Name : Aditi Arya

College : Amity University Gurgaon

- **Blockchain Basics (Definition)**

A **blockchain** is a decentralized digital ledger that records transactions across a network of computers in a way that prevents modification of past data. Each block contains transaction data, a timestamp, a cryptographic hash, and the hash of the previous block, linking them in a chain. Since data in any one block cannot be altered without changing all subsequent blocks, this provides security and trust without a central authority. Blockchains are maintained by consensus mechanisms like Proof of Work or Proof of Stake, ensuring integrity across a distributed network.

- **Real-Life Use Cases**

1. **Supply Chain Management**: Track the origin and movement of goods from production to delivery with transparency and traceability.
2. **Digital Identity**: Use blockchain for decentralized identity verification, reducing fraud and improving security in online systems.

Block Anatomy (Diagram & Merkle Root)

Here’s a block structure:

```
Index: 1
Timestamp: 2025-06-07
Data: {"sender":"A","receiver":"B","amount":50}
Previous Hash: a98x...d2
Merkle Root: 3ab4...912
Nonce: 4353
Hash: 0000a93f...
```

Merkle Root Explanation (with Example)

Merkle trees hash pairs of data recursively until a single hash, the **Merkle Root**, is produced. For example:

Transactions:
T1 = A → B: $50
T2 = C → D: $100
T3 = E → F: $200
T4 = G → H: $10

Hashes:
H1 = hash(T1), H2 = hash(T2), H3 = hash(T3), H4 = hash(T4)
H12 = hash(H1 + H2), H34 = hash(H3 + H4)
Merkle Root = hash(H12 + H34)

If even one transaction is altered, the Merkle root changes, helping quickly verify data integrity without examining all data.

- **Consensus Conceptualization**

Proof of Work (PoW):
A consensus method where miners solve complex mathematical puzzles to add a block. It requires energy because it involves repeated trial-and-error hashing using computational power. This makes tampering costly and discourages attacks.

Proof of Stake (PoS):
In PoS, validators are chosen based on the amount of cryptocurrency they "stake" as collateral. It’s energy-efficient compared to PoW, and wealthier participants have a higher chance of being selected to validate new blocks.

Delegated Proof of Stake (DPoS):
A variation of PoS where token holders vote to elect a few trusted delegates (validators) to produce blocks. This system increases speed and efficiency but introduces some centralization risk due to limited validator set.