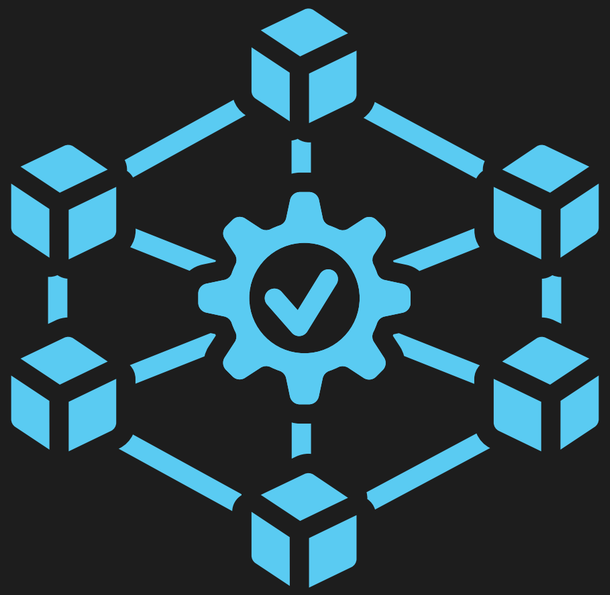
Blockchain: How does it work?

Vathna.lay@cadt.edu.kh

Introduction to Consensus

- Consensus refers to the general agreement or collective decision-making process among a group of participants.
- Example: Voting, Organizational agreement
- Consensus is crucial in distributed systems to ensure that all parties agree on a single version of truth.

Consensus in Blockchain



- Consensus in a blockchain network is a process by which all participants agree on the validity of transactions and the current state of the ledger.
- Consensus is Crucial in Blockchain:
  - Ensures data consistency across distributed nodes
  - Prevents double-spending and fraudulent activities.
  - Maintains trust without a central authority.

What Can Go Wrong Without Consensus

- Forking: splits into multiple chains due to lack of agreement
- Inconsistent Ledger: Different nodes have different transaction histories, leading to confusion and loss of trust.

Consensus Mechanisms

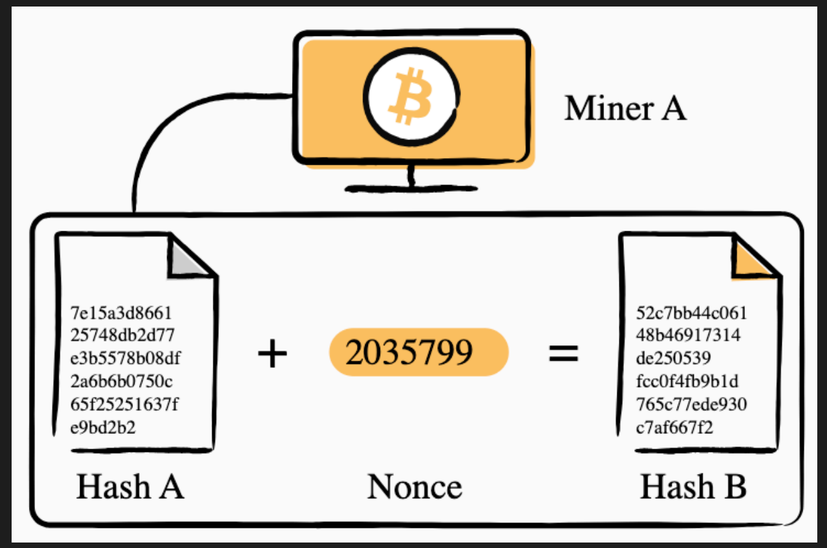
Consensus mechanisms are protocols used by blockchain network to validate transactions and maintain the integrity of the chain

- Proof of Work: a mechanism that requires participants (miners) to solve complex mathematical problems to validate a
- Proof of Stack: a mechanism that selects validators based on the number of coins they hold and are willing to “stake” as collateral

Proof of Work (PoW) Overview

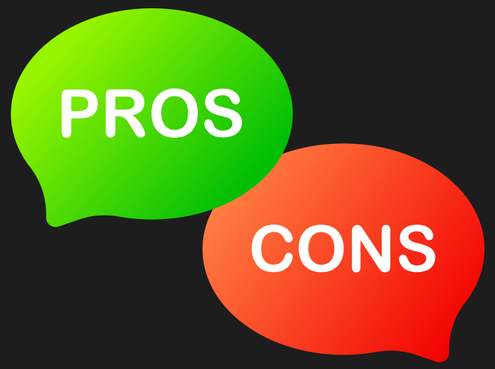
- Miners compete to solve a mathematical puzzle, which involves finding a nonce that, when hashed, produces a hash with a specified number of leading zeros.
- The first miner to solve the puzzle gets the right to add the new block to the blockchain and is rewarded with cryptocurrency (e.g., Bitcoin).

