Unit II
Consensus Mechanism:
Permissioned Blockchain, Permisionless Blockchain , Different Consensus Mechanism- Proof of Work, Proof of Stake, Proof of Activity, Proof of Burn, Proof of Elapsed Time, Proof of Authority, Proof of Importance.

Unit II: Consensus Mechanisms in Blockchain
1. Types of Blockchain Networks

Blockchain networks are categorized based on their accessibility and control mechanisms. The two primary types are permissioned and permissionless blockchains.

Permissioned Blockchain

Definition

A permissioned blockchain is a network where participation is restricted, requiring authorization from a central authority or consortium. This controlled environment enables greater efficiency and security for enterprise applications.

Features

- **Restricted Network Access**: Only approved participants can join and interact within the blockchain network.
- **Known Network Participants**: Since access is limited, all members are identified, enhancing trust and reducing malicious activities.
- **Faster Transaction Processing**: Transactions are processed quickly due to reduced computational requirements and a smaller number of validating nodes.
- **Higher Privacy and Confidentiality**: Sensitive data remains within authorized participants, making it suitable for industries requiring compliance and confidentiality.
- **Lower Energy Consumption**: Since consensus mechanisms like Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) are used, they require minimal computational resources compared to Proof of Work (PoW).

Examples

- **Hyperledger Fabric**: An enterprise-grade blockchain framework designed for supply chain, banking, and healthcare applications.
- **Corda**: Focused on financial applications, allowing businesses to transact directly with high privacy.
- **Quorum**: An enterprise-focused version of Ethereum, designed for banking and financial use cases.

Use Cases

- **Enterprise Solutions**: Corporations use permissioned blockchains to manage and secure business processes.
- **Banking and Finance**: Facilitates secure transactions, cross-border payments, and settlements.

- **Supply Chain Management**: Ensures transparency, efficiency, and traceability in logistics and inventory.

Permissionless Blockchain

Definition

A permissionless blockchain, also known as a public blockchain, allows anyone to participate in the network without prior authorization. It operates in a fully decentralized manner, ensuring openness and transparency.

Features

- **Open Network Access**: Anyone with an internet connection can join, validate transactions, and participate in consensus mechanisms.
- **Anonymous/Pseudonymous Participants**: Participants can operate without revealing their real identities, ensuring privacy.
- **Complete Decentralization**: No single entity controls the network, reducing the risk of censorship and manipulation.
- **Higher Security**: Due to widespread distribution of nodes, the network is resilient against attacks.
- **Often Higher Energy Consumption**: Some consensus mechanisms, such as PoW, require significant computational power, leading to higher energy consumption.

Examples

- **Bitcoin**: The first and most widely adopted cryptocurrency, using PoW.
- **Ethereum**: A decentralized blockchain supporting smart contracts and dApps.
- **Litecoin**: A Bitcoin alternative with faster transaction speeds.

Use Cases

- **Cryptocurrencies**: Decentralized digital currencies, such as Bitcoin and Ethereum.
- **Public Applications**: Decentralized finance (DeFi) and decentralized applications (dApps).
- **Global Systems**: Open-source blockchain-based systems used for identity verification, voting, and record-keeping.

---

2. Consensus Mechanisms

Consensus mechanisms are protocols used to achieve agreement among distributed nodes about the state of a blockchain. They ensure network security, validity, and decentralization. Below are the major consensus mechanisms used in blockchain networks.

Proof of Work (PoW)

Definition

PoW requires validators (miners) to solve complex mathematical problems to validate transactions and create new blocks.

Process

1. Miners compete to find a nonce (a random number) that, when hashed, produces a value below a target threshold.
2. The first miner to solve the puzzle adds the next block to the chain.
3. The miner receives a block reward and transaction fees.

Advantages

- Highly secure against attacks.
- Established and proven mechanism.

Disadvantages

- Energy-intensive.
- Potential centralization due to mining pools.
- Slower transaction processing.

Examples

- Bitcoin, Litecoin, Dogecoin.

Proof of Stake (PoS)

Definition

PoS selects validators based on the amount of cryptocurrency they hold and are willing to "stake."

Process

1. Validators lock up their cryptocurrency as a stake.
2. The probability of being selected is proportional to the amount staked.
3. Validators earn transaction fees for confirming transactions.
4. Malicious validators risk losing their stake.

Advantages

- Energy-efficient.
- Reduces risk of centralization.
- Faster transactions.

Disadvantages

- "Nothing at stake" problem.
- "Rich get richer" scenario.

Examples

- Ethereum 2.0, Cardano

Proof of Authority (PoA)

Definition

Blocks are validated by a limited number of approved validators who have established reputations.

Process

1. A set of trusted validators take turns creating blocks.
2. Validators are known entities.
3. Transactions are confirmed rapidly without computational competition.

