Blockchain Basics

(1) What is Blockchain?

Answer :- A blockchain is a decentralized, tamper-resistant digital ledger where transaction records are grouped into "blocks." Each block links to the previous one using its cryptographic hash, creating a secure chain. This structure ensures immutability: once a block is added, altering it would break the chain unless the entire network agrees. Blockchains rely on consensus protocols, like Proof of Work or Proof of Stake, enabling trust without central authorities.

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

(i) How is blockchain used in supply chain tracking?

Answer :- Companies like **Walmart , Maersk , De Beers** , and **Volvo** use blockchain to record and trace the journey of goods from farms or mines through processing and shipping to the end consumer. This creates transparent, tamper-proof records that help ensure food safety, prevent counterfeits, and verify ethical sourcing.

(ii) How does blockchain support digital identity?

Answer :- Projects like **Proof of Humanity**, **Voatz**, and tech from **Blockchain Labs (COOV)** use blockchain to store and verify personal credentials such as ID, biometrics, or voter eligibility in a secure, decentralized way. This enhances privacy, reduces fraud, and enables trusted authentication without centralized control .

Block Anatomy

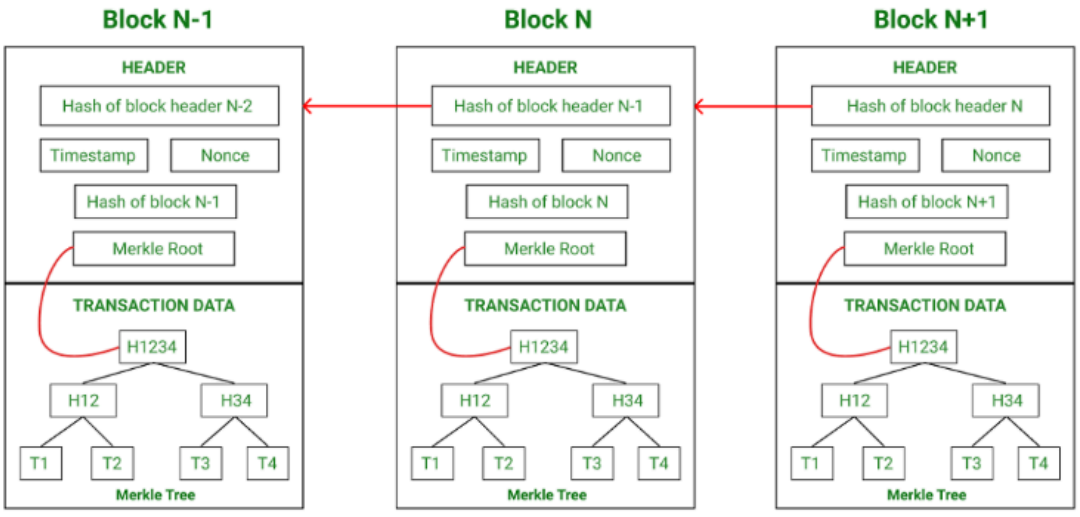
(3) Briefly explain with an example how the Merkle root helps verify data integrity.

Answer :- Imagine a block with 4 transactions: T1, T2, T3, and T4. Each one is hashed (H1…H4). Then H1+H2 gets hashed into H12, and H3+H4 into H34. Finally, H12+H34 gets hashed into the Merkle root (H1234). If someone alters T2 to T2′, H2 changes → H12 changes → Merkle root changes .

To check if T2 is in the block, a node only needs H2 (leaf), its sibling H1, and H34 from the tree. Recomputing upward and matching the known Merkle root proves T2 is authentic without downloading all transactions.

(4) Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root

Answer :-



Consensus Conceptualization

(5) Explain in brief

(i) What is Proof of Work and why does it require energy?

Answer :-

Proof of Work (PoW) is a system used in blockchain networks like Bitcoin to ensure security and consensus. Miners must solve complex mathematical puzzles to validate transactions and add new blocks to the blockchain. This process requires significant computational power and, consequently, a large amount of electricity. The energy-intensive nature of PoW makes it secure but also raises environmental concerns due to high electricity consumption.

(ii) What is Proof of Stake and how does it differ ?

Answer :- Proof of Stake (PoS) is a system used in blockchain networks to validate transactions and add new blocks. Instead of solving complex puzzles like in Proof of Work (PoW), PoS selects validators based on the number of coins they hold and are willing to "stake" as collateral. The more coins a person stakes, the higher their chances of being chosen to validate transactions. This method is more energy-efficient than PoW because it doesn't require massive computational power. For example, Ethereum transitioned to PoS in 2022, reducing its energy consumption by over 99% .

(iii) What is Delegated Proof of Stake and how are validators selected?

Answer :- Delegated Proof of Stake (DPoS) is a system where blockchain users vote for a few trusted delegates to validate transactions and create new blocks. Instead of everyone participating directly, users delegate their voting power to these elected representatives. The more tokens a user holds, the more influence they have in the voting process. Delegates are chosen based on their reputation and performance; if they act dishonestly or fail to perform well, they can be voted out and replaced by others. This system aims to make the blockchain faster and more efficient by limiting the number of active validators.