1. **Blockchain Basics**

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

Blockchain is an innovative, decentralized method of sharing data that can ensure secure, transparent, and immutable information sharing over a distributed network.

Data is stored in a block that is linked in succession to other blocks. Each block consists of an encrypted hash, a timestamp, and transaction information that collectively mean each record is immutable, meaning the data cannot be altered or deleted unless the entire network agrees to the change.

This technology has many applications in businesses where multiple parties need to share the same data reliably without the involvement of a central authority.

Built-in elements of cryptographic storage and consensus can disallow any changes and ensure each party maintains the same shared view of the same ledger.

Blockchain is often deployed to track transactions such as orders, payments, and account changes, and is most beneficial to industries that require data integrity, discoverability, and transparency.

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

Supply Chain (Walmart):

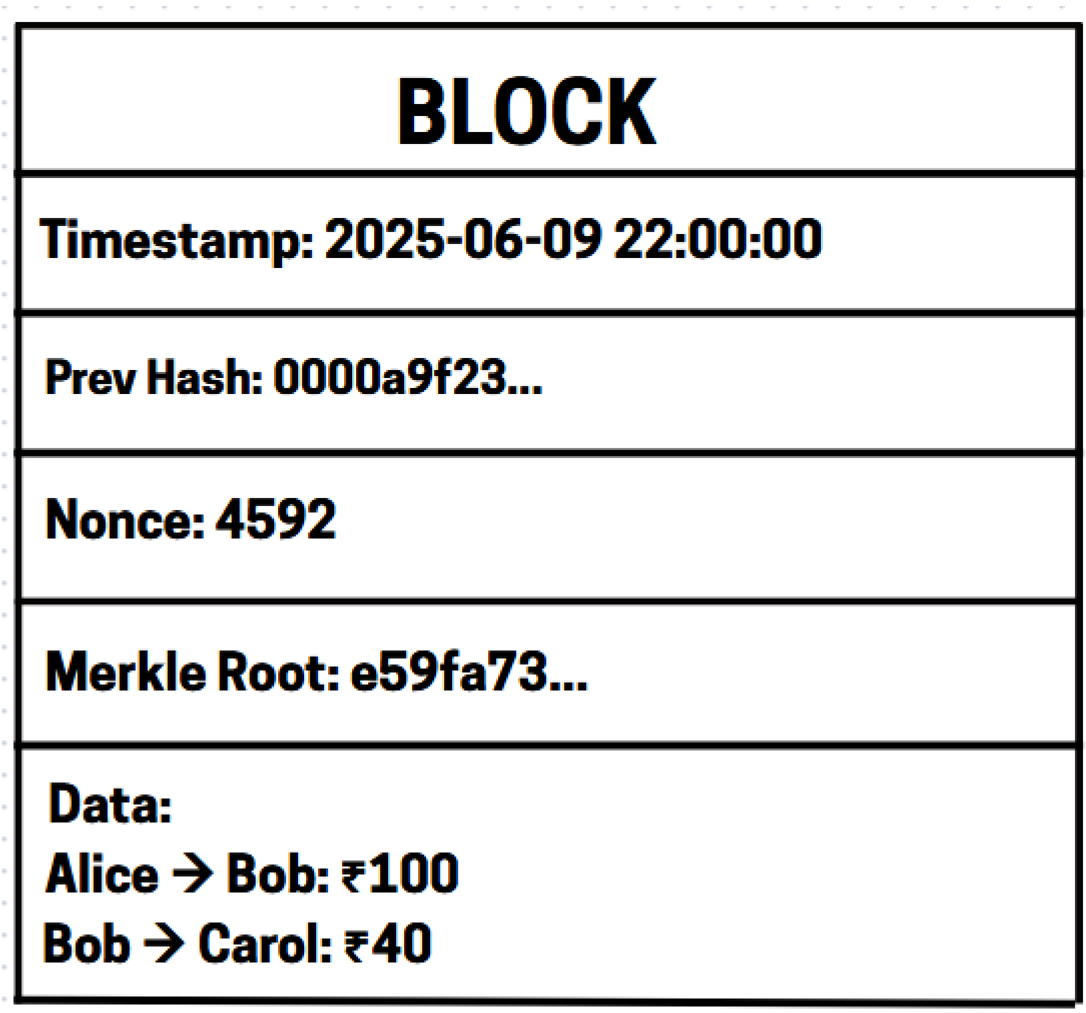
Walmart uses blockchain to track leafy greens from seed to shelf. It ensures food safety and can trace the origin of products like sliced mangoes in seconds, instead of days.

Digital Identity (QuarkID):

Buenos Aires launched QuarkID, a blockchain-based system that gives residents secure, private digital identities, allowing access to services while keeping full control of personal data.

1. **Block Anatomy**

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



BLOCK

Timestamp: 2025-06-09 22:00:00

Prev Hash: 0000a9f23...

Nonce: 4592

Merkle Root: e59fa73...

Data:
Alice → Bob: ₹100
Bob → Carol: ₹40

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

- A Merkle Root is the top hash of a Merkle Tree, a data structure used in blockchains to ensure data integrity and efficient verification.
- In this tree, each leaf node is the hash of a transaction, and each non-leaf node is the hash of its two child hashes.
- This continues upward until a single root hash—the Merkle Root—is formed.
- If any transaction changes, its hash will also change, which affects the parent hashes all the way up to the root.
- So, if the Merkle Root changes, it means some data was tampered with—thus verifying integrity.

  Example:

  - In Bitcoin, to check if a transaction exists in a block, you don't need to check every transaction.
  - Instead, you only verify the path of hashes from that transaction up to the Merkle Root.
  - If the computed root matches the one stored in the block, the transaction is valid and untampered.

2. **Consensus Conceptualization**

- **Explain in brief (4–5 sentences each):**

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

1. Proof of Work (PoW) is a consensus mechanism used in blockchains like Bitcoin to validate transactions and add new blocks.
2. It requires miners to solve complex mathematical puzzles using powerful computers.
3. The first miner to solve the puzzle gets to add the block and earn a reward, such as cryptocurrency tokens.
4. This process is computationally intensive and requires a large amount of electricity.
5. The high energy use makes the network secure, as altering the blockchain would require an enormous amount of computing power.

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

1. Proof of Stake (PoS) is a consensus mechanism that selects validators based on how many tokens they own and stake, rather than computational power.
2. Validators are chosen to verify transactions and create new blocks, earning rewards for their service.
3. Unlike PoW, PoS is energy-efficient and more environmentally friendly since it doesn't require solving complex puzzles.
4. If validators act maliciously, they risk losing a part of their staked tokens. PoS is also more scalable, making it suitable for blockchains that handle high transaction volumes.

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

1. Delegated Proof of Stake (DPoS) is an improved version of PoS where token holders vote to elect a small group of delegates (validators) to manage the blockchain.
2. These elected delegates are responsible for validating transactions and producing blocks.
3. The more tokens a user holds, the more voting power they have in the election process.
4. This system enhances speed and scalability by limiting the number of active validators while promoting democratic participation.
5. DPoS is also energy-efficient and used in networks like EOS, Steem, and BitShares.