Association For Cyber Security

Consensus Mechanisms List

Consensus mechanisms are vital protocols that ensure the integrity, security, and functionality of blockchain networks by allowing distributed nodes to agree on the state of the blockchain.

Proof of Work (PoW)

Proof of Work (PoW) is the original consensus mechanism used by Bitcoin and many other cryptocurrencies. In PoW, miners compete to solve complex mathematical puzzles using computational power. The first miner to solve the puzzle gets the right to add a new block to the blockchain and receives a reward, usually in the form of cryptocurrency.

Working Principles:

- Miners collect transactions and bundle them into a block.
- They then solve a cryptographic puzzle (finding a nonce that, when hashed with the block's data, produces a hash with a specific number of leading zeros).
- The first miner to solve the puzzle broadcasts the block to the network.
- Other nodes validate the block and add it to their copy of the blockchain if it is valid.
- The process repeats for the next block.

Proof of Stake (PoS)

Proof of Stake (PoS) is an alternative to PoW that aims to reduce energy consumption and improve scalability. In PoS, validators are chosen to create new blocks and validate transactions based on the number of tokens they hold and are willing to lock up as collateral.

Working Principles:

- Validators lock up a certain amount of cryptocurrency as a stake.
- A validator is randomly selected to propose a new block based on their stake and other factors.
- Other validators attest to the block's validity.
- If the block is validated, the proposer and the attesters receive rewards.
- If a validator acts maliciously, they can lose their staked tokens.

Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) is a variation of PoS that involves token holders voting to elect a small number of delegates who will validate transactions and create new blocks on their behalf.

Working Principles:

- Token holders vote for a fixed number of delegates.
- Elected delegates take turns producing blocks and validating transactions.
- If delegates fail to perform their duties, they can be voted out and replaced.
- Delegates share a portion of the rewards with the voters.

Practical Byzantine Fault Tolerance (PBFT)

Practical Byzantine Fault Tolerance (PBFT) is a consensus mechanism designed to work efficiently in environments where nodes may fail or act maliciously. It is often used in permissioned blockchain networks.

Working Principles:

- Nodes in the network (replicas) communicate to agree on the order of transactions.
- A primary node proposes a block, and other nodes validate and vote on it.
- If a sufficient number of nodes (usually two-thirds) agree, the block is added to the blockchain.
- If the primary node fails, a new primary is elected.

Proof of Authority (PoA)

Proof of Authority (PoA) is a consensus mechanism where a limited number of pre-approved validators, known as authorities, are responsible for validating transactions and creating new blocks.

Working Principles:

- Validators are chosen based on their identity and reputation.
- Only these authorities can create new blocks and validate transactions.
- The identity of validators is public, and they must maintain their reputation to stay in the network.

Proof of Participation (PoP)

Proof of Participation (PoP) is a consensus mechanism designed to ensure that participants in the blockchain network are actively engaged in the network's activities. It rewards users not only for holding tokens but also for their active participation, such as making transactions, voting, or contributing to the network in other ways.

Working Principles:

- Users earn participation points for engaging in network activities.
- Points can be accumulated through various actions, such as validating transactions, voting in governance decisions, or providing network services.
- Participants with higher points have a higher probability of being selected to create new blocks.
- Rewards are distributed based on participation points, incentivizing active involvement in the network.

Proof of History (PoH)

Proof of History (PoH) is a novel consensus mechanism used by the Solana blockchain. It establishes a historical record that proves that an event has occurred at a specific moment in time. This proof allows nodes to agree on the order of events without having to rely on the traditional consensus protocols.

Working Principles:

- PoH relies on a cryptographic timestamp that records the sequence of events in the blockchain.
- Each event or transaction is hashed along with a count and a timestamp, creating a verifiable and immutable sequence.
- This sequence can be used to prove the chronological order of transactions, reducing the need for extensive communication between nodes.

- PoH can be combined with other consensus mechanisms (like PoS) to enhance overall network efficiency and security.

Proof of Elapsed Time (PoET)

Proof of Elapsed Time (PoET) is a consensus mechanism designed to achieve consensus with minimal energy consumption. It is used by the Hyperledger Sawtooth blockchain platform.

Working Principles:

- Nodes in the network are required to wait for a random period of time, determined by a **trusted execution environment (TEE)** such as Intel's SGX.
- Each node sleeps for a randomly chosen period and the first node to complete its waiting period gets to create the next block.
- The waiting time is enforced by the TEE, ensuring fairness and randomness in block creation.

Proof of Space (PoSpace) / Proof of Capacity (PoC)

Proof of Space (PoSpace), also known as **Proof of Capacity (PoC),** is a consensus mechanism that uses disk space to secure the blockchain.

Working Principles:

- Miners allocate a portion of their hard drive space to store cryptographic proofs.
- The amount of space dedicated determines the probability of being selected to create a new block.
- Larger storage capacity increases a miner's chances of being chosen.

Proof of Burn (PoB)

Proof of Burn (PoB) is a consensus mechanism where participants "burn" (destroy) a portion of cryptocurrency to gain the right to create new blocks.

Working Principles:

- Participants send a certain amount of cryptocurrency to an unspendable address, effectively removing it from circulation.
- In return, they earn the right to create new blocks and receive rewards.
- The more cryptocurrency burned, the higher the chance of being selected.

Association for Cyber Security looks forward towards your success!
Contact us: +91 7938001181 | Email: info@acs.albussec.com