Theoretical Part

1.Blockchain Basics

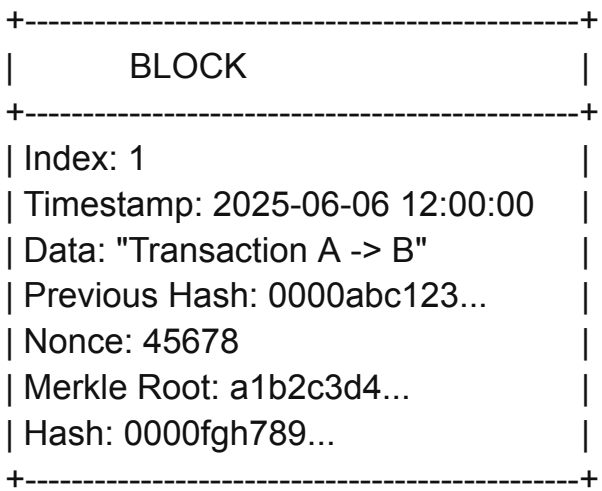
A blockchain is a distributed database or ledger shared across a computer network's nodes. They play a crucial role in maintaining a secure and decentralized record of transactions.Blockchains can be used to make data in any industry immutable.Since a block can’t be changed, the only trust needed is at the point where a user or program enters data.This reduces the need for trusted third parties,who add costs and can make mistakes.
Blockchains store data in blocks linked together via cryptographic hashes.In Bitcoin’s case, the blockchain is decentralized, so no single person or group has control—instead, all users collectively retain control. Decentralized blockchains are immutable, which means that the data entered is irreversible.

Real-life use cases

Financial Services
: Enabling faster, cheaper cross-border payments and reducing fraud in banking.

Government Usage
: Secure voting systems and land registry management

2.Block Anatomy



The Merkle root is a single hash summarizing all transactions. It's calculated by hashing individual transactions, then pairing and rehashing until one final root hash is formed.

This structure takes advantage of the collision resistance of hash functions. A hash function is considered collision resistant if it is difficult to find two inputs that produce the same hash output.

This property of collision resistance means that it is infeasible to find two different Merkle trees that contain the same transaction root since doing so would require finding at least one hash collision. As long as the root of the Merkle tree is protected against modification, the data that it contains can be stored simply as an ordered list.

With this list, anyone can regenerate the tree and compare the calculated root hash to the stored one. If they match, then the data has not been modified. If they do not match, then the data has been tampered with.

3. Consensus Conceptualization

Proof of Work(PoW)

Miners compete against one another to solve extremely complex computational puzzles using high powered computers.The first to come up with the 64-digit hexadecimal number ('hash') earns the right to form the new block and confirm the transactions. The successful miner is also rewarded. As it requires large amounts of computational resources and energy in order to generate new blocks, the operating costs behind PoW are notoriously high.

Proof of Stake(PoS)

Validators are chosen based on their coin ownership or "Stake".The more coins stacked, the better the odds to be chosen as a Validator. In PoS system simply earn a transaction fee. It requires less computation and is more energy efficient than PoW.

Delegated Proof of Stake(DPoS)

Stakeholders vote to elect a limited number of validators.Voting power is proportional to the amount of stake and reputation combined(previous transactions records).DPoS is a variation of PoS.