# Blockchain Fundamentals Assignment

## 🧱 Blockchain Basics

Blockchain is a decentralized, distributed digital ledger that securely records transactions across many computers. It stores information in blocks, each containing data, a timestamp, a unique hash, and the hash of the previous block. These blocks are linked, forming a chain that ensures data integrity — if any block is altered, all subsequent blocks become invalid unless recalculated. This structure makes blockchain tamper-resistant and transparent. It is widely known as the technology behind cryptocurrencies like Bitcoin, but it also has broader applications such as supply chain tracking, digital voting, and identity management. Unlike centralized systems, blockchain operates without a single controlling authority, increasing trust and accountability.

Real-life use cases:

1. Supply Chain Management – Tracking the journey of goods (e.g., agricultural produce) from farm to retailer in India, ensuring authenticity and quality.

2. Digital Identity – Using blockchain to verify Aadhaar-based identity in a decentralized, fraud-proof system.

## Block Anatomy

Diagram of a Block:

Block Header

Index : 3

Timestamp : 2025-06-07 00:45:00

Previous Hash : 0987abc123...

Nonce : 19821

Merkle Root : b3458d... (hash tree)

Block Data

- Tx1: A → B (₹500)

- Tx2: B → C (₹200)

- Tx3: A → D (₹300)

Merkle Root Explanation:

The Merkle root is the topmost hash of a Merkle tree, created by recursively hashing all transactions in a block. It helps verify whether a transaction exists in a block without revealing the entire data.  
Example: If a block contains 4 transactions, to confirm that Tx2 (B → C ₹200) exists, you only need a small set of hashes to validate against the Merkle root — not the whole dataset. This ensures fast and secure verification and immediately detects if even a single transaction has been altered.

## Consensus Conceptualization

What is Proof of Work (PoW)?

Proof of Work is a consensus mechanism where miners solve complex computational puzzles to validate transactions and create new blocks. The first miner to solve the problem is rewarded, often in cryptocurrency. This method consumes large amounts of electricity because miners perform trillions of hash operations, making it expensive to manipulate. The high cost and computational difficulty protect the network from attacks but also make PoW energy-intensive and less sustainable.

What is Proof of Stake (PoS)?

Proof of Stake selects validators based on the number of coins they lock up (stake) in the system. Instead of solving puzzles, validators are chosen to add blocks based on their stake size, which reduces energy consumption. The logic is that validators with more stake have more to lose and are thus incentivized to act honestly. PoS is faster and more eco-friendly than PoW, making it popular in newer blockchain systems like Ethereum 2.0.

What is Delegated Proof of Stake (DPoS)?

Delegated Proof of Stake involves voting. Coin holders vote to elect a small number of delegates who will validate transactions and create blocks. This system speeds up consensus and reduces the number of validating nodes, improving efficiency. However, it relies heavily on reputation and trust, since only a few nodes (delegates) maintain the blockchain. DPoS is widely used in systems where fast transaction confirmation is critical, like EOS.