Mini Task 1 – Theoretical Report

# 1. Blockchain Basics

## Definition:

A blockchain is a distributed and decentralized digital ledger that securely records transactions across many computers in a way that prevents modification. Each block contains a set of transactions, a timestamp, and a reference (hash) to the previous block. This chaining of blocks ensures immutability. Blockchain operates without a central authority, relying on consensus mechanisms to validate transactions, making it transparent and secure. It is the foundational technology behind cryptocurrencies but has broader applications due to its trustless and tamper-proof nature.

## Real-Life Use Cases:

- Supply Chain Management: Blockchain can track the origin and journey of products from manufacture to delivery, increasing transparency and reducing fraud.

- Digital Identity: It allows individuals to control their identity and share verified credentials securely without centralized databases.

# 2. Block Anatomy

## Block Diagram:

+---------------------------------------------------+  
| Block |  
+---------------------------------------------------+  
| Index: 1 |  
| Timestamp: 2025-06-09 23:00:00 |  
| Data: { sender: Alice, receiver: Bob, amount: 5 } |  
| Previous Hash: 0000abc123... |  
| Merkle Root: a34f9d1b... |  
| Nonce: 562 |  
| Hash: 0000f3c2e1... |  
+---------------------------------------------------+

## Merkle Root Explanation:

A Merkle root is derived from hashing pairs of transaction hashes until one final hash remains. This root represents the summary of all transactions in the block. For example, given 4 transactions (T1, T2, T3, T4), their hashes are combined and hashed pairwise until one hash (the Merkle root) remains. If even a single transaction is altered, the Merkle root changes, making tampering easily detectable and ensuring data integrity.

# 3. Consensus Conceptualization

## Proof of Work (PoW):

Proof of Work is a consensus mechanism where miners solve complex mathematical puzzles to validate transactions and add new blocks. It requires significant computational power and energy because the hash must meet a difficulty condition (e.g., start with several zeroes). This makes the process secure but resource-intensive.

## Proof of Stake (PoS):

Proof of Stake selects validators based on the amount of cryptocurrency they hold and are willing to 'stake' as collateral. The more coins one stakes, the higher the chance of being chosen. Unlike PoW, PoS is energy-efficient since it doesn’t involve solving puzzles.

## Delegated Proof of Stake (DPoS):

In DPoS, stakeholders vote to elect a small group of delegates or validators who are responsible for block production. The voting power is proportional to the stake. Validators are selected based on votes, and this system improves speed and scalability while maintaining decentralization.