

Blockchain Introduction

Blockchain is a buzzword in today's technology and this technology is described as the most disruptive technology of the decade. Thus, Blockchain is used for the secure transference of items like money, contracts, property rights, stocks, and even networks without any requirement of Third Party Intermediaries like Governments, banks, etc. Once the data is stored in the Blockchain it becomes very difficult to manipulate the stored data. A Blockchain is a Network Protocol like SMTP. However, Blockchain cannot be run without the Internet. Blockchain is useful in many areas like Banking, Finance, Healthcare, Insurance, etc.

A blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way without the need for a central authority.

Key Characteristics:

- **Open:** Anyone can access blockchain.
- **Distributed or Decentralised:** Not under the control of any single authority.
- **Efficient:** Fast and Scalable.
- **Verifiable:** Everyone can check the validity of information because each node maintains a copy of the transactions.
- **Permanent:** Once a transaction is done, it is persistent and can't be altered.

Blockchain can be defined as the Chain of Blocks that contain some specific Information. Thus, a Blockchain is a ledger i.e file that constantly grows and keeps the record of all transactions permanently. This process takes place in a secure, chronological (Chronological means every transaction happens after the previous one) and immutable way. Each time when a block is completed in storing information, a new block is generated.

Distributed Systems:

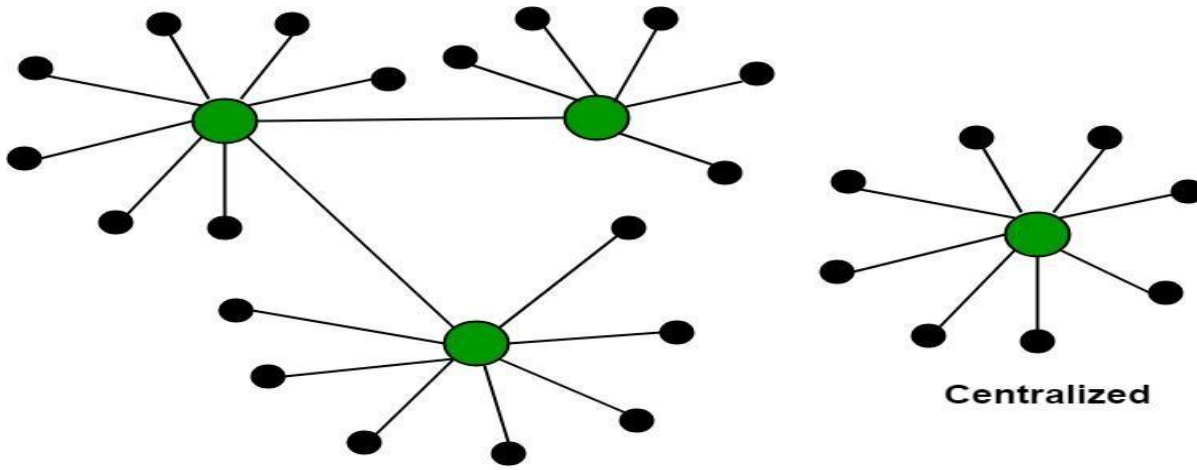
Understanding distributed systems is essential to our understanding blockchain, as blockchain was a distributed system at its core. It is a distributed ledger that can be centralized or decentralized. A blockchain is originally intended to be and is usually used as a decentralized platform. It can be thought of as a system that has properties of the both decentralized and distributed paradigms. It is a decentralized-distributed system.

Distributed systems are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion to achieve a common outcome. It is modeled in such a way that end users see it as a single logical platform. For example, Google's search engine is based on a large distributed system; however, to a user, it looks like a single, coherent platform.

A **node** can be defined as an individual player in a distributed system. All nodes are capable of sending and receiving messages to and from each other. There is no Central Server or System which keeps the data of Blockchain. The data is distributed over Millions of Computers around the world which are connected with the Blockchain. This system allows Notarization of Data as it is present on every Node and is publicly verifiable. A node can be defined as an individual player in a distributed system. All nodes are capable of sending and receiving messages to and from each other.

