Theoretical Part:

1.Blockchain Basics:

- Blockchain:

  The blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties. Each transaction is verified by the majority of participants of the system.It contains every single record of each transaction. Bitcoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or group of individuals name ‘Satoshi Nakamoto’ published a white paper on "*BitCoin: A peer-to-peer electronic cash system*" in 2008.Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction. One of the famous use of Blockchain is Bitcoin. Bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the Internet.

- Two real-life usecases:

  - supply chain:

    Blockchain technology can transform supply chain management by making it more transparent, trackable, and efficient. Companies like IBM and Walmart are already utilizing blockchain to track products, ensure authenticity, and optimize logistics. This helps prevent counterfeiting, improves product safety, and streamlines the supply chain process

  - Digital Identity:

    Blockchain can secure digital identity verification, reducing identity theft risks. For instance, SelfKey leads blockchain-based identity management, providing users with control over their identity and enhancing online security. This technology can be particularly useful in various sectors, including government services and financial institution

2.Block Anatomy:

  - Block:

BLOCK
Previous Hash: 0000000000000000007a...
Timestamp : 2025-06-09 14:23:00 UTC
Nonce : 2348923

Merkle Root : a3f1e2b6781c4d8e9f1b2...
Data: - T x1: Alice → Bob: 2 BTC - Tx2: Bob → Charlie: 1 BTC - Tx3: Dave → Alice: 0.5 BTC ....

o Merkle root:

A Merkle root is a cryptographic hash that represents the entirety of a Merkle tree, which is a data structure used to efficiently verify the integrity of a large dataset. In the context of blockchain, a Merkle root is used to summarize the transactions within a block. Each transaction in a block is hashed to produce a unique digital fingerprint.

The transaction hashes are paired and hashed together, creating a new level of hashes. This process is repeated until only one hash remains, which is the Merkle root.The Merkle root is included in the block header, allowing nodes to verify the integrity of the transactions within the block.

Merkle tree :

```
                Root Hash
                    |
          +----------+--------+
          |                   |
      Hash 0-0           Hash 0-1
          |                   |
     +-----+-----+       +----+----+
     |           |       |         |
  Hash A Hash B   Hash C Hash D
     |         |        |          |
  Data A    Data B    Data C    Data D
```

3. Consensus Conceptualization:

- Proof of Work:

Proof of Work (PoW) is a consensus mechanism that requires miners to solve complex mathematical puzzles to validate transactions. This process consumes significant energy due to the computational power required. The energy-intensive mining process is necessary to secure the network and validate transactions. It involves iterating through inputs to find a valid hash.

- Proof of Stake :

  Proof of Stake is a consensus mechanism where validators are chosen to create new blocks based on the amount of cryptocurrency they hold (their "stake"). Unlike Proof of Work, doesn't require energy-intensive mining. Instead, validators are selected based on their stake, making it more energy-efficient and potentially more secure. This approach reduces the environmental impact and can process transactions faster.

- Delegated Proof of Stake:

  Delegated Proof of Stake (DPoS) is a consensus mechanism where users vote for validators, known as delegates or witnesses. Validators are selected based on the number of votes they receive. These validators are responsible for creating new blocks and validating transactions. The voting process allows users to participate in the validation process. This approach is more democratic and efficient.