactions made to and from that address.

LINK:
1. https://www.coindesk.com/bitcoins-taproot-privacy-tech-is-ready-but-one-things-standing-in-the-way/
2. https://blog.wavesplatform.com/review-of-blockchain-consensus-mechanisms-f575afae38f2