Blockchain Technology

In recent times, we are getting to hear about a new terminology that is Blockchain Technology. Blockchain is defined as a distributed database shared among different computer nodes. Database stores information in digital format. Blockchain guarantees the security of the data stored on it. Moreover, Blockchain is ideal for delivering the data as it provides a fast and complete transparent flow of information to access specified members only. A blockchain network can track the accounts, information flow, orders, etc.

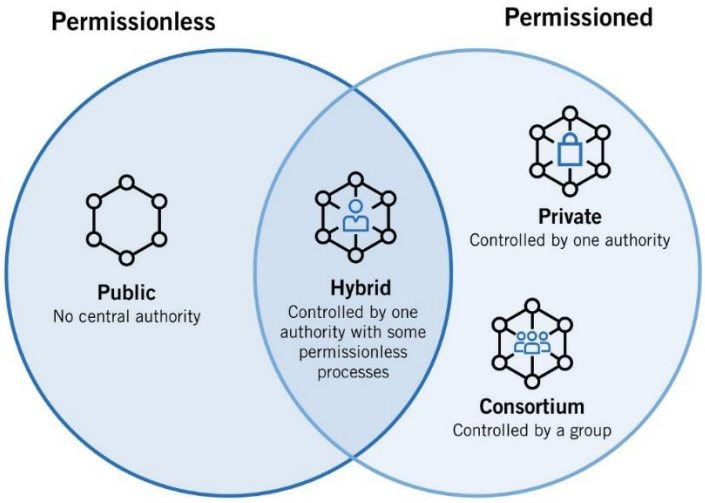
There is a difference between a database and a blockchain. It is how the data is structured. A blockchain collects information together in groups, known as blocks, which are storage spaces for holding the data. Considering that the database stores information in tables.

The key elements in a blockchain include:
1) **Distributed Ledger Technology**: It is referred to as the technological infrastructure and protocols. All network members have access to the distributed ledger and its immutable record of transactions. This helps in maintaining the record of transactions only once and reduces duplication chances.

2) **Immutable records:** It is referred to as any records that can remain unchanged. No member can change the transaction records. If there is any error, then a new record is added and then both the transaction records are visible.

3) **Smart Contracts**: These are generally programs stored in a blockchain that runs when it meets predetermined conditions. A smart contract is an agreement between two people in the form of computer code. It runs on the blockchain, is stored on a public database, and cannot be changed. The transactions that happen in a smart contract are processed by the blockchain, which means they can be sent automatically without a third party.

There are four different types of blockchain:



1) **Public Blockchain:** A public blockchain is an open chain that does not require any kind of authorization to join. The general public can participate without authorization because it is not controlled by anyone. The public blockchain allows all branches of the chain to create and validate data. Bitcoin and Ethereum are two popular blockchain examples.

2) **Private Blockchain:** A private blockchain is a sort of blockchain in which only one organization has access to the entire network. It is the absolute opposite of a public blockchain. Private blockchain includes security to who has access to the data. The members of that organization have access to the data. Therefore, this leads to speedy decision-making and increases transaction processes.

3) **Consortium blockchain**: It offers the new kid on the block to join the established structure and share information instead of starting from scratch. This technology helps organizations to find solutions together and save time and

development costs. Consortium blockchains are also known as Federated blockchains.
Hyperledger blockchain is the largest consortium blockchain.

4) **Hybrid Blockchain**: It is a world-changing blockchain. It provides better solutions and is used in government offices, businesses, and many organizations. The data stored in a hybrid blockchain is visible, accessible to all members, and have the chance of being tampered with. However, some applications are not exposed to public or private users.

IBM food trust is an example of a hybrid blockchain.

The functioning of the blockchain is dependent on three components: data, hash, and previous block hash.

Step 1: Data

The type of data stored in a block differs from the type of blockchain. If the data is about Bitcoin, the blockchain maintains data about a transaction record such as the sender, receiver, and transaction amount.

Step 2: Hash

A hash is included in the block. When a block is created, its hash is computed. Hash changes if something in the block changes. That is why hashing aids in detecting changes in a blockchain. If a block's fingerprint changes, it is no longer the same block.

Step 3: Previous data hash

A hash of a previous block is the final piece in a blockchain. The hash of the preceding block aids in the creation of a chain, and as a result of these aspects, the blockchain is secure to use and trust. In a blockchain, each block is connected to the previous hash's data, so if anything is tampered with or changed, the hash changes immediately and then all the blocks recognize it and change accordingly. To make the blockchain valid again, the hash of tampered blocks is altered by default, as are the hashes of other blocks.

Blockchains are growing with time, introducing new developments like smart contracts, which have been shown to be extremely useful. Blockchain is a technology that has captivated many people due to its successful operation.

“*The blockchain cannot be described just as a revolution. It is a tsunami-like phenomenon, slowly advancing and gradually enveloping everything along its way by the force of its progression.*”