

PART A

I)

(a)Decentralization:(Total: 3 marks)

-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. (Total: 1 marks)

-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.(Total: 1 marks)

-Transparency:

All participants in a public blockchain network can view and verify transactions. This openness enhances accountability and trust among users.(Total: 1 marks)

b)Advantages of Centralized Networks: (Total: 3 marks)

-Faster decisions due to centralized authority.(Total: 0.75 marks)

-Controlled access to data and resources.(Total: 0.75 marks)

Disadvantages:

-Single point of failure can compromise the entire network.(Total: 0.75 marks)

-Harder to coordinate with increasing network size and complexity. (Total: 0.75 marks)

c)Bitcoin uses blockchain by recording every transaction into blocks.(Total: 3 marks)

- These blocks are linked using cryptographic hashes (Total: 1 marks)

- validated by a network of miners using Proof of Work (PoW) (Total: 1 marks)

- Once validated, the block is added to the blockchain, making the transaction permanent and tamper-proof. (Total: 1 marks)

d)Proof of Work requires solving computational puzzles, while Proof of Stake (Total: 3 marks)

- selects validators based on stake. (Total: 1.5 marks)

- PoW is energy-intensive; PoS is more energy-efficient and scalable. (Total : 1.5 marks)

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

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

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

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

PART B

II)Blockchain types:(Total: 12 marks)

- Public: Fully decentralized, open to all. (Total :2 marks)

- Private: Central authority controls access.(Total:2 marks)

- Consortium: Controlled by a group. (Total: 2 marks)
- Comparison:
 - Security: Public is most secure via consensus; private relies on internal mechanisms. (Total: 2 marks)
 - Scalability: Private chains scale better. (Total: 2 marks)
 - Decentralization: Public > Consortium > Private. (Total: 2 marks)

III) Centralized: (Total: 12 marks)

- High scalability (Total: 1 marks)
- low fault tolerance and security. (Total: 1 marks)
- Centralized networks are simpler but vulnerable to failure. (Total: 1 marks)

Decentralized:

- High fault tolerance and security (Total: 1 marks)
- lower scalability. (Total: 1 marks)
- Decentralized/distributed networks improve fault tolerance and security. (Total: 1 marks)

Distributed:

- Best balance with multiple nodes and redundancy (Total: 3 marks)
- Trade-offs exist in complexity, coordination, and cost. (Total :3 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) (Total :1 marks)
- Used by Bitcoin. (Total :1 marks)
- requires computation (mining). (Total :1 marks)
- Energy-intensive and slow. (Total :1 marks)
- High security but low efficiency. (Total :1 marks)

Proof of Stake (PoS):

- Chooses validators based on stake. (Total :1 marks)
- Validators are chosen based on the amount of cryptocurrency they stake. (Total :1 marks)
- Used by Ethereum 2.0. (Total :1 marks)
- Energy-efficient and faster than PoW. (Total :1 marks)
- Delegated Proof of Stake (DPoS):
 - Stakeholders vote for a limited number of delegates to validate blocks. (Total :1 marks)
 - Extremely scalable and fast. (Total :1 marks)
 - Less decentralized, vulnerable to cartelization. (Total :1 marks)

Stakeholders elect delegates to validate blocks.

V) Key Components of a Blockchain Transaction: (Total :12 marks)

- Transaction Data: Includes sender and receiver addresses, amount of cryptocurrency or digital asset, and optional metadata. (Total :2 marks)
- Digital Signature: Ensures that the transaction is authorized by the sender using their private key. (Total :2 marks)

Transaction Hash: A unique identifier generated by hashing the transaction data.

- Used for reference and integrity checks. (Total :2 marks)
- Timestamp: The exact date and time when the transaction was initiated. (Total :2 marks)
- Nonce: A random or sequential number added to ensure the transaction hash is unique. (Total :2 marks)
- Block Reference: Once validated, the transaction is added to a block and inherits the block's hash and position in the chain. (Total :2 marks)

VI) Ethereum Ecosystem Components: (Total :12 marks)

- Smart Contracts (Total :2 marks)
- Ethereum Virtual Machine (EVM) (Total :2 marks)

- Wallets (e.g., MetaMask) (Total :2 marks)
- Development Tools (Remix, Truffle, Ganache) (Total :2 marks)
- Nodes/Clients (Geth, OpenEthereum) (Total :2 marks)
- Ethereum Tokens (ERC-20, ERC-721) (Total :2 marks)

VII)Function modifiers in Solidity are used to change the (Total:12 marks) behavior of functions.

-They help in restricting access, validating conditions, or automating repetitive tasks. (Total:1 marks)

Types of Modifiers:

- onlyOwner: (Total:1 marks)
 - Restricts function execution to the contract owner. (Total:1 marks)
 - Use case: Admin functionalities like pausing the contract or changing ownership. (Total:1 marks)
- view: (Total:1 marks)
 - Declares that the function will not modify the blockchain state. (Total:1 marks)
 - Use case: Fetching data like balance or contract variables. (Total:1 marks)
- pure: (Total:1 marks)
 - Declares that the function neither reads nor modifies the state.(Total:1 marks)
 - Use case: Utility functions like math calculations.(Total:1 marks)
- payable:
 - Marks the function as capable of receiving Ether. (Total:1 marks)
 - Use case: Accepting payments or donations.(Total:1 marks)

VIII)Hyperledger Reference Architecture Components: (Total:12 marks)

- Consensus Layer:
 - Responsible for validating and agreeing upon the order of transactions.(Total:1.5 marks)
- Smart Contract Layer (Chaincode):
 - Contains the business logic written in languages like Go, Java, or Node.js.(Total:1.5 marks)
- Communication Layer:
 - Provides secure communication between peers in the network. (Total:1.5 marks)-
- Data Store Layer:
 - Maintains the ledger and state databases (LevelDB/CouchDB). (Total:1.5 marks)
- Identity Services:
 - Manages digital identities using Public Key Infrastructure (PKI). (Total:1.5 marks)
- APIs and SDKs:
 - Used by developers to interact with the blockchain network. (Total:1.5 marks)
- Security and Privacy Module:
 - Ensures encryption, access control, and data privacy. (Total:1.5 marks)
- Diagram (Total:1.5 marks)

IX)Types of Blockchain Attacks: (Total :12 marks)

- 51% Attack:(Total:1.5 marks)
 - An attacker controls the majority of the network hash rate.
 - Impact: Double spending, halting network operations, loss of trust.
- Sybil Attack:(Total:1.5 marks)
 - Fake nodes flood the network to gain influence.
 - Impact: Disrupts consensus, network manipulation.
- Replay Attack:(Total:1.5 marks)
 - Reusing a transaction from one chain on another.
 - Impact: Unauthorized transactions.
- Smart Contract Vulnerabilities:(Total:1.5 marks)
 - Bugs or backdoors in contracts (e.g., DAO hack).
 - Impact: Fund theft, data manipulation.
- Routing Attacks:(Total:1.5 marks)

- Hijacking network traffic between nodes.
- Impact: Delayed or blocked transactions.
- Timejacking Attack:(Total:1.5 marks)
- Manipulating node clocks to influence consensus.
- Impact: Forks, transaction delays.

Impact on Security and Trust:

- Loss of funds and data.(Total:1.5 marks)
- Network instability and hard forks.
- Erosion of user trust in the platform.

Mitigation Strategies:

- Strong consensus mechanisms (PoS, DPoS).(Total:1.5 marks)
- Regular smart contract audits.
- Multi-factor authentication.