UNIT 3: Blockchain

Blockchain

A blockchain is a peer-to-peer distributed ledger technology. Which is an immutable, decentralized, encrypted, distributed ledger technology.

The name comes from its structure, in which individual records, called blocks, are linked together in single list, called a chain. Blockchains are used for recording transactions made with cryptocurrencies, such as Bitcoin, and have many other applications.

Each transaction added to a blockchain is validated by multiple computers on the Internet (Miners). These systems form a peer-to-peer network.

Key Characteristics / Benefits of Blockchain Technology:

- ✓ **Open**: Anyone can access blockchain.
- ✓ **Distributed or Decentralised:** Not under the control of any single authority.
- ✓ **Efficient:** Fast and Scalable.
- ✓ **Permanent:** Once a transaction is done, it is persistent and can't be altered.
- ✓ **Time-saving:** No central Authority verification needed for settlements making the process faster and cheaper.
- ✓ **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced.
- ✓ **Tighter security:** No one can temper with Blockchain Data as it shared among millions of Participant. The system is safe against cybercrimes and Fraud.
- ✓ **Secure:** There is no unauthorized access to Blockchain made possible through Permissions and Cryptography.
- ✓ **Transparent:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data.

Contents of a Block.

Blockchain starts with a block. Each block stores the following information in it:

1. **Index:** Position of the block in blockchain. Index of genesis block is 0.
2. **Time stamp:** The time when that particular block was created.
3. **Hash:** Numeric value that uniquely identifies data just like our fingerprints.
4. **Previous hash:** Hash value of the previous block. For genesis block, this value is 0.
5. **Data:** Data stored on the node. For example, transactions.
6. **Nonce:** It is a number used to find a valid hash. To generate this number, the processing power is used.

3 Pillars of Blockchain Technology

The three main properties of Blockchain Technology are:

- ✓ **Decentralization**: In a decentralized system, the information is not stored by one single entity. In fact, everyone in the network owns the information.
- ✓ **Transparency:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data.
- ✓ **Immutability:** It means that once something has been entered into the blockchain, it cannot be tampered with.

Disadvantages of current transaction system:

- ➢ Cash can only be used in low amount transaction locally.
- ➢ Huge waiting time in the processing of transactions.
- ➢ Need to third party for verification and execution of Transaction make the process complex.
- ➢ If the Central Server like Banks is compromised, whole System is affected including the participants.
- ➢ Organization doing validation charge high process thus making the process expensive.

Cryptocurrency

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which is immutable. Many cryptocurrencies are decentralized networks based on blockchain technology. Cryptocurrencies are electronic peer-to-peer currencies. They don't physically exist.

Examples of cryptocurrency

The first blockchain-based cryptocurrency was Bitcoin, which still remains the most popular and most valuable. Other are:

1. Bitcoin
2. Ripple
3. Litecoin
4. Libra
5. Bitcoin Cash
6. Chainlink

Bitcoin

- ✓ Bitcoin is a completely decentralised, peer-to-peer, permissionless cryptocurrency put forth in 2009 by Satoshi Nakamoto.
- ✓ Bitcoin is the first blockchain application.
- ✓ It is permissionless , i.e. open to anyone.
- ✓ Bitcoin blockchain size is growing exponentially.

Why Bitcoins ?

Bitcoins can be used to buy merchandise anonymously. In addition, international payments are easy and cheap because bitcoins are not tied to any country or subject to regulation. Small businesses may like them because there are no credit card fees. Some people just buy bitcoins as an investment, hoping that they'll go up in value.

Smart Contract

The term was coined by **Nick Szabo**, a computer scientist and cryptographer, in 1996.

A smart contract, also known as a cryptocontract

A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

Advantages of Smart Contracts:

- ✓ **Immutable:** No one can change it once it is deployed on blockchain.
- ✓ **Distributed:** All the steps of the contract can be validated by every participating party — no one can claim later that the contract was not validated.
- ✓ **Saves money:** Since there is no need of third-party to run or maintain the contract, the cost is saved.

Popular Smart Contract Platforms:

- ➢ Ethereum
- ➢ Hyperledger
- ➢ Ripple
- ➢ Rootstock

Applications of Blockchains

Blockchain can be used in practically all those scenarios where middlemen are involved. Here are some of the use-cases.

1. **Cryptocurrency**: this is the most well-known use of Blockchain. By implementing Blockchain, parties are able to transact with each other without the involvement of any bank. For instance, a person sitting in the United States can transfer bitcoins to one based out of India without intervention from any bank. This lead to the creation of a lot of cryptocurrencies, Bitcoin being the most popular one.

2. **Advertising**: Currently, companies like Google and Facebook control almost all of the digital advertising traffic of the world. However, Blockchain can potentially eliminate that. Here, Google and Facebook are essentially middlemen that control the advertising ecosystem. Using Blockchain the producers and the consumers can be connected directly through a decentralized system.

3. **Real Estate:** In the Real Estate industry, there are middlemen in the form of brokers who often charge exorbitant fees for pairing the buyer with the sellers. Using Blockchain, such middlemen can be eliminated to save the cost. Basically, instead of relying on centralized advertising/listing portals, a Blockchain can be used where the producers (advertisers or real-estate sellers) can provide their ads/listings and consumers can see them directly without any middlemen.

4. **Healthcare**: The health records of patients can be securely stored in a Blockchain so that when the patient visits another doctor, he/she can directly share those records with the new doctor. The best part about using Blockchain here is that there is no need for a centralized portal where these records are stored. Therefore, the cost can be lowered significantly. Health records could include a lot of things like:
   - Diagnostic by doctor
   - Medical History
   - Lab reports

5. **Voting:** Online voting has been resisted by many due to concerns such as security and fraud. Blockchain can successfully eliminate these concerns as it will present a clear record of the votes that have been cast. The tamper-proof feature of a blockchain makes it difficult to hack a blockchain-enabled voting system. With blockchain, the voting process can be carried out comfortably from the confines of the voter's homes. This may result in a significant rise in voter turnout.

6. **Insurance**: Arguably the greatest blockchain application for insurance is through smart contracts. These contracts allow customers and insurers to manage claims in a transparent and secure manner. All contracts and claims can be recorded on the blockchain and validated by the network, which would eliminate invalid claims, since the blockchain would reject multiple claims on the same accident.

7. **Media**: Media companies have already started to adopt blockchain technology to eliminate fraud, reduce costs, and even protect Intellectual Property (IP) rights of content - like music records.

8. **Taxes**: Blockchain tech could make the cumbersome process of filing taxes, which is prone to human error, much more efficient with enough information stored on the blockchain.