Mini Task 1: Build & Explain a Simple Blockchain

By Ankan Dutta (Group-C)

Mail id: ankanudl18@gmail.com

Theoretical Part

1. Blockchain Basics

- **Define blockchain in your own words (100–150 words).**

Answer :

Blockchain is a decentralized, distributed, and public digital ledger that records transactions across many computers. It operates as a shared, immutable record, ensuring that once data is added, it cannot be altered. This technology is often used to track assets, record transactions, and provide a secure, transparent, and tamper-proof system. Bitcoin is the most popular cryptocurrency, an example of the blockchain. Blockchain Technology first came to light when a person or group of individuals named ‘Satoshi Nakamoto’ published a white paper on "*Bitcoin: A peer-to-peer electronic cash system*" in 2008.

Key Features:
Decentralized:
No single entity controls the blockchain; it's shared across a network of computers.
Distributed:
Data is stored across multiple computers, making it highly resistant to tampering.
Public:
Anyone can access the blockchain data and view the transactions.
Immutable:
Once a transaction is recorded in a block and added to the chain, it cannot be altered or deleted.
Consensus Mechanism:
A consensus mechanism is used to verify and validate transactions, ensuring that they are legitimate and that all participants agree on the state of the ledger.
Transparency:
All transactions are publicly accessible, allowing anyone to verify their validity and track the movement of data.

- **List 2 real-life use cases (e.g., supply chain, digital identity).**

Answer:

Financial Services:

Faster Transactions:

Blockchain can significantly reduce transaction times in financial services, enabling real-time settlements and minimizing exchange rate risks.

Improved KYC:

Blockchain-based solutions like "Smart Identity" can streamline the Know Your Customer (KYC) process, making it easier for banks and other financial institutions to verify customer identities.

Secure Asset Management:

Blockchain provides a secure and transparent platform for managing assets, including cryptocurrencies and other digital assets.

Healthcare:

Secure Patient Records:

Blockchain can be used to create secure and decentralized electronic medical records, improving data sharing and privacy.

Streamlined Business Processes:

Blockchain solutions can streamline various healthcare processes, such as insurance claims processing and medication tracking.

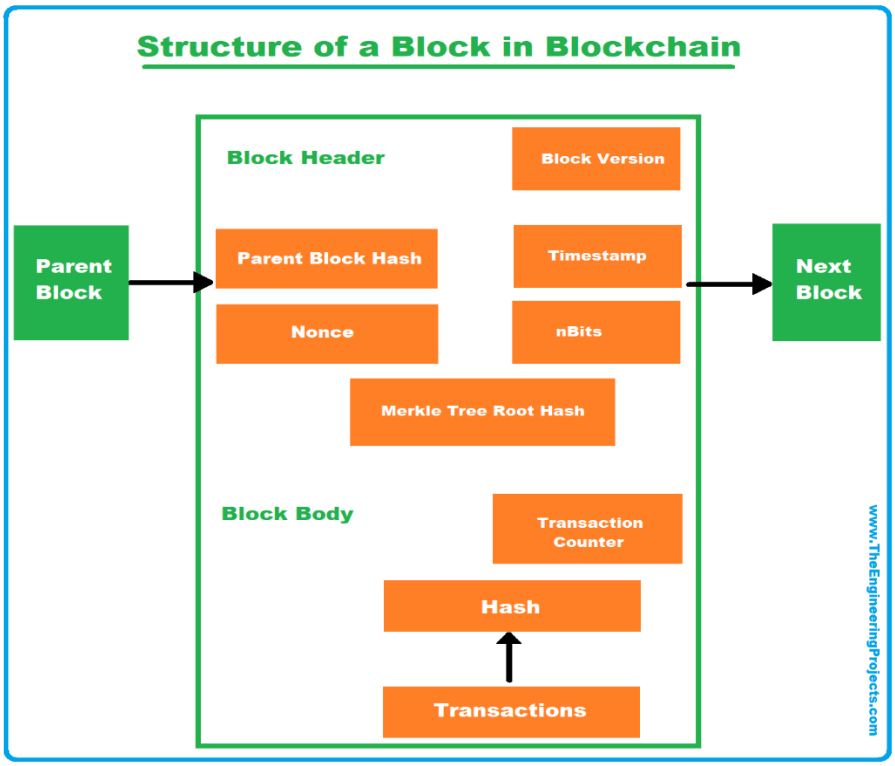
Drug Detection:

Blockchain solutions can streamline various healthcare processes, such as insurance claims processing and medication tracking. The blockchain system increases security through chain code-based transactions. When blockchains are used in quality control and counterfeit drugs identification, it improves safety . Anti-counterfeit medicine systems, such as the Anti-Counterfeit Medicine System (ACMS), are being used to combat counterfeiting.

