Day 1 Blockchain Notes

What is Blockchain?

Blockchain is a decentralized, distributed digital ledger that stores transaction records across multiple computers in a way that ensures the security and integrity of the data. Instead of relying on a central authority to verify transactions, the blockchain uses a network of computers (nodes) that follow a consensus mechanism to validate and record transactions.

A blockchain consists of a series of blocks, each containing a list of transactions. Each block is connected to the previous one via a cryptographic hash. This creates a chain of blocks, hence the name "blockchain". This structure makes it highly secure, as altering any information in a block would require changing all subsequent blocks, which is nearly impossible.

Key Features of Blockchain:

- **Decentralization**: The control is distributed among the participants in the network, removing the need for central intermediaries like banks or government bodies.
- **Transparency**: Transactions are visible to all participants, ensuring accountability.
- **Immutability**: Once a transaction is recorded, it cannot be altered or deleted.
- **Security**: Each block contains a cryptographic hash, a unique identifier that secures it against tampering.

Example: In the Bitcoin blockchain, every transaction is recorded as a block, which is validated by miners using Proof of Work (PoW). This decentralized approach ensures that Bitcoin can operate without a central bank.

History of Blockchain:

- **1991 - Cryptographic Time-stamping**: Haber and Stornetta introduced the idea of using cryptography to securely timestamp documents. This concept would later evolve into blockchain technology.

- **2008 - Bitcoin Whitepaper**: Satoshi Nakamoto's whitepaper proposed a peer-to-peer system for transferring digital currency without relying on a trusted third party, introducing the concept of blockchain.

- **2009 - Bitcoin Genesis Block**: Nakamoto mined the first block of the Bitcoin blockchain, marking the beginning of a new era for digital currency.

- **2015 - Ethereum and Smart Contracts**: Ethereum introduced smart contracts, which are self-executing contracts that run on the blockchain. This allowed for more complex decentralized applications (DApps) beyond just digital currency.

Inside a Block:

- A block is composed of several key elements:
  - **Transactions**: A list of all validated transactions.
  - **Timestamp**: The time when the block was created.
  - **Hash**: A unique cryptographic hash that represents the contents of the block.
  - **Previous Block Hash**: Each block is linked to the previous block via its hash, ensuring the chain remains intact and secure.

Example: In the Bitcoin blockchain, each block contains a list of Bitcoin transactions, a timestamp of when the block was created, and the hash of the previous block. This makes the blockchain immutable and secure.

Blockchain Consensus Mechanisms:

Blockchain networks need a way to ensure that all participants agree on the state of the blockchain. This is done through consensus mechanisms like Proof of Work (PoW) and Proof of

Stake (PoS).

- **Proof of Work (PoW)**: In PoW, miners compete to solve a cryptographic puzzle. The first miner to solve the puzzle gets to add the next block to the blockchain and is rewarded with cryptocurrency (e.g., Bitcoin). This process requires significant computational power, making it energy-intensive.

Example: Bitcoin uses PoW, where miners compete to solve complex mathematical problems. The winner gets to add a new block to the Bitcoin blockchain and is rewarded with newly minted Bitcoin.

- **Proof of Stake (PoS)**: In PoS, validators are selected based on the amount of cryptocurrency they hold. The more coins a validator owns, the higher the chances they have of being chosen to validate the next block. This is less energy-intensive than PoW.

Example: Ethereum 2.0 uses PoS, where validators are selected based on the amount of Ethereum they stake. This method is more energy-efficient compared to PoW.