Q1.Define blockchain in your own words (100-150 words).

Ans:A blockchain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

This ledger is shared across a network of computers (nodes), and additions require collective agreement, known as consensus. Because copies exist on many nodes and each block references the one before it, the system becomes exceptionally resistant to changes or tampering. Blockchain enables secure, transparent, and decentralized record-keeping without relying on a single central authority. While famously used by cryptocurrencies like Bitcoin, it’s also applied in areas like supply chains, digital identities, and smart contracts.

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

Ans: Here are two real-world use cases of blockchain technology:

1.Supply Chain Tracking & Transparency:-

Blockchain provides a tamper-proof ledger of product journeys from origin to consumer, enhancing accountability and traceability.

Food & perishables example: Walmart, in partnership with IBM, leverages its Food Trust Network to trace items like mangoes and leafy greens in just seconds. This expedites contamination responses and reduces waste

Luxury & commodities example: Companies like De Beers and Everledger use blockchain to track diamonds from mine to market, ensuring each stone's authenticity and ethical sourcing

2. **Digital Identity & Credentials:-**

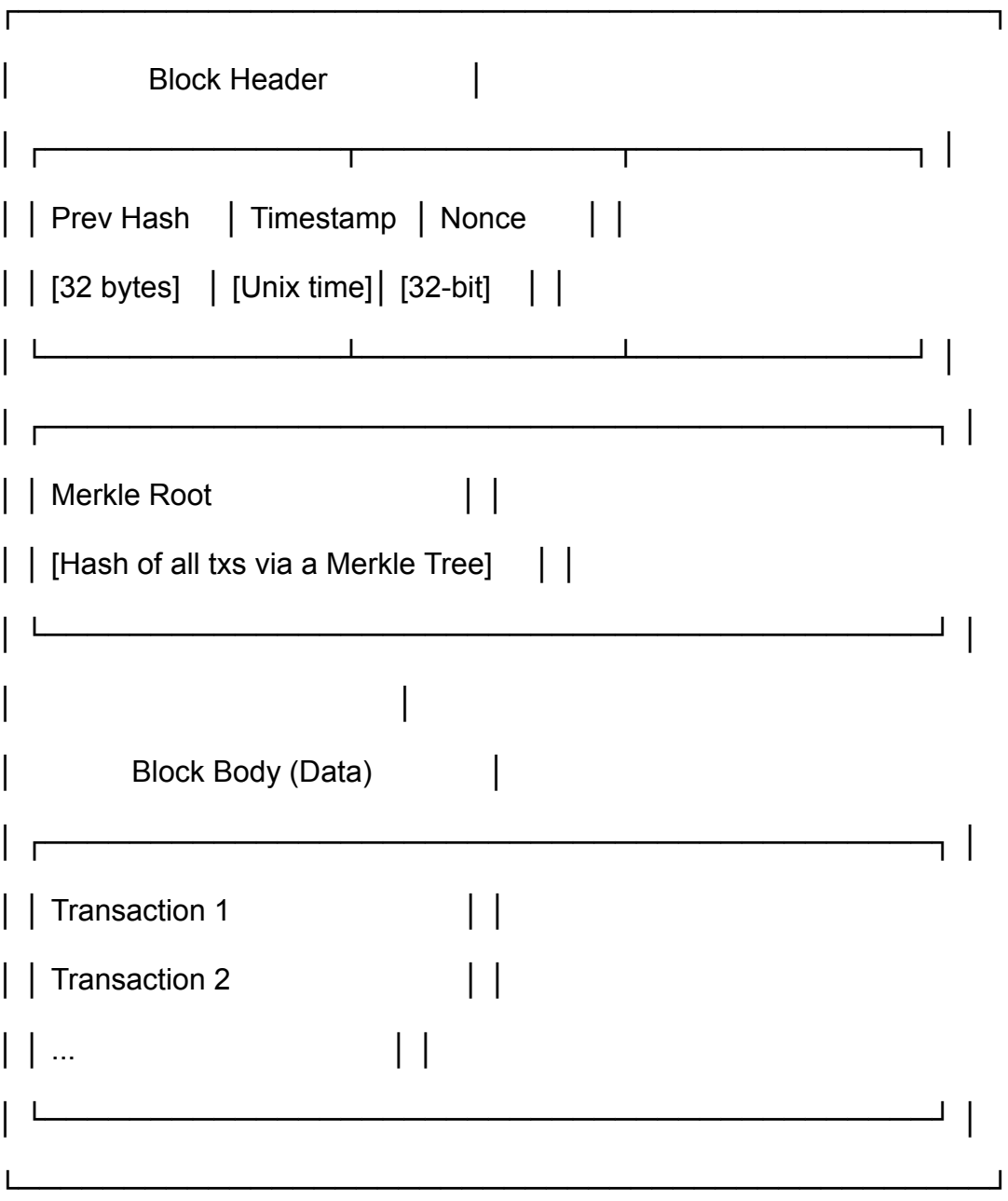
Blockchain enables secure, user-controlled identities and certifications, reducing fraud and improving data privacy.