2. Block Anatomy

- **Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.**

Answer:



- **Briefly explain with an example how the Merkle root helps verify data integrity.**

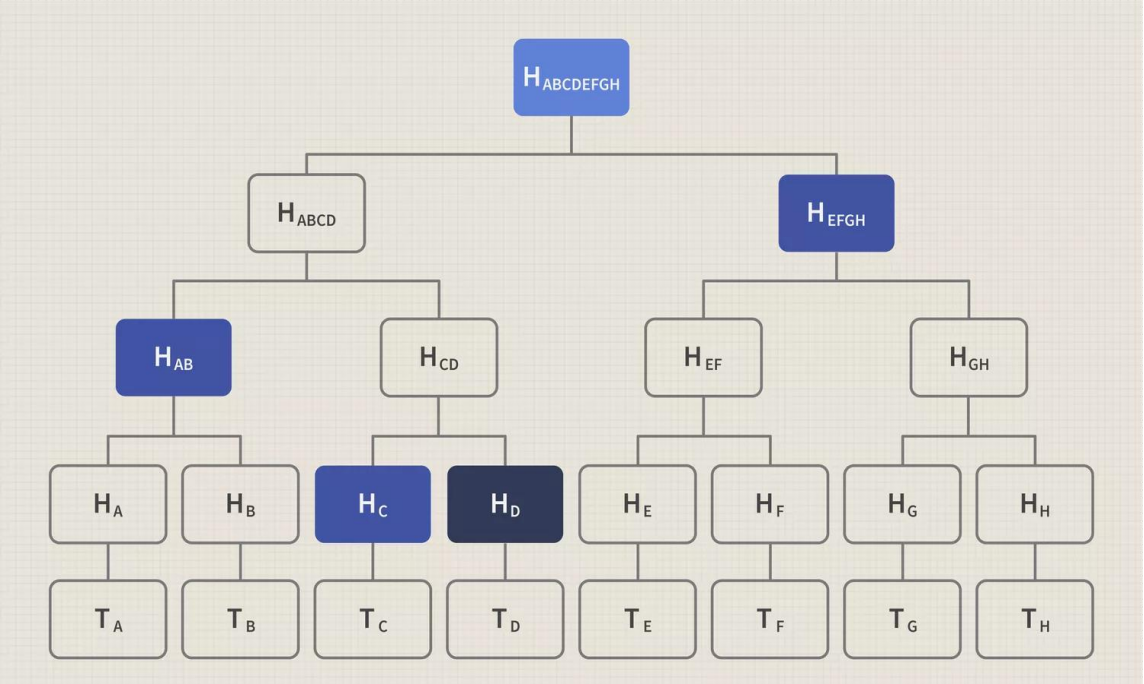
Answer:

A Merkle root is the result of hashing the transactions in a block, pairing those hashes, and hashing them again until a single hash remains. Some blockchains use it to verify transactions without hashing and pairing hashes to compare Merkle roots generated by other nodes. This technique reduces the time needed to verify the transactions included in a block.
Every transaction occurring on the blockchain network is hashed. However, these hashes are not stored in sequential order on the block but in the form of an upside-down tree structure such that each hash is hashed with another hash until all hashes have been turned into one hash.

Merkle Proof

The Merkle root is used to verify transactions because a blockchain node only needs to check select blocks within the Merkle tree. This is called the Merkle

proof. For example, in the Merkle tree below, the blockchain only needs to verify H_{AB}, H_C, and H_{EFGH} to make sure block hash H_D is included and accurate.



3. Consensus Conceptualization

- **What is Proof of Work and why does it require energy?**

  Answer:

  Proof of Work (PoW) is a consensus mechanism used in blockchains to verify transactions and add new blocks, ensuring the integrity of the network. It requires participants (miners) to solve complex computational puzzles to validate transactions, essentially "mining" for new blocks and receiving rewards in cryptocurrency.

  Miners consume high amounts of computing power in order to find the solution to the hard mathematical puzzle. It leads to a waste of precious resources(money, energy, space, hardware). It is expected that 0.3% of the world's electricity will be spent to verify transactions by the end of 2028.

- **What is Proof of Stake and how does it differ?**

  Answer:

Proof-of-stake (PoS) is a consensus mechanism in blockchain technology that secures networks by using the economic stake of participants rather than computational power.

Nodes on a network stake an amount of cryptocurrency to become candidates to validate the new block and earn the fee from it. Then, an algorithm chooses from the pool of candidates the node which will validate the new block. This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age based selection, randomization process) to make the selection fair to everyone on the network.

The key difference is PoS achieves consensus by requiring participants to stake crypto behind the new block they want to be added to a cryptocurrency's blockchain. Meanwhile, PoW achieves consensus by requiring participants to spend computational power and electricity by solving complex mathematical problems to generate a new valid block.

- **What is Delegated Proof of Stake and how are validators selected?**

Answer:

DPoS is an extension of Proof of Stake (PoS), where users stake their tokens to validate transactions and secure the network.

Delegated Proof of Stake (DPoS) is a consensus mechanism where users elect delegates to validate transactions and create blocks on a blockchain network. Validators, or delegates, are selected through a voting process, with each voter's weight determined by their stake in the network.

In DPoS, users vote for their preferred delegates, who are then responsible for validating transactions and creating new blocks. The number of votes a delegate receives determines their position in the network. The voting process can vary, but typically, users can vote directly or delegate their voting power to another entity. Each vote's weight is usually proportional to the number of tokens held by the voter.

How Validators Are Selected in DPoS?

In DPoS, users vote for their preferred delegates, who are then responsible for validating transactions and creating new blocks. The number of votes a delegate receives determines their position in the network. The voting process can vary, but typically, users can vote directly or delegate their voting power to another entity. Each vote's weight is usually proportional to the number of tokens held by the voter.

1. Token holders vote for their preferred validators (often called "witnesses" or "block producers").

2. Voting power is proportional to the voter's stake (e.g., more tokens = more voting weight).
3. The network selects the top N (e.g., 21 in EOS, 101 in Lisk) highest-voted validators.
4. These validators take turns producing blocks in a round-robin or randomized order.
5. Validators earn block rewards and transaction fees.
6. Voters may receive a share of rewards if their chosen validator is active.
7. If a validator misbehacks (e.g., downtime, censorship), stakeholders can vote them out.