PART A
I) a)
Decentralization:
Blockchain operates on a peer-to-peer network where no single authority controls the data. Each node holds a copy of the ledger, enabling transparency and eliminating the need for intermediaries.

Immutability:
Once data is recorded in a block and added to the chain, it cannot be altered or deleted without consensus from the network. This ensures data integrity and builds trust.

Transparency:
All participants in a public blockchain network can view and verify transactions. This openness enhances accountability and trust among users.

b)
Advantages of Centralized Networks:

Faster decisions due to centralized authority.

Controlled access to data and resources.

Disadvantages:
Single point of failure can compromise the entire network.

Harder to coordinate with increasing network size and complexity.

c)
- Bitcoin uses blockchain by recording every transaction into blocks. (0.5 marks)
- These blocks are linked using cryptographic hashes (0.5 marks)
- validated by a network of miners using Proof of Work (PoW) (0.5 marks)
- Once validated, the block is added to the blockchain, making the transaction permanent and tamper-proof. (0.5 marks)

d)
- Proof of Work requires solving computational puzzles, while Proof of Stake selects validators based on stake. (1.5 marks)
- PoW is energy-intensive; PoS is more energy-efficient and scalable. (1.5 marks)

e)
CAP theorem : a distributed system cannot have consistency , availability and partition tolerance at the same time.(3 marks)

f)
The Merkle root summarizes all transactions in a block. It ensures data integrity and allows efficient and secure
verification of transactions without revealing all data. (3 marks)

g)

A decentralized ledger is a database that is consensually shared and synchronized across multiple sites, institutions, or
geographies, reducing the risk of centralized failure. (3 marks)

h)
A Distributed Ledger is a database held and updated independently by each participant (or node) in a large network.
Blockchain is a type of distributed ledger. (3 marks)

PART B
II)
Blockchain types:
1. Public: Fully decentralized, open to all. (2 marks)
2. Private: Central authority controls access.(2 marks)
3. Consortium: Controlled by a group. (2 marks)
Comparison:
- Security: Public is most secure via consensus; private relies on internal mechanisms. (2 marks)
- Scalability: Private chains scale better. (2 marks)
- Decentralization: Public > Consortium > Private. (2 marks)
III)
Centralized:
- High scalability (1 mark)
- low fault tolerance and security. (1 mark)
- Centralized networks are simpler but vulnerable to failure. (1 mark)
Decentralized:
- High fault tolerance and security (1 mark)
- lower scalability. (1 mark)
- Decentralized/distributed networks improve fault tolerance and security. (1 mark)
Distributed:
- Best balance with multiple nodes and redundancy (1.5 marks)
- Trade-offs exist in complexity, coordination, and cost. (1.5 marks)
IV)
Consensus Mechanisms:
A consensus mechanism is a protocol through which blockchain nodes agree on a single version of the truth (i.e., valid transactions).
- Proof of Work (PoW):
Used by Bitcoin. (1 mark)
requires computation (mining). (1 mark)
Energy-intensive and slow. (1 mark)
High security but low efficiency. (1 mark)
- Proof of Stake (PoS):
Chooses validators based on stake. (1 mark)
Validators are chosen based on the amount of cryptocurrency they stake. (1 mark)
Used by Ethereum 2.0. (1 mark)
Energy-efficient and faster than PoW.(1 mark)
- Delegated Proof of Stake (DPoS):
Stakeholders vote for a limited number of delegates to validate blocks. (1 mark)
Extremely scalable and fast. (1 mark)
Less decentralized, vulnerable to cartelization. (1 mark)

Stakeholders elect delegates to validate blocks. (1 mark)

V)
Key Components of a Blockchain Transaction:

Transaction Data: Includes sender and receiver addresses, amount of cryptocurrency or digital asset, and optional metadata. (2 marks)

Digital Signature: Ensures that the transaction is authorized by the sender using their private key. (2 marks)

Transaction Hash: A unique identifier generated by hashing the transaction data. Used for reference and integrity checks. (2 marks)

Timestamp: The exact date and time when the transaction was initiated. (2 marks)

Nonce: A random or sequential number added to ensure the transaction hash is unique. (2 marks)

Block Reference: Once validated, the transaction is added to a block and inherits the block's hash and position in the chain. (2 marks)

VI)
Ethereum Ecosystem Components:
1. Smart Contracts (2 marks)
2. Ethereum Virtual Machine (EVM) (2 marks)
3. Wallets (e.g., MetaMask) (2 marks)
4. Development Tools (Remix, Truffle, Ganache) (2 marks)
5. Nodes/Clients (Geth, OpenEthereum) (2 marks)
6. Ethereum Tokens (ERC-20, ERC-721) (2 marks)

VII)
Function modifiers in Solidity are used to change the behavior of functions. They help in restricting access, validating conditions, or automating repetitive tasks. (2 marks)

Types of Modifiers:
1. onlyOwner: (1 mark)
   - Restricts function execution to the contract owner. (1 mark)
   - Use case: Admin functionalities like pausing the contract or changing ownership. (1 mark)

2. view: (1 mark)
   - Declares that the function will not modify the blockchain state. (1 mark)
   - Use case: Fetching data like balance or contract variables. (1 mark)

3. pure: (1 mark)
   - Declares that the function neither reads nor modifies the state. (1 mark)
   - Use case: Utility functions like math calculations. (1 mark)

4. payable: (1 mark)
   - Marks the function as capable of receiving Ether. (1 mark)
   - Use case: Accepting payments or donations. (1 mark)

VIII)
Hyperledger Reference Architecture Components:

1. Consensus Layer:
   - Responsible for validating and agreeing upon the order of transactions. (1.5 marks)

2. Smart Contract Layer (Chaincode):
   - Contains the business logic written in languages like Go, Java, or Node.js. (1.5 marks)

3. Communication Layer:
   - Provides secure communication between peers in the network. (1.5 marks)

4. Data Store Layer:
   - Maintains the ledger and state databases (LevelDB/CouchDB). (1.5 marks)

5. Identity Services:
   - Manages digital identities using Public Key Infrastructure (PKI). (1.5 marks)

6. APIs and SDKs:
   - Used by developers to interact with the blockchain network. (1.5 marks)

7. Security and Privacy Module:
   - Ensures encryption, access control, and data privacy. (1.5 marks)
- Diagram (1.5 marks)

IX)
Types of Blockchain Attacks:

1. 51% Attack:(0.5 marks)
   - An attacker controls the majority of the network hash rate.
   - Impact: Double spending, halting network operations, loss of trust.

2. Sybil Attack:(0.5 marks)
   - Fake nodes flood the network to gain influence.
   - Impact: Disrupts consensus, network manipulation.

3. Replay Attack:(0.5 marks)
   - Reusing a transaction from one chain on another.
   - Impact: Unauthorized transactions.

4. Smart Contract Vulnerabilities:(0.5 marks)
   - Bugs or backdoors in contracts (e.g., DAO hack).
   - Impact: Fund theft, data manipulation.

5. Routing Attacks:(0.5 marks)
   - Hijacking network traffic between nodes.
   - Impact: Delayed or blocked transactions.

6. Timejacking Attack:(0.5 marks)
   - Manipulating node clocks to influence consensus.
   - Impact: Forks, transaction delays.

Impact on Security and Trust:
- Loss of funds and data.(1.5 mark)
- Network instability and hard forks.(1.5 mark)
- Erosion of user trust in the platform.(1.5 mark)

Mitigation Strategies:
- Strong consensus mechanisms (PoS, DPoS).(1.5 mark)
- Regular smart contract audits.(1.5 mark)
- Multi-factor authentication.(1.5 mark)