1) Blockchain Basics

Blockchain is a type of digital ledger that keeps information safe, clear, and unchangeable by spreading it among many users. The transaction history is stored in blockchain as a series of blocks, with each block having a set of transactions. Cryptography links every block to the block that came before it, making the record permanent. Without the need for a central authority, blockchain lets a network of participants cross-check all data.

The integrity and validity of the data are achieved thanks to consensus algorithms like Proof of Work or Proof of Stake. As blockchain is fully open and secure from tampering, it is the perfect choice for use cases requiring transparency and safety.

Real-Life Uses for Data Mining:

a) Through Blockchain, it is possible to follow goods from their creation to purchase by consumers, ensuring they are genuine. It prevents fraud, minimizes delays, and enhances the performance of the supply chain.

b) Blockchain makes it possible to safely manage and keep digital identities. People can safely keep their own personal information by managing who has it.

2) Block Anatomy

All the information in a block is compressed and shown by the Merkle root, which is a cryptographic hash. The Merkle tree places the data into pairs and then hashes the pairs repeatedly until there is only a single root hash. This root hash is kept as part of the block to help confirm the correctness of all the data. If the data in just one block is updated, the Merkle root will be updated as well, which allows anyone to notice tampering easily.

Example : The Merkle root might be used in a supply chain to summarize all the details of a product’s journey. When the details regarding the product are modified, the Merkle root shall transform, showing that the product’s details have been changed.

Block Anatomy

Block

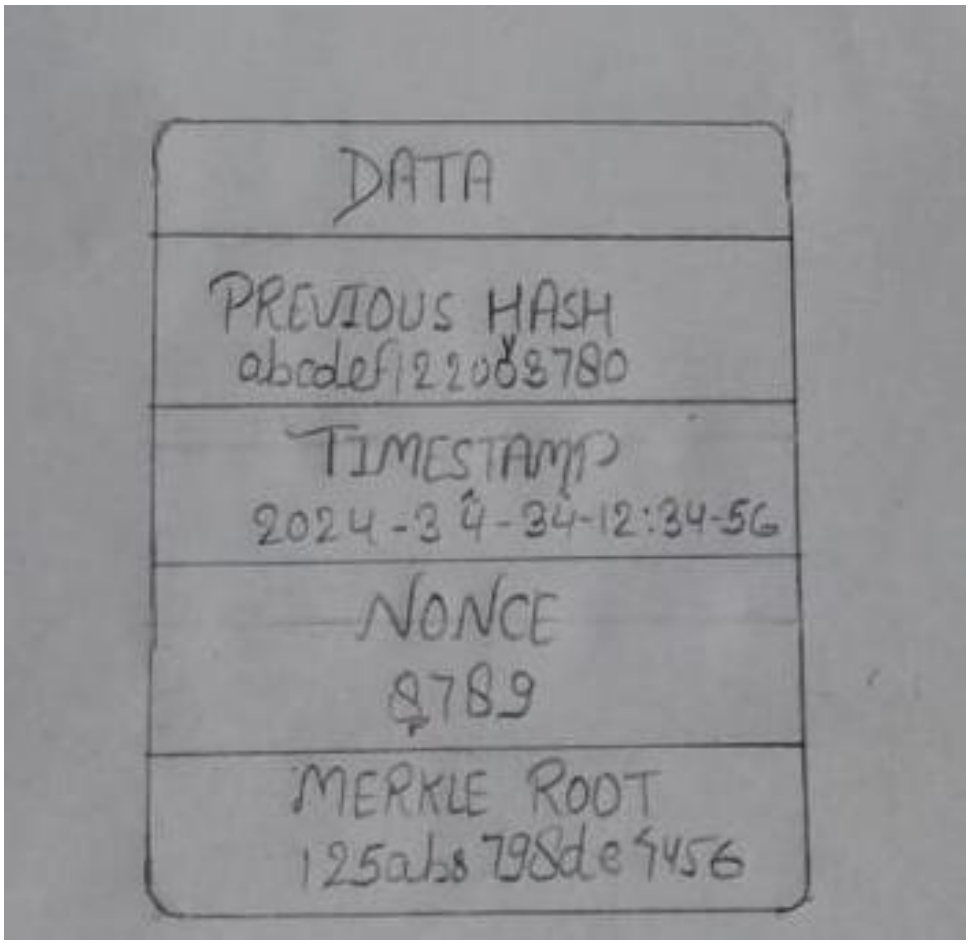
Data: (Transaction or Record)

Previous Hash: (Hash of the previous block)

Timestamp: (Date and Time the block is created)

Nonce: (A random number used in Proof of Work)

Merkle Root: (Root Hash of the Merkle Tree)



3) Consensus Conceptualization

a) Proof of Work (PoW): is a method that confirms transactions and adds them to a blockchain. Miners engage in solving problems and the first successful person holds the right to add their block to the chain. Securing the network takes a lot of powerful machines, and electricity is needed for this process. Making manipulations in the blockchain becomes more difficult the more energy is used in the network.

   Example : It is the job of Bitcoin miners to use energy to solve cryptographic puzzles for transaction verification. Because of this process, no transactions that could be fraudulent are allowed into the blockchain.

b) Proof of Stake (PoS): In Proof of Stake, users who own cryptocurrency and 'stake' it are chosen to build new blocks to confirm the transactions. Proof of Stake operations do not depend on demanding amounts of energy, unlike those of Proof of Work. Validators get paid for verifying transactions correctly, but they may lose all their investment if they approve dishonest transactions.

c) Difference from PoW: In contrast to PoW, PoS runs efficiently since it doesn't need complicated calculations. Consequently, it picks validators according to how much they invest, which is less demanding and happens more quickly.

d) Delegated Proof of Stake (DPoS): In Delegated Proof of Stake (DPoS), certain crypto holders pick a few reliable people called "delegates" to join the network and approve each block. People are elected as delegates because of their strong reputation and high voting power. DPoS is meant to create a faster and more scalable network by having just a small number of validators.

e) Validator Selection in DPoS: People in the community vote to pick which validators (delegates) will most likely be chosen in DPoS. Users with more tokens have extra voting authority and can choose delegates they respect for looking after the blockchain. Although this way makes consensus fast, it could give power to only a small number of validators.