PART A

I.

(a) Decentralization:

Blockchain operates on a peer-peer network where no single authority controls the data. Each node holds a copy of the ledger.

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.

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.

These blocks are linked using cryptographic hashes.

Each new block is validated by a decentralized network of miners.

Uses the Proof of Work (PoW) consensus mechanism.

d)Proof of Work (PoW) requires miners to solve complex puzzles, consuming more energy. Proof of Stake (PoS) selects validators based on stake, which is energy-efficient and faster.

e)CAP theorem states that a distributed system cannot have consistency , Availability and partition tolerance simultaneously.

f)Merkle root helps verify data integrity in a block. Any change in a transaction alters the root, making tampering detectable.

g)A decentralized ledger is a digital system where data is stored across multiple nodes, eliminating the need for a central authority.

h)A Distributed Ledger is a consensus of replicated, shared, and synchronized digital data spread across multiple sites, countries, or institutions. Blockchain is a distributed ledger.

PART B

II)Types of Blockchain:

- Public Blockchain:

Open to everyone. Anyone can join and participate in the network.

Highly decentralized. Example: Bitcoin, Ethereum.

Uses consensus protocols like Proof of Work or Proof of Stake.

Pros: Transparency, security, and community-driven.

Cons: Slower transactions, scalability issues.

- Private Blockchain:

Controlled by a single organization. Only selected participants can join.

Used for internal operations. Example: Hyperledger Fabric.

Pros: Faster, more efficient.

Cons: Less decentralized, more vulnerable to manipulation.

- Consortium Blockchain:

Controlled by a group of organizations (consortium).

Balanced decentralization and scalability.

Used in banking, supply chains (e.g., R3 Corda).

Pros: Trust among known participants, performance.

Cons: Governance complexity.

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).It is based on three concepts: i)Proof of Work (PoW): Proof of Work is Used by Bitcoin.

The Miners solve complex puzzles to validate transactions and create new blocks. It is Energy-intensive and slow. It offers High security but low efficiency.

ii) Proof of Stake (PoS): In PoS, Validators are chosen based on the amount of cryptocurrency they stake. It is Used by Ethereum 2.0. PoS is Energy-efficient and faster than PoW.

Its Security depends on economic incentives. iii) Delegated Proof of Stake (DPoS): In DPos, Stakeholders vote for a limited number of delegates to validate blocks.

It is Used by EOS, TRON. They are Extremely scalable and fast and Less decentralized, vulnerable to cartelization.

V)Sender (or Payer): The entity that initiates the transaction by sending cryptocurrency or data. This is usually represented by a public key or address.

Receiver (or Payee): The entity that receives the cryptocurrency or data. Like the sender, the receiver is identified by a public key or address.

Transaction Amount: The quantity of cryptocurrency or digital assets being transferred. In the case of data transactions, this might refer to the amount of data being sent or stored.

Timestamp: The exact time when the transaction was created or initiated. This helps to ensure the chronological order of transactions on the blockchain.

Transaction Fees: A fee that is paid to incentivize miners or validators to include the transaction in the blockchain. The fee amount may vary depending on network congestion or the size of the transaction.

Transaction Data: The data associated with the transaction. For cryptocurrency transactions, this could be the amount of cryptocurrency being sent, the digital signature, and other relevant metadata.

Signature (Digital Signature): A cryptographic signature generated by the sender’s private key. It ensures the authenticity and integrity of the transaction by proving that it came from the legitimate sender.

Transaction ID (Hash): A unique identifier for the transaction, which is typically the hash of the transaction data. This hash is used to identify and track the transaction on the blockchain.

Input and Output:

Input: Refers to the source of the funds being spent. It usually contains a reference to a previous transaction output that the sender has the right to spend.

Output: The destination for the transferred funds, typically referencing the receiver’s public key.

VII)Mining in Blockchain:

Mining is the process of verifying blockchain transactions and adding them to the public ledger (blockchain).

Functions:

Secures the network by validating transactions.

Prevents double spending.

Introduces new cryptocurrency into circulation.

Mining Process (PoW example):

Transactions are grouped into a block.

Miners compete to solve a complex cryptographic puzzle.

The first to solve it gets to add the block and is rewarded with coins.

Other nodes verify the solution and accept the block.

Hardware Used:

Initially CPUs, later GPUs, and now specialized ASICs.

Types of Mining: Solo mining: Individual miner tries to solve blocks alone.

Pool mining: Group of miners combine resources and share rewards.

Cloud mining: Renting mining power from data centers.

Environmental Impact:

PoW consumes large amounts of electricity.

PoS and other alternatives are more sustainable.

IX)Double Spending in Blockchain:

Double spending occurs when the same digital currency is spent more than once. This is a serious problem in digital cash systems.

Why It’s a Problem:

Digital data can be copied.

Without prevention, users could replicate tokens and spend them multiple times.

How Blockchain Prevents It:

Every transaction is broadcast to the entire network.

Transactions are verified and recorded in blocks through consensus.

Once a transaction is confirmed and added to the chain, it becomes immutable.

Network nodes reject conflicting transactions.

Common Double Spending Attacks:

Race Attack: Two conflicting transactions are sent simultaneously.

Finney Attack: A pre-mined block with a transaction is withheld and later released.

51% Attack: An attacker controls the majority of the network hash rate and can reverse confirmed transactions.

Real-World Example:

In 2020, the Ethereum Classic network experienced multiple 51% attacks, resulting in double-spent transactions.

Prevention Techniques:

Wait for multiple confirmations (e.g., 6 for Bitcoin).

Use secure and up-to-date nodes.

Rely on blockchain platforms with strong consensus and high hash power.