SMVS
Page No.
Date : / /

Consensus

* Consensus :

=> Consensus Mechanism ensures that all nodes agree on the validity and order of transmission in network.

Consensus Algorithms establish reliability and trust in the Blockchain network.

=> Why Blockchain needs Consensus Mechanism:

Blockchain are decentralized network where multiple nodes validate and agree transaction without the central authority.

This Mechanism help all nodes agree on the current state of the blockchain.

Consensus Mechanism prevent double-spending and ensure that all transaction are legitimate and accurately recorded.

They Protect the blockchain from malicious attack and ensure network remains trustworthy.

Consensus Mechanism allowing nodes to independently verify and agree on transaction.

=> Consensus in Synchronous Blockchain System:

In Synchronous Blockchain system, all nodes have synchronized time clock.

Between all the nodes messages are delivered within a known time frame.

In this system, Consensus can be achieved relatively easily because nodes are rely on the timing of message delivery.

Protocol like Paxos variants are often used.

SMVS
Page No.
Date : / /

=> Consensus in Asynchronous Blockchain System:

In this system, No gurantees about message delivery time between Nodes.

Nodes operate independently without synchronous clock so, message can be delayed indefinitely.

Achieving consensus in Asynchronous system is more difficult.

Protocols need to handle uncertainties in message delivery and communication.

Bitcoin operates in Asynchronous System where delays and failures are part of the design.

* Explain Proof of Work:

=> Proof of Work is used in Consensus Mechanism to validate transaction and secure blockchain.

It involves solving complex mathematical problem to add new block in the blockchain.

=> Working:

1 Problem Solving:

The network creates a cryptographic puzzle that are require computational power to solve.

Miners compete to solve this puzzle by performing various hash calculation.

The First Miner to Find a valid solution broadcast it to the network.

2 Validation:

Other nodes in the networks verify the correctness of the solution provided by the miner.

Once verified, the new block is appended to the blockchain

SMVS
Page No.
Date : / /

3 Difficulty Adjustment:

The difficulty of the puzzle adjust periodically based on the network's overall computational power.

=> Advantages:

1 PoW provides strong security against attacks.

2 It supports decentralization approach.

=> Disadvantages:

1 PoW is highly energy-intensive.

2 Extensive computational work can lead to scalability issues.

=> Example: Bitcoin.

* Proof of Stake:

=> Proof of Stake is a consensus mechanism used in Blockchain network to ~~to~~ validate transaction.

Proof of stake relies on the ownership of the cryptocurrency.

=> Working:

1 Stake-Based Validation

In PoS, Validators are chosen to create the new block and validate transaction based on the amount of cryptocurrency.

Validators are seleted through various methods which can include random selection.

2 Block Creation and Validation:

The selected Validator proposes a new block of transaction.

Other validator in the network verify the proposed block.

If the block is valid by the majority, it is added to the network.

SMVS
Page No.
Date : / /

3 Rewards and Penalties :

Validators earn rewards for successfully validating and proposing the block.

If Validator fail to perform their duties than loss the part of their staked cryptocurrency.

=> Advantages :

1 PoS is much less energy-intensive

2 PoS can handle higher volume of the transaction

=> Disadvantages :

The System may favor those with more cryptocurrency.

=> Example : Cardano Blockchain

* Proof of Burn :

=> Proof of Burn is a consensus mechanism used to achieve network consensus.

In this system, Network Participants have to burn a portion of their cryptocurrency.

=) Working:

1 Burning Coins:

Participants send a certain amount of their cryptocurrency to a predetermined "burn address".

The Burning Coin is used to demonstrate the participant's commitment to network.

2 Block Validation:

Participants who burn coins become eligible to validate transaction or create new block.

The Participant selected to validate transaction and create new block.

Other Participant verify and agree on the block before it

added to the blockchain

3 Rewards and Incentives:

Successful Validator are rewarded with new cryptocurrency.

=> Advantages:

1 More energy energy-efficient compared to PoW.

2 PoB can reduce the risk of the centralization.

=> Disadvantages:

1 Burning coins are irreversible, means participant can loss their coins

2 PoB can favor those have to afford burn more coin.

=> Example: Counterparty.

Page No.
Date : / /

* Proof of Elapsed Time:

=> Proof of Elapsed Time is a Consensus mechanism designed to achieve consensus in blockchain.

PoET is developed by Intel for the Hyperledger Sawtooth Blockchain.

In this, Participants have to given a radom wait time.

=> Working:

1 Random wait time:

Each node into the network give the random wait time before proposing the block.

The nodes that waits the shortest time being eligible to propose the next block.

2 Trusted Execution Environment:

PoET relies on a hardware-based TEEs such as Intel's SGX.

SMVS
Page No.
Date : / /

3 Block Proposal:

After the random wait time expires, the node that has shortest wait time is selected to create new block.

Other nodes verify the proposed block and the validity of time.

4 Rewards and Penalties:

The node that successfully proposes a block is rewarded with transaction fee or cryptocurrency.

If a node fails to follow protocol, it may be Penalized.

=> Advantages:

1 More energy-efficient compare to PoW

2 Higher transaction Throughput

=> Disadvantages:

1 PoET relies on hardware devices.

2 Less Commonly used, which may have limited practical support.

=> Example: Hyper Ledger Sawtooth

* Sybil Attack in Blockchain:

=> A Sybil Attack is a type of security threat in distributed network.

Sybil means person with multiple personality disorder

In this attack, Attacker create multiple fake identities or nodes.

=) Work:

1 Identity Creation:

The Attacker generater a large number of a fake node or identities within the network.

This nodes appear as legitimate

SMVS
Page No.
Date : / /

participants but are controlled by attacker.

2 Exploting Network Mechanism :

In a Consensus mechanism, Attacker fake node can block transaction or creating forks in blockchain.

The fake node can disrupt network operation by overwhelming the network traffic.

3 Impact on Network :

The Integrity of blockchain can be compromised.

Blockchain can reduced the trust.

=> Mitigation Strategies :

1 Implement reputation systems where node can build trust over time.

2 Use Identity Verification mechanism.

Date : / /

3 Use some trusted entities in the network design.

4 Use Hybrid Consensus model

5 Implement Staking Mechanism where nodes have to lock-up some amount of Cryptocurrency.

* Denial of Services in Blockchain

=> A Denial of Service attack in blockchain involves overwhelming the system's resources.

The goal of the DOS attack is to disrupt the normal operation of network.

This Attack makes system unavailable for legitimate users.

=> Types :

1 Network Layers Attack :

Attacker flood the network with

SMVS
Page No.
Date : / /

excessive data or transaction requests in network.

Also Attacker create large number of fake node or identities in the network.

2 Resource Exhaustion:

Attacker may send transaction that require significant computational resources.

Attacker submitting the transaction or data that can fill the storage of blockchain.

3 Consensus Disruption:

Attackers may create fork in the blockchain to disrupt the consensus system.

4 Smart Contract Exploits:

Attackers exploit vulnerabilities in smart contract to create transaction.

=> Mitigation Strategies:

1 Implement rate limits of the transaction request.

2 Enhance Node coordination to ensure efficient load distribution

3 Use optimized data structure and algorithm to handle higher size volumes of data.

4 Develop Adaptive consensus protocols

5 Implement monitoring tools to find patterns of network.