Blockchain Basics

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

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

Ans - A blockchain is a distributed digital ledger that securely stores transactions on multiple computers in such a manner that altering them is impossible. It is made up of a sequence ofconnected blocks, each with information, a timestamp, and a cryptographic hash of the previous block. By having this chain formation, data integrity and transparency are guaranteed. Once data is stored on a blockchain, it is practically impossible to modify without modifying all subsequent blocks, rendering it extremely secure from tampering and fraud. Since it is kept by several participants (nodes), blockchain does away with the requirement for a central authority, allowing trustless and open record-keeping in a range of applications.

Supply Chain Management: Blockchain tracks the origin, processing, and shipping of products transparently, reducing fraud and ensuring authenticity.

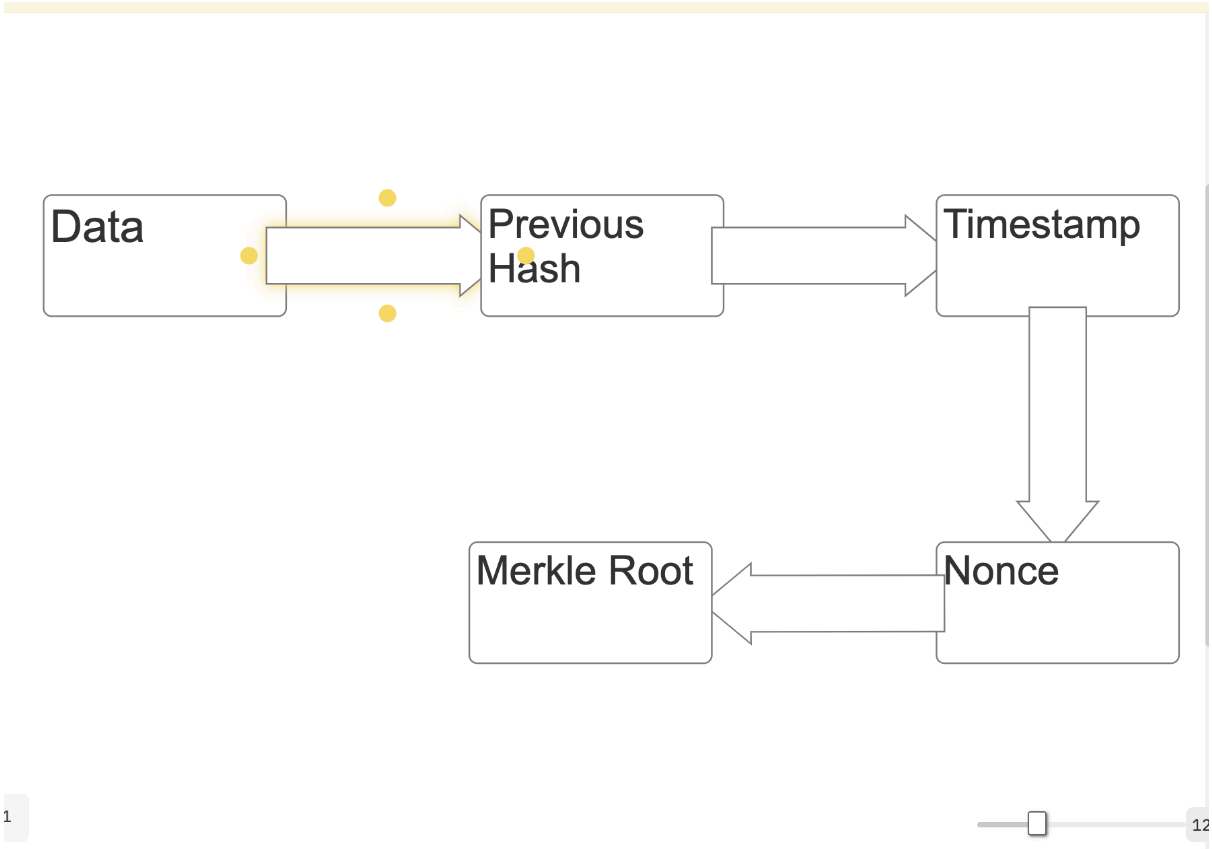
Digital Identity Verification: Blockchain enables secure and self-sovereign identity management, allowing individuals to control their personal data without relying on centralized databases.

Block Anatomy

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

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

Ans -



The **Merkle root** is a single hash derived from all transaction hashes in a block, organized in a binary tree structure called a Merkle tree. This structure allows efficient and secure verification of data integrity. For example, if one transaction changes, its hash will change, which cascades up to the Merkle root, making it different from the original. This helps nodes quickly verify whether a transaction is part of the block without checking all data individually.

3.

e.

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

Proof of Work (PoW) is a consensus mechanism where miners solve complex mathematical puzzles by repeatedly hashing data with different nonces until a hash meets a difficulty target (e.g., starts with a certain number of zeros). This process requires significant computational power and energy because many attempts are needed before finding a valid hash. PoW secures the network by making it costly to alter the blockchain, thus deterring attacks.

What is Proof of Stake and how does it differ?

Proof of Stake (PoS) is a consensus method where validators are chosen to create new blocks based on the number of coins they hold and are willing to "stake" as collateral. Unlike PoW, PoS doesn’t require energy-intensive computations, making it more energy-efficient. Validators are incentivized to act honestly because they risk losing their staked coins if they behave maliciously.

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

Delegated Proof of Stake (DPoS) is a variation of PoS where coin holders vote to elect a small group of trusted delegates (validators) who are responsible for validating transactions and producing blocks. Validators are selected based on the votes they receive. This approach increases efficiency and scalability but involves a degree of centralization compared to PoW or PoS.