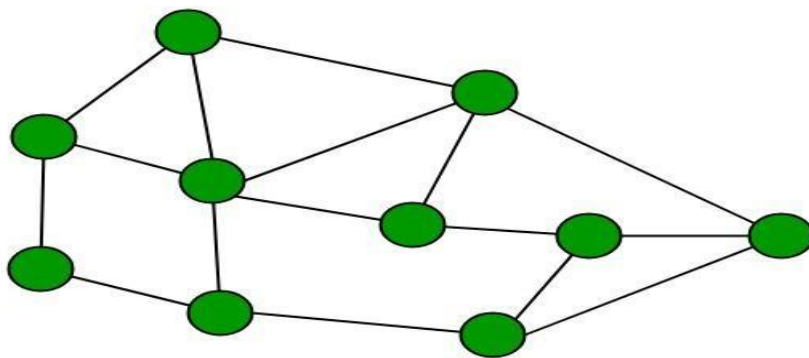
Nodes can be honest, faulty, or malicious and have their own memory and processor. A node that can exhibit arbitrary behavior is also known as a Byzantine node. This arbitrary behavior can be intentionally malicious, which is detrimental to the operation of the network. Generally, any unexpected behavior of a node on the network can be categorized as Byzantine. This term arbitrarily encompasses any behavior that is unexpected or malicious.

The main challenge in distributed system design is coordination between nodes and fault tolerance. Even if some of the nodes become faulty or network links break, the distributed system should tolerate this and should continue to work flawlessly in order to achieve the desired result. This has been an area of active research for many years and several algorithms and mechanisms has been proposed to overcome these issues.



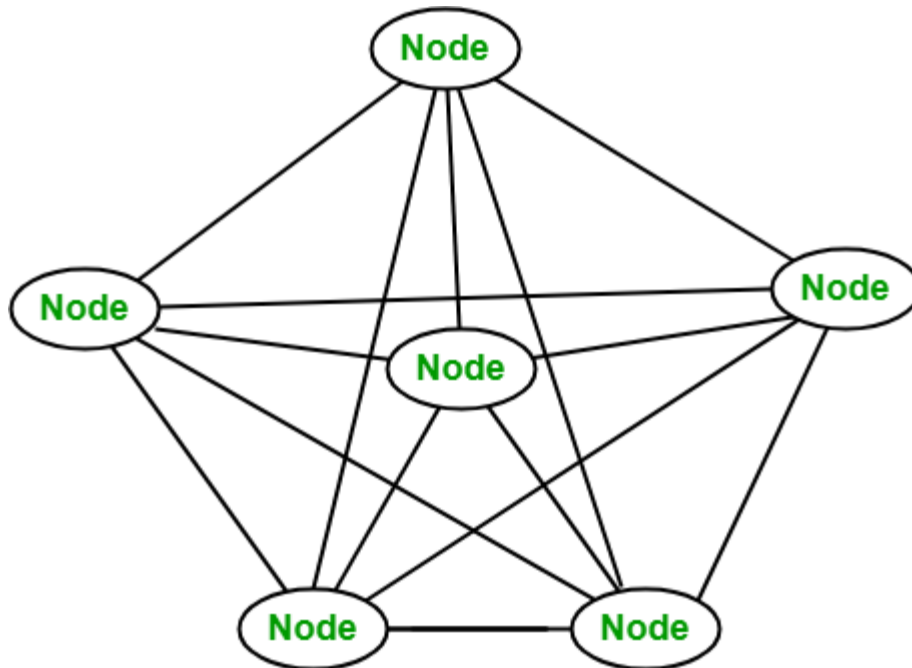
Decentralized

Centralized



Distributed

A network of nodes: A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. Client helps in validating and propagates transaction on to the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.



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.

Building trust with Blockchain:

Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with its that you don't need to when operating on a Blockchain network.

Blockchain builds trust through the following five attributes:

- **Distributed:** The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real-time as there is no central server controlling the data.
- **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. They themselves can verify the identities without the need for mediators.
- **Consensus-based:** All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.
- **Flexible:** Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Network can evolve in pace with business processes.