Blockchain Basics

Q1: Define blockchain in your own words

A1: A blockchain is a decentralized, distributed, and Permanent digital record.

- It's a continuously growing list of records, called "blocks."
- Blocks are securely linked together using cryptography.
- Each block contains a timestamp, transaction data, and a cryptographic hash of the previous block, creating a tamper-proof chain.
- This decentralized nature means no single entity controls the network, enhancing security and transparency.
- Once a transaction is recorded on the blockchain, it's virtually impossible to alter or tamper, making it highly reliable for tracking data and assets.
- Blockchain also enables smart contracts, which are self-executing agreements that run on the blockchain.
- This system is used in many industries like finance, healthcare, and supply chain to ensure data integrity.

Q2: List 2 real-life use cases (e.g., supply chain, digital identity).

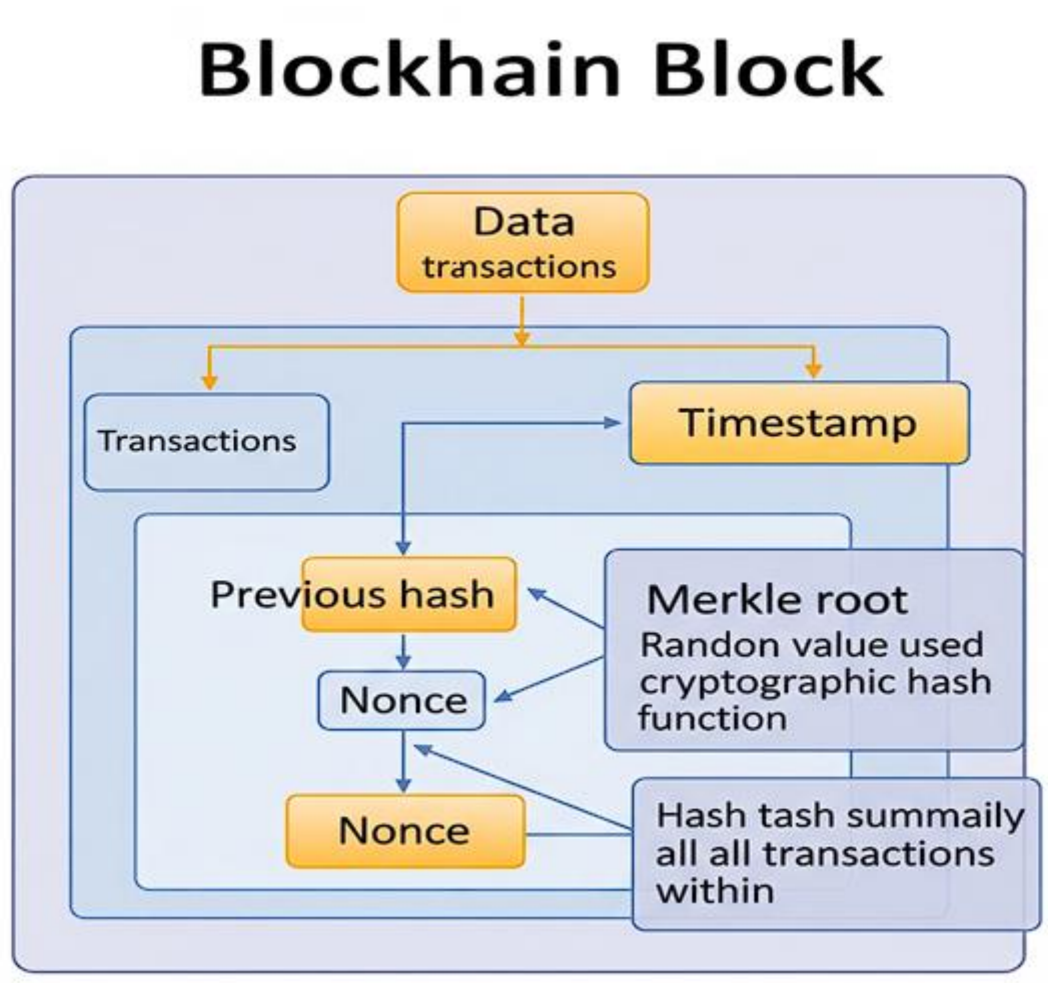
A2:

1. Supply Chain Management:
    - Provides end-to-end transparency in supply chains.
    - Tracks products from origin to consumer.
    - Helps verify authenticity, reduce fraud, and ensure ethical sourcing.
2. Digital Identity:
    - Gives people control over their own digital identities, basically users can control their personal data.
    - Allows users to grant access to specific entities when needed.
    - Enhances privacy and security by reducing dependence on a central source.

Block Anatomy

Q3:Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.

A3:



Q4: Briefly explain with an example how the Merkle root helps verify data integrity.

A4: Merkel root is a single digital fingerprint that represents all transactions inside a block.

- It's the root of a Merkle tree, a binary tree of hashes.
- To create it, individual transactions are hashed.
- Pairs of these hashes are then combined and hashed again.
- This process continues until a single root hash remains.

Example:

- If a block contains four transactions (Tx1, Tx2, Tx3, Tx4), they are first hashed to H1, H2, H3, H4.
- Then, H1 and H2 are hashed together to form H12, and H3 and H4 to form H34.
- Finally, H12 and H34 are hashed to create the Merkle Root.
- If even one transaction (e.g., Tx2) is changed/modified/tampered with, its hash (H2) changes.
- This change in H2 in turn changes H12, and because of that, the entire Merkle Root changes.

- It allows fast and easy confirmation of transactions by just using the Merkle Root.

Consensus Conceptualization

Q5: What is Proof of Work and why does it require energy?

A5: Proof of Work is a consensus mechanism where miners compete to solve a complex computational puzzle to add the next block to the blockchain.

- Miners use a lot of computer power to find a special number called a nonce.
- When this nonce is combined with the block's data and hashed, it produces a hash that meets a predefined difficulty target (e.g., starting with a ‘x’ number of zeros).
- The first miner to find this nonce gets to add the block and earn a reward.
- Mining with PoW takes lots of electricity because of the huge number of calculations miners perform.
- This high energy cost helps protect the network from tampering or getting hacked, keeping it secure.

Q6: What is Proof of Stake and how does it differ?

A6: Proof of Stake is another way to agree on new blocks, where validators are picked based on how much cryptocurrency they lock up. Here “lock up” means “to hold and temporarily freeze cryptocurrency so it can’t be spent or moved”.

- Rather than racing with computers, validators are randomly picked.
- Selection is often weighted by the size of their stake.
- If a validator proposes an invalid block or acts maliciously, they risk losing a portion or all of their staked assets (a process called "slashing").
- Unlike PoW, PoS motivates with money instead of energy costs.
- It requires significantly less energy as it doesn't involve solving complex mathematical puzzles through brute force.

Q7: What is Delegated Proof of Stake and how are validators selected?

A7: Delegated Proof of Stake is a variation of PoS(Proof of Stake) where token holders do not directly validate transactions themselves.

- Rather than everyone participating, they vote for a few delegates(Selected people who make decisions and secure the blockchain) to run the network.
- These elected delegates then take turns creating and validating new blocks.
- The selection of validators is primarily based on their popularity among token holders, who can vote for or against delegates at any time.
- This system aims to achieve faster transaction speeds and greater scalability compared to traditional PoS, as fewer participants are involved.
- If a delegate misbehaves, they can be voted out by the community.