PART A

I. a)
Key characteristics of blockchain technology include decentralization, immutability, transparency, consensus mechanisms, and cryptographic security.

b)
Advantages of centralized networks: faster decision-making, simpler infrastructure. Disadvantages: single point of failure, vulnerability to attacks. Decentralized networks offer improved security and resilience, but can be complex and slower.

c)
Bitcoin uses blockchain to store every transaction in blocks, ensuring transparency and immutability. Each block is linked to the previous, making tampering extremely difficult.

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)
It states that a distributed system cannot have consistency , Availability and partition tolerance simultaneously.
- consistency : Every node must have the same , current , identical copy of data
- Availability : Every node is up , accessible for use , accept request and respond to request.
- partition tolerance : The system must work despite the failure of some nodes.

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.

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).

- Proof of Work (PoW):

Used by Bitcoin.

Miners solve complex puzzles to validate transactions and create new blocks.

Energy-intensive and slow.

High security but low efficiency.

- Proof of Stake (PoS):

Validators are chosen based on the amount of cryptocurrency they stake.

Used by Ethereum 2.0.

Energy-efficient and faster than PoW.

Security depends on economic incentives.

Delegated Proof of Stake (DPoS):

Stakeholders vote for a limited number of delegates to validate blocks.

Used by EOS, TRON.

Extremely scalable and fast.

Less decentralized, vulnerable to cartelization.

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.