1)Define blockchain

A blockchain is a decentralized and distributed ledger technology that records transactions across multiple computers in a network in a secure, transparent, and tamper-proof manner. Each record in this system is stored inside a data structure called a block. A block contains important information such as transaction data, the hash of the previous block, a timestamp, a unique number called a nonce, and a Merkle Root. These blocks are linked together to form a continuous, immutable chain. Any modification in a block would require altering all the subsequent blocks, making it nearly impossible to tamper with the data. Cryptographic hashing and decentralized storage ensure the security, authenticity, and transparency of the stored information. Blockchain eliminates the need for intermediaries, making it widely useful in applications like cryptocurrency, digital identity, and supply chain tracking.

➢ Real-life use cases

1️⃣ Supply Chain Management:

Blockchain allows real-time tracking of products from manufacturing to delivery. It increases transparency, verifies authenticity, prevents fraud, and ensures efficiency across each stage of the supply chain.

2️⃣ Digital Identity Management:

Blockchain provides secure digital identity storage. It lets users control access to their personal information while reducing risks of identity theft and simplifying online verification processes for services like banking, healthcare, and voting.

➢ Block Anatomy

1)Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.

- **Data**
- **Previous Hash**
- **Timestamp**
- **Nonce**
- **Merkle Root**

2)Briefly explain how the Merkle root helps verify data integrity (with example)

A **Merkle Root** is a single hash value derived from all the hashes of transactions in a block, organized using a Merkle Tree. This makes it easier to verify the integrity of data quickly without checking each individual transaction.

Example:
If a block contains four transactions: Tx1, Tx2, Tx3, and Tx4:

- First, each transaction is hashed.
- Then, pairs of hashes are combined and hashed again.
- This continues until one final hash (Merkle Root) remains.

If even a single transaction's data changes, its hash will change, altering the Merkle Root. This allows blockchain systems to quickly detect tampering without scanning all transaction data.

➢Consensus Conceptualization

1)What is Proof of Work and why does it required energy?

Proof of Work (PoW) is a consensus mechanism where network participants called miners solve complex mathematical problems to validate transactions and add new blocks to the blockchain. The first

miner to solve the problem gets rewarded.
It requires significant energy because these puzzles involve trial-and-error hashing, where miners must repeatedly guess a nonce value to produce a valid hash below a target value. This process consumes substantial computational resources and electricity.

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

Proof of Stake (PoS) is a consensus mechanism where validators are chosen to create new blocks based on the number of cryptocurrency coins they hold and lock as a stake.
Unlike PoW, it does not involve solving energy-intensive puzzles. Validators with a higher stake have a greater chance of being selected to validate transactions and earn rewards. This system is faster and more energy-efficient than Proof of Work.

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

Delegated Proof of Stake (DPoS) is an improved version of PoS where stakeholders vote to elect a limited number of trusted validators (called delegates) to validate transactions and produce new blocks. Token holders cast votes proportional to their holdings, ensuring validators are accountable to the community. DPoS improves scalability, transaction speed, and decentralization by involving the community in selecting and managing block validators.