Nonce and Difficulty Level



- Nonce is a random value that miners change to find a hash that meets the network’s difficulty requirement
- Example: Suppose the network's difficulty requires finding a hash that starts with four leading zeros. Miners will repeatedly change the nonce value and re-hash the block data until they find a hash that meets this condition. For example, if the data is "Block 5 Data" and the current nonce is "9821", the miner will keep changing the nonce until the hash looks like "0000a3b45c...".

Pros & Cons of PoW



Pros:

- Difficult for attackers to alter the blockchain due to the computational power required
- Proven track record: PoW has been successfully used in Bitcoin since 2019

Cons:

- Energy consumption: mining requires a significant amount of electricity, leading to environmental concerns.
- Scalability issues: Transaction speeds are limited due to the time it takes to solve the puzzle.

Proof of Stake (PoS)

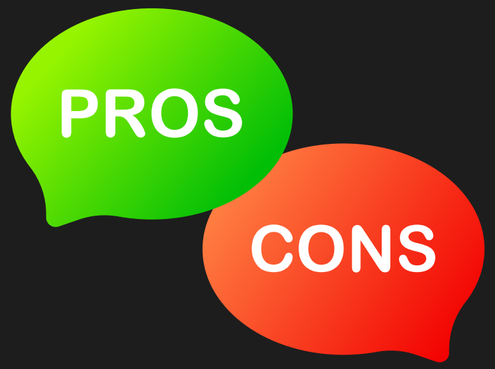
- Proof of Stake is a consensus mechanism where validators are chosen based on the amount of cryptocurrency they hold and are willing to lock up as a stake.
- How PoS Works:
  - Validators are selected to propose and validate blocks based on their stake.
  - The more coins a participant holds, the higher their chance of being selected as a validator.

PoW->PoS

- Ethereum 2.0's Transition to PoS:

- Ethereum is moving from PoW to PoS to improve energy efficiency and scalability. Validators replace miners, reducing the need for high computational power.

Pros & cons of Proof of Stake



Pros:

- Energy Efficiency: PoS consumes significantly less energy compared to PoW.
- Faster Transactions: Blocks can be added more quickly, improving transaction speeds.

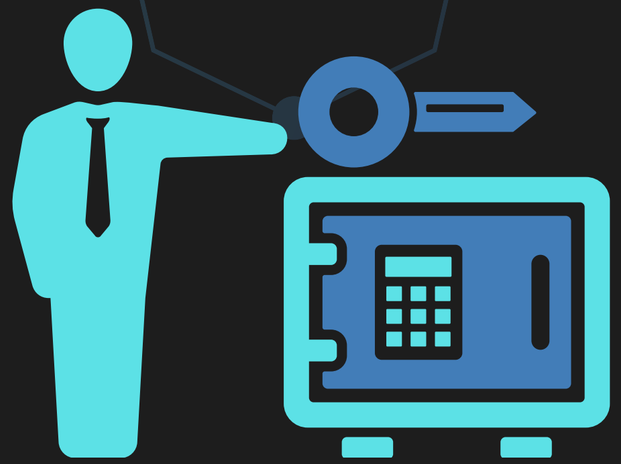
Cons:

- Centralization Risk: Wealthier participants with more coins have more influence, potentially leading to centralization.
- Nothing at Stake Problem: Validators might validate multiple forks, potentially compromising the chain's integrity.

