1. Introduction to Blockchain

What is Blockchain?

- **Definition**: A blockchain is a **decentralized, distributed ledger** that records transactions across a network of computers. It consists of a chain of **blocks**, each containing data, a **hash** (unique fingerprint), and the **hash of the previous block**.
- **Key Features**:
  - **Decentralized**: No single entity controls the network.
  - **Immutable**: Once data is recorded, it cannot be altered.
  - **Transparent**: All participants can view the transactions.
  - **Secure**: Uses cryptography to secure data.

Why Do We Need Blockchain?

- **Problems with Traditional Databases**:
  - Centralized systems are vulnerable to:
    - **hacks**,
    - **data manipulation**
    - **single points of failure**.
  - Lack of transparency and trust in centralized systems.
  - **No single point of failure**—improves security and reliability.
- **Blockchain Solves These Issues**:
  - Decentralization ensures no single point of control.
  - Immutability prevents tampering with data.
  - Transparency builds trust among users.

Feature	**Traditional Database**	**Blockchain**
Centralization	Centralized server	Decentralized (P2P)
Security	Can be hacked easily (vulnerable to single point attacks)	Uses cryptographic security

Modification	Data can be altered	Data is immutable
Trust	Requires trusted third-party	Trustless system
Transparency	Limited to authorized users	Transparent to all network participants

---

2. How Blockchain Works

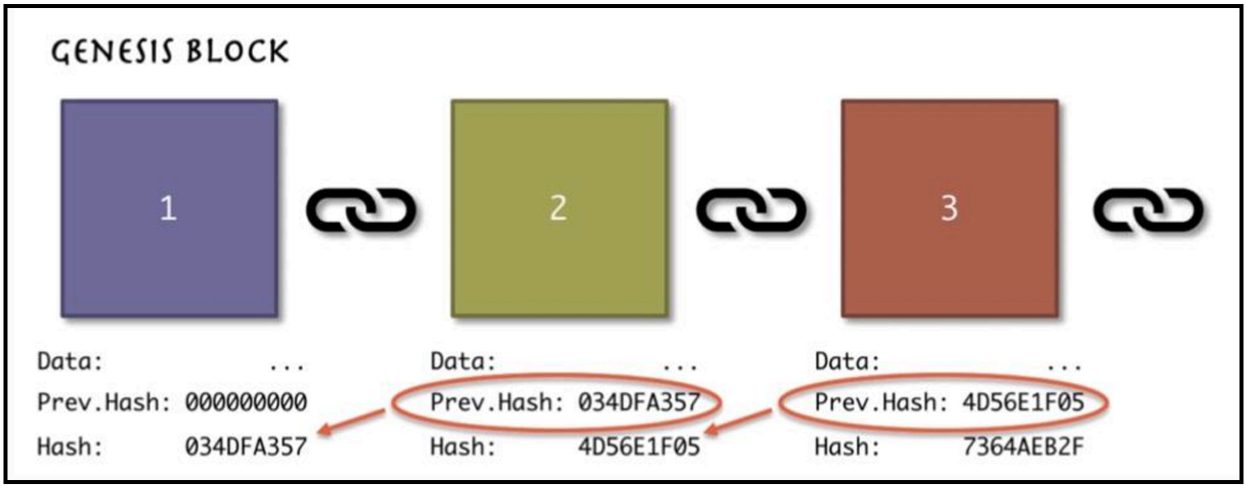
Structure of a Block

- Each block contains:
  - **Data**: Transactions or other information (e.g., "Hello World").
  - **Previous Hash**: The hash of the previous block (links blocks together).
  - **Hash**: A unique fingerprint of the block's contents (generated using **SHA256**).

Genesis Block:

The first block in the blockchain, which has no previous hash.

Diagram Explanation:



- The diagram shows a simple blockchain with three blocks:
  - **Block 1 (Genesis Block)**: No previous hash.

    - **Block 2**: Contains the hash of Block 1.
    - **Block 3**: Contains the hash of Block 2.
- This chaining of blocks ensures **data integrity**.

---

3. SHA256 Hash Algorithm

What is SHA256?

- **Definition**: A cryptographic hash function that takes an input and produces a **64-character hash**.
- **Key Properties**:
    - **Deterministic**: Same input always produces the same hash.
    - **One-Way**: Cannot reverse-engineer the input from the hash/ Cannot be reversed.
    - **Avalanche Effect**: A small change in input drastically changes the hash.
    - **Collision Resistant**: Two different inputs cannot produce the same hash.

Example:

- If you hash the word "Hello", you get a specific hash. If you change it to "hello" (lowercase), the hash will be completely different.

---

4. Immutable Ledger

What is an Immutable Ledger?

- **Definition**: A ledger that cannot be altered once data is recorded.
- **Traditional Ledgers**:
    - Prone to **tampering** and **errors**.
    - Example: Property deeds can be forged or destroyed.
- **Blockchain Ledger**:
    - Data is **immutable** and **secure**.
    - Example: Property records on a blockchain cannot be altered, ensuring ownership rights.

---

5. Peer-to-Peer (P2P) Network

What is a P2P Network?

- **Definition**: A decentralized network where each participant (node) has equal authority and a copy of the blockchain.
- **Key Features**:
    - **No Central Authority**: No single point of control.
    - **Anonymity**: Users interact without revealing their real identities.
    - **Consensus**: Majority of the nodes must agree on the validity of transactions.

Explanation:

- Each node has a copy of the blockchain.
- If a block is added, all nodes update their copies.
- If a hacker tries to alter a block, the network detects the inconsistency and rejects the change.

---

6. Mining and Consensus Mechanisms

What is Mining?

- **Definition**: The process of validating transactions and adding them to the blockchain.
- **How Mining Works**:
    - Miners solve a **cryptographic puzzle** to find a **nonce** (a number used once) that generates a hash below a certain target.
    - The first miner to solve the puzzle gets to add the block and is rewarded (e.g., with cryptocurrency).
    - Miners continuously change the nonce until they find a hash below the **difficulty target**.

Nonce and Cryptographic Puzzle:

- **Nonce**: A random number that miners change to generate a valid hash.
- **Target**: A threshold set by the network. Miners must find a hash below this target.
- **Golden Nonce**: The correct nonce that produces a valid hash(below the target).

7. Key Components of Blockchain

1. Nodes:

- Participants in the network that validate transactions and maintain the blockchain.

2. Miners:

- Special nodes that solve cryptographic puzzles to add blocks, and get financial incentives based on their work.

3. Users:

- Individuals or entities that perform transactions on the blockchain.

4. Smart Contracts:

- Self-executing contracts with predefined rules (not covered in detail in this PDF but important to note).

8. Why is Blockchain Secure?

1. Decentralization:

- No single point of failure.

2. Cryptography:

- Uses SHA256 hashing and public-private key encryption.

3. Consensus Mechanisms:

- Proof of Work (PoW) and Proof of Stake (PoS) ensure agreement among nodes.

4. Immutability:

- Once data is recorded, it cannot be altered.

9. Forging the Blockchain

- A hacker would need to modify the blockchain on **51% of the nodes** to alter a transaction.
- The system automatically restores the correct version if an attack is detected.

10. Key Terms to Remember

- **Block**: A container for data in a blockchain.
- **Hash**: A unique fingerprint of data.
- **Nonce**: A number used once in mining.
- **Genesis Block**: The first block in a blockchain.
- **P2P Network**: A decentralized network of nodes.