Theoretical Part:

1. Blockchain Basics

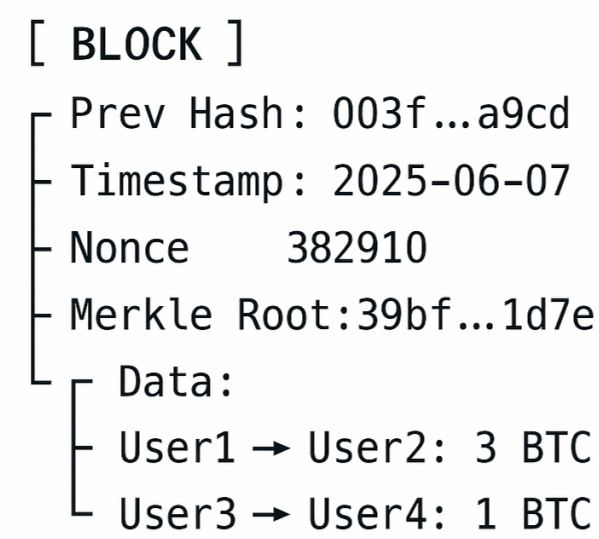
● A blockchain is a decentralized, immutable digital ledger that records data in blocks linked together in a chain. Each block contains a cryptographic hash of the previous block, a timestamp, and the transaction data. Because each block references the previous one, tampering with a single block disrupts the entire chain, making it secure and trustworthy. Blockchains operate without a central authority and rely on consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions. They are commonly used in cryptocurrencies like Bitcoin, Ethereum.

● Real-Life Use Cases:

1. Supply Chain – Track the movement and origin of goods.

2. Digital Identity Verification.

2. Block Anatomy



●

● A Merkle root is a single hash that represents all the transactions in a block. Transactions are paired and hashed repeatedly until a single hash remains. This final hash is the Merkle root. For example, if one transaction changes, its hash changes, and so do all parent hashes, which alters the Merkle root. Thus, it helps verify data integrity efficiently without checking each transaction.

3. Consensus Conceptualization

● Proof of Work (PoW):

PoW requires energy.

● Proof of Stake (PoS):

In PoS, validators are chosen based on the number of coins they hold and stake. It consumes less energy than PoW.

● Delegated Proof of Stake (DPoS):

In DPoS, validators are chosen based on votes, making the system faster but potentially more centralized.