Mini Task 1

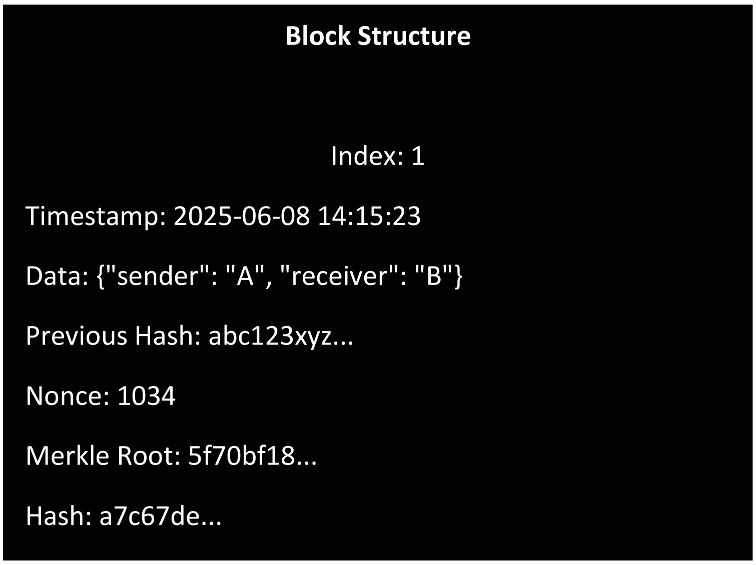
Blockchain

A blockchain is a decentralized, distributed digital ledger that stores data in a chain of blocks. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Since each block links to the previous one, it becomes almost impossible to tamper with, if anyone tries to change one block, the whole chain's integrity breaks. Blockchains are maintained by a network of nodes and use consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions without a central authority. This makes them secure, transparent, and trustless.

Real-life Use Cases

- Supply Chain Management – Track products across the supply chain to ensure transparency and detect tampering or delays (e.g., IBM Food Trust with Walmart).
- Digital Identity – Users can manage their own identity data without relying on centralized authorities (e.g., SelfKey, Sovrin).

Anatomy of a Block



Block Structure

Index: 1

Timestamp: 2025-06-08 14:15:23

Data: {"sender": "A", "receiver": "B"}

Previous Hash: abc123xyz...

Nonce: 1034

Merkle Root: 5f70bf18...

Hash: a7c67de...

Mekle Root

A Merkle tree organizes transaction data in a block into a binary tree where each leaf is a hash of a transaction, and each parent node is the hash of its children. The Merkle root is the topmost hash of the tree.

Example: If a block contains 4 transactions (T1, T2, T3, T4), the Merkle Root is

Hash(Hash(T1+T2) + Hash(T3+T4)).

It is particularly helpful to avoid checking all transactions. Just a few hashes (Merkle proof) can verify whether a specific transaction exists and is untampered.

Consensus Conceptualization

Proof of Work

PoW requires participants (miners) to solve complex mathematical puzzles (by computing hashes) to validate a block. The first miner to solve the puzzle gets to add the new block to the blockchain and earns a reward. Because the puzzle is hard to solve but easy to verify, it helps prevent tampering and ensures trust without needing a central authority. It’s energy-intensive because it involves thousands of hash computations per second, which becomes a downgrade due to environmental impacts and expensive hardware needs.

Proof of Stake

Proof of Stake replaces the mining race with a system where validators are chosen based on the amount of cryptocurrency they "stake" or lock in as collateral. More stake = higher chance of being chosen to validate the next block, which creates an incentive to behave honestly (or lose stake). This eliminates the need for intense computation, making PoS significantly more energy-efficient and eco-friendly than PoW. It's also faster and scales better for newer blockchains, making it a popular choice for Ethereum 2.0 and other modern chains.

Delegated Proof of Stake

In DPoS, users don’t directly validate blocks instead, they vote (usually based on stake) to elect a small group of delegates or witnesses who do the block validation on their behalf. These chosen delegates are responsible for creating and confirming blocks, which makes the system much faster and more scalable than traditional PoS. DPoS introduces a democratic element — users can change their delegates anytime, holding them accountable. This makes it suitable for applications that prioritize speed and governance (e.g., EOS, TRON).