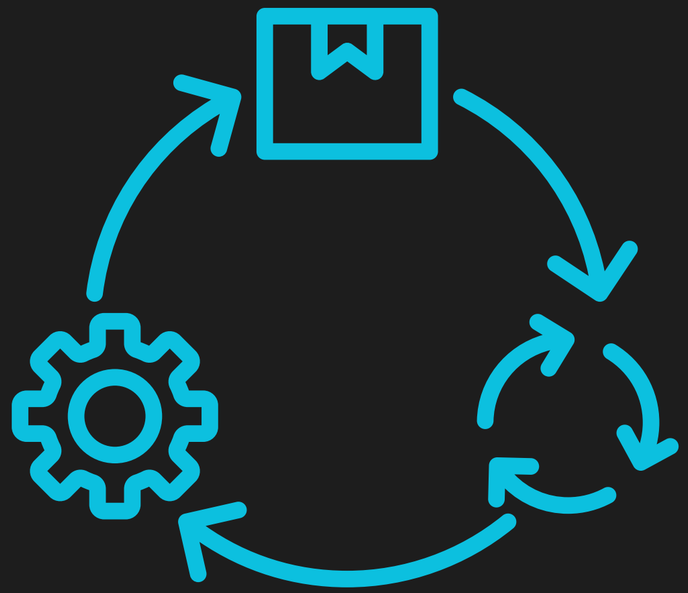
PoW vs PoS

- Security
- Scalability
- Energy Usage
- Network Participants

Role of Miners and Validators



Transaction Lifecycle in Blockchain



- **Creating a Transaction:** Users create a transaction with details like sender, receiver, and amount.
- **Broadcasting to the Network:** The transaction is broadcasted to nodes across the network.
- **Validation by Nodes:** Nodes validate the transaction for authenticity and correctness.
- **Inclusion in a Block:** Valid transactions are grouped and added to a new block.
- **Confirmation:** Once a block is added, the transaction is confirmed, and subsequent blocks further solidify its place in the blockchain.

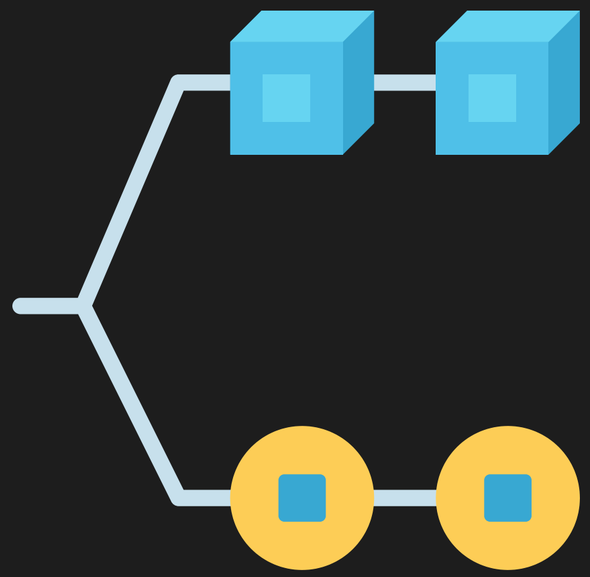
Role of Nodes in Blockchain Network

- **Full Nodes:** Store the entire blockchain and validate new transactions and blocks.
- **Mining Nodes (PoW):** Compete to add new blocks by solving cryptographic puzzles.
- **Validator Nodes (PoS):** Participate in validating blocks based on their stake.
- **Light Nodes:** Store part of the blockchain and rely on full nodes for verification.
- **Communication:** Nodes communicate to keep the blockchain updated and synchronized, ensuring data consistency.

Consensus in Action

- **Achieving Consensus:** How nodes work together to agree on the addition of new blocks.
- **Validation Process:** Nodes validate transactions and proposed blocks to maintain the integrity of the blockchain.
- **Role of Digital Signatures:** Ensuring transactions are secure and verified as authentic.

