Armaan Shamsaasef

Blockchain Technologies

Blockchain Technology - SY0-701 1.4

Core Concept: A decentralized, distributed, and immutable digital ledger that records transactions across many computers.

Key Characteristics

1. Decentralized & Distributed:
    - There is no central authority (like a bank or government) controlling the ledger.
    - The ledger is copied and distributed across a vast network of computers (nodes). Everyone has the same copy.
2. Immutable:
    - Once a transaction is recorded in a block and added to the chain, it is extremely difficult to change or remove.
    - This is enforced by cryptographic hashing.

How a Blockchain Works: The "Block" and "Chain"

1. The Block:

- Each block contains:
    - A list of transactions (e.g., "Alice sends 5 Bitcoin to Bob").
    - The hash of the previous block in the chain.
    - Its own unique hash (like a cryptographic fingerprint), which is calculated based on its contents.

2. The Chain:

- Blocks are linked together in a linear, chronological order.
- Each block's hash is dependent on the previous block's hash.
- Video Analogy: Imagine a child's toy train where each car (block) is linked to the one before it.

The Power of Immutability: What Prevents Tampering?

If an attacker tries to alter a transaction in a past block:

1. The hash of that block changes instantly.
2. Because that block's hash is now different, it breaks the link to the next block in the chain (whose "previous hash" field no longer matches).
3. The attacker would have to recalculate the hashes for every single subsequent block in the chain, which requires a massive amount of computing power.
4. Furthermore, they would have to do this on over 50% of the distributed network copies simultaneously to create a new consensus.

This makes tampering computationally infeasible and is what creates trust in a trustless environment.

Use Cases

- Cryptocurrency: The original and most famous use case (e.g., Bitcoin, Ethereum). It acts as a public financial ledger.
- Smart Contracts: Self-executing contracts where the terms are written directly into code and run on the blockchain (e.g., Ethereum).
- Supply Chain Management: Tracking the provenance and journey of goods from origin to consumer in an unchangeable ledger.
- Identity Management: Creating a secure, unforgeable digital identity.

Summary

- Decentralized: No single owner, runs on a peer-to-peer network.
- Distributed Ledger: Everyone has a copy, ensuring transparency.
- Immutable: Records cannot be altered due to cryptographic hashing linking the blocks.
- Core Value: Provides a verifiable and permanent record of transactions without needing a central authority.