Advantages

- High efficiency and scalability.
- No need for mining.
- Fast transaction finality.

Disadvantages

- Less decentralized.
- Requires trust in validators.

Examples

- VeChain, POA Network, private Ethereum implementations.

Proof-of-Authority consensus

This section describes Proof-of-Authority consensus and its implementation in Apla.

What is Proof-of-Authority consensus

In blockchain platforms, consensus mechanisms can be divided into *permissionless* (Bitcoin, Etherium) and *permissioned* (Apla, Ethereum Private).

In a permissioned blockchain, all nodes are pre-authenticated. This advantage allows to use consensus types that provide high transaction rate in addition to other benefits. One of these consensus types is *Proof-of-Authority* (PoA) consensus.

Proof-of-Authority (PoA) is a new consensus algorithms family that provides high performance and fault tolerance. In PoA, rights to generate new blocks are awarded to nodes that have proven their authority to do so. To gain this authority and a right to generate new blocks, a node must pass a preliminary authentication.

Advantages of PoA consensus
Compared to other consensus types that require a proof of spent computational resources (Proof-of-Work) or an existing “share” (Proof-of-Stake), PoA consensus has several notable advantages:

- High-performance hardware is not required. Compared to PoW consensus, PoA consensus does not require nodes to spend computational resources for solving complex mathematical tasks.
- The interval of time at which new blocks are generated is predictable. For PoW and PoS consensuses, this time varies.
- High transaction rate. Blocks are generated in a sequence at an appointed time interval by authorized network nodes. This increases the speed at which transactions are validated.
- Tolerance to compromised and malicious nodes, as long as 51% of nodes are not compromised. Apla implements a ban mechanism for nodes and means of revoking block generation rights.

PoA consensus and common attack vectors

Denial-of-service attacks

An attacker sends a large number of transactions and blocks to a targeted network node in an attempt to disrupt its operation and make it unavailable.

The PoA mechanism makes it possible to defend against this attack:

- Because network nodes are pre-authenticated, block generation rights can be granted only to nodes that can withstand DoS attacks.

- If a node is unavailable for a certain period, it can be excluded from the list of validating nodes.

51% attack

In PoA consensus, the 51% attack requires an attacker to obtain control over 51% of network nodes. This is different from the 51% attack for the Proof-of-Work consensus types where an attacker needs to obtain 51% of network computational power. Obtaining control of the nodes in a permissioned blockchain network is much harder than obtaining computational power.

In a PoW consensus type network, an attacker can increase computation power (performance) of the controlled network segment thus increasing the controlled percentage. This makes no sense for PoA consensus, because the computational power of the node has no effect on the blockchain network decisions.

By design, Proof of Work consensus algorithm is vulnerable to Majority Attacks (51% attacks). Any miner with over 51% of mining power is able to control the canonical chain until their hash power falls below 50%. This allows them to reorg the blockchain, double-spend, censor transactions, and completely control block production.

A blockchain is a distributed ledger—essentially a database—that records transactions and information about them. The blockchain's network reaches a majority consensus about transactions through a validation process. The blocks where the data is stored are sealed. The blocks are linked together via cryptographic techniques where previous block information is recorded in each block. This makes the blocks nearly impossible to alter once they are confirmed enough times.

The 51% attack is an attack on the blockchain, where a group controls more than 50% of the hashing power, the computing that solves the cryptographic puzzle of the network. This group then introduces an altered blockchain to the network at a very specific point in the blockchain, which is theoretically accepted by the network because the attackers would own most of it.

Changing historical blocks—transactions locked in before the start of the attack—would be extremely difficult even in the event of a 51% attack. The further back the transactions are, the more difficult it is to change them. It would be impossible to change transactions before a checkpoint, where transactions become permanent in Bitcoin's blockchain(PoW)

---

3. Comparison of Consensus Mechanisms

Mechanism	Energy Use	Decentralization	Security	Scalability	Transaction Speed
PoW	Very High	High	High	Low	Low
PoS	Low	Medium-High	Medium	Medium	Medium-High
PoA	Low	Low	Medium	High	Very High

---

4. Selection Criteria for Consensus Mechanisms

When choosing a consensus mechanism, the following factors should be considered:

- **Security Requirements**: The level of resistance needed against attacks (e.g., PoW for high security).
- **Performance Needs**: Required transaction throughput and block finality speed.
- **Energy Considerations**: The environmental impact and cost of computational resources.
- **Decentralization Goals**: Whether a network requires full decentralization or partial trust.
- **Application Type**: Whether the blockchain is public, private, financial, or non-financial.
- **Network Size**: The number of participating nodes and how consensus affects their interactions.
- **Regulatory Compliance**: Compliance with laws such as KYC/AML and requirements for identifiable validators.

By evaluating these factors, organizations and developers can select the most appropriate consensus mechanism for their specific blockchain use case.