Forks in Blockchain

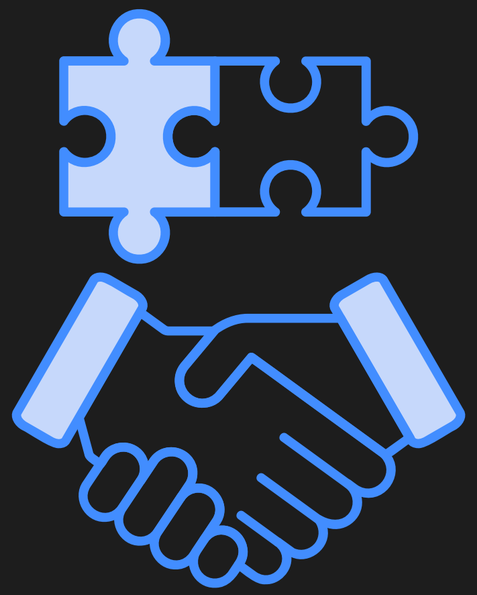


- **What are Forks?:** Situations where different versions of the blockchain exist temporarily.
  - **Soft Forks:** Backward-compatible updates where only non-upgraded nodes reject new blocks.
  - **Hard Forks:** Permanent splits requiring all nodes to upgrade to the new version, leading to two separate chains.
- **Examples:** Bitcoin vs. Bitcoin Cash.
- **Resolving Forks:** Consensus is used to determine which chain becomes the main chain.

Security Features of Blockchain

- **Immutability:** Once data is recorded, it cannot be changed without consensus from the majority of nodes.
- **Cryptographic Hashes:** How hashes like SHA-256 provide security and ensure the integrity of data.
- **Digital Signatures:** Ensure the authenticity of transactions by verifying the identity of the sender.

Blockchain Integrity



- **Hash Changes and Impact:** How altering data in a block changes its hash, breaking the chain.
- **Role of Consensus:** How the decentralized consensus mechanism helps prevent tampering.
- **Public Transparency:** Blockchain's public nature acts as a deterrent to malicious activities, as all participants can verify changes.

MCQ

What is the main purpose of consensus in blockchain?

a. To ensure data is consistent across all nodes

b. To control the price of cryptocurrency

c. To validate only the first transaction of the day

d. To allow miners to compete for rewards

MCQ

In Proof of Work (PoW), what do miners need to find to add a new block to the blockchain?

a. A digital signature

b. A nonce

c. A public key

d. A private key

MCQ

Which of the following is a key benefit of Proof of Stake (PoS) over Proof of Work (PoW)?

a. Higher energy consumption

b. Lower transaction speed

c. Reduced energy consumption

d. More complex cryptographic puzzles

MCQ

What happens when a blockchain experiences a hard fork?

a. The network stops working

b. The blockchain splits into two separate chains

c. All nodes are required to downgrade

d. Transactions are reversed

MCQ

In Proof of Stake, what determines the likelihood of a validator being chosen to propose a new block?

a. The number of transactions verified

b. The amount of cryptocurrency staked

c. The speed of their computer

d. The number of peers in the network

MCQ

Which of the following describes a "nonce" in the context of Proof of Work?

a. A unique digital signature used to sign blocks

b. A random value that miners adjust to solve a cryptographic puzzle

c. A type of validator used in Proof of Stake

d. The number of transactions in a block

MCQ

What is "slashing" in Proof of Stake (PoS)?

a. Rewarding validators with extra coins

b. Penalty for malicious behavior by taking away part of the stake

c. A way to speed up block creation

d. A method for adjusting the difficulty level

MCQ

Which of the following is a feature that helps ensure blockchain security?

a. Centralized control

b. Digital signatures

c. Faster block creation

d. Single point of failure

MCQ

What is the "Nothing at Stake" problem in Proof of Stake?

a. Validators losing all their cryptocurrency for misbehaving

b. Validators having no incentive to validate transactions

c. Validators validating multiple forks without any penalty

d. Miners not receiving rewards for their work

Use Case 1: Green Energy Initiatives

- Imagine a blockchain project focused on tracking and trading renewable energy credits. The goal is to make sure that the blockchain is as environmentally friendly as possible and does not consume excessive amounts of energy.
- **Question:** Which consensus mechanism (Proof of Stake or Proof of Work) would be more suitable for this project and why?

Use Case 2: High Security for a Financial Network

- Consider a blockchain being developed for a global financial system that requires very high security and protection against potential attacks. The system needs to handle high-value transactions, and the focus is on ensuring immutability and making it extremely difficult for any malicious actor to alter the blockchain.
- Question: Which consensus mechanism (Proof of Stake or Proof of Work) would be more suitable for this project and why?