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

A blockchain is a decentralized, append-only digital ledger that records data in a series of linked blocks. Each block is cryptographically connected to the previous one, which guarantees both immutability and transparency.

Rather than relying on a central authority, blockchain employs distributed consensus mechanisms such as Proof of Work or Proof of Stake to validate transactions.

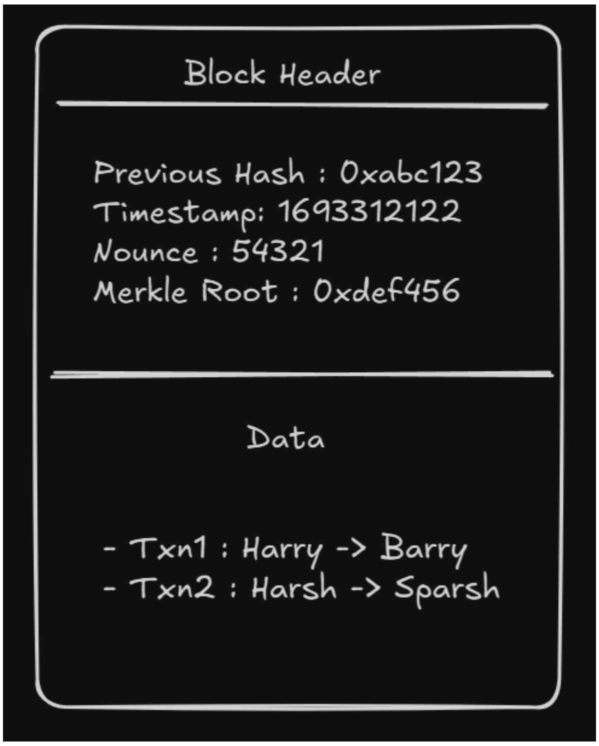
This design enhances resistance to tampering, censorship, and single points of failure. Once data is recorded on the blockchain, it becomes nearly impossible to alter without the consent of the entire network, fostering trust in environments where participants may not know or trust one another.

2. List 2 real-life use cases.

a. Healthcare Data Management : Blockchain enables secure sharing of medical records between hospitals, patients, and insurers. It ensures data integrity, prevents tampering, and allows patients to control who accesses their information.

b. Intellectual Property & Copyright Protection : Creators can register their work (music, art, code) on a blockchain to timestamp ownership and licensing terms. This provides proof of creation and helps track unauthorized use or plagiarism.(Eg: NFTs)

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



Block Header

Previous Hash : 0xabc123
Timestamp: 1693312122
Nounce : 54321
Merkle Root : 0xdef456

Data

- Txn1 : Harry -> Barry
- Txn2 : Harsh -> Sparsh

4. Briefly explain with an example how the Merkle root helps verify data integrity.
A Merkle root is a hash representing all transactions in a block. Each transaction is hashed, then pairs of hashes are combined and hashed repeatedly until a single root hash is formed.
Example:
If Tx1 = A and Tx2 = B, then Merkle root = hash(hash(A) + hash(B)).
If someone alters Tx1, the Merkle root changes, alerting the system to tampering. This makes data verification efficient without checking every single transaction.

5. What is Proof of Work and why does it require energy?
PoW requires miners to solve a complex mathematical puzzle (hashing) to add a block.
Solving it takes substantial computational power and electricity, which secures the network against spam and attacks. The energy cost makes tampering economically unviable.

6. What is Proof of Stake and how does it differ?
In PoS, validators are chosen to propose blocks based on the amount of cryptocurrency they "stake" as collateral.
It's more energy-efficient than PoW since it doesn't require intensive computation, and malicious behavior risks losing the staked amount.

7. What is Delegated Proof of Stake and how are validators selected?
DPoS involves token holders voting for a limited number of trusted delegates who produce blocks and validate transactions.
Validators are selected by reputation and vote weight, promoting faster consensus but with more centralization risk.