National ID systems: China launched its RealDID framework in December 2023—a blockchain-based decentralized identifier system that supports secure personal identity verification across services

Education credentials: The Cardano blockchain, through its Atala identity solution, is used to issue and verify academic credentials—for instance, verifying university records in Georgia and Ethiopia

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

Ans:Here's a clear and simple ASCII-style diagram of a blockchain block displaying its main components—**Data**, **Previous Hash**, **Timestamp**, **Nonce**, and **Merkle**



Component breakdown:

- **Previous Hash**: Links this block to its predecessor—securing the chain integrity via cryptographic pointers. Without it, the sequence would break
- **Timestamp**: Records when the block was created, used for ordering and timestamping purposes .

- **Nonce**: A random 32-bit number miners adjust to meet the Proof-of-Work requirement—critical for mining validity.

- **Merkle Root**: A single hash representing all transactions in the block, enabling efficient integrity checks without inspecting every transaction.

- **Data (Transactions)**: The actual content—such as cryptocurrency transactions or supply chain logs.

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

A **Merkle root** ensures data integrity by acting like a digital fingerprint for a whole set of data. Here's a simple example :

How It Works

1. **Leaf hashes**: Suppose you have items A, B, C, and D. First, hash each one to get:
    - H(A), H(B), H(C), H(D)
2. **Parent hashes**: Pair them up and hash the concatenations:
    - H(AB) = hash(H(A) // H(B)), H(CD) = hash(H(C) // H(D))
3. **Merkle root**: Hash the parent hashes:
    - Root = hash(H(AB) // H(CD))

This single root hash now cryptographically represents all four item.

Verifying a Single Item (Example)

You only want to verify that **item B** is intact, without downloading A, C, D.

1. Compute **H(B)**.
2. Get a **Merkle proof**: a small set of hashes—here, H(A), H(CD)—needed to trace B's branch up to the root
3. Recreate the hashes:
    - Compute H(AB) = hash(H(A) // H(B))

- Then compute Root' = hash(H(AB) // H(CD))

4. Compare Root' with the known Merkle root:
    - If they match, B is **verified**—unaltered and included in the original dataset.
    - If not, the data integrity has failed

Q5.Explain in brief (4–5 sentences each):
What is Proof of Work and why does it require energy?
What is Proof of Stake and how does it differ?
What is Delegated Proof of Stake and how are validators selected?

Ans:**Proof of Work (PoW)** is a consensus mechanism used primarily in blockchains like Bitcoin. It ensures that all participants agree on the transaction history without needing a central authority. Here's how it works—and why it uses so much energy.

It relies on brute-force hash puzzles requiring vast electricity and hardware to keep the network secure.

In PoS, participants—called **validators**—lock up (stake) a certain amount of the blockchain's native cryptocurrency to participate in block validation. The selection process is typically random, weighted by how much they stake.

Both consensus models offer robustness, but PoS achieves similar security **more sustainably** while reducing entry barriers, supporting faster transactions, and enabling scalability improvements (like sharding).

Delegated Proof of Stake (DPoS) is a governance-driven, energy-efficient consensus mechanism that builds on PoS by enabling token holders to **elect** a small group of trusted delegates (often called witnesses or block producers), who then validate transactions and create blocks on behalf of the network.

Validator Selection Process

Voting Power = Stake
Delegates are ranked based on the total tokens staked *for* them. The top N delegates form the active validator group .
Reputation & Performance Matter
Delegates earn trust and votes by delivering high uptime, reliable performance, and transparent communication .

Reward Sharing
Many delegates distribute a portion of block rewards back to voters, creating a direct financial incentive to support them .

Continuous Accountability

Because delegates can be voted out at any time, there's strong motivation to act correctly and avoid penalties such as missing blocks or getting slashed