**Introduction**

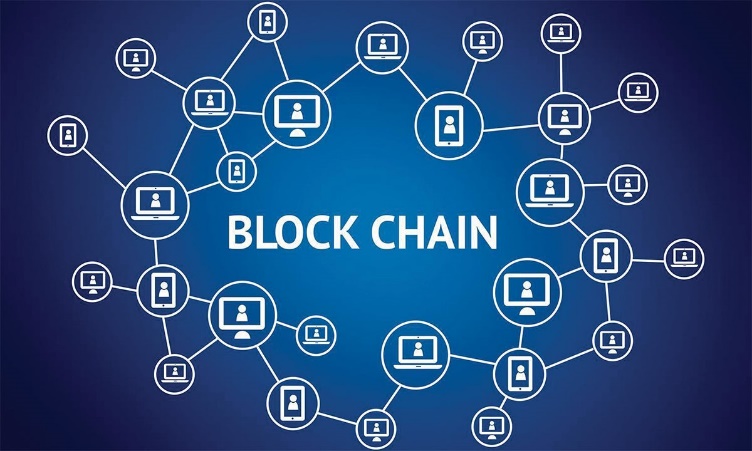
A blockchain is a distributed, peer-to-peer database that hosts a continuously growing number of transactions. Each transaction, referred to as a “**block**,” is secured through cryptography, timestamped, and validated by every authorized member of the database using consensus algorithms (i.e., a set of rules). A transaction that is not validated by all members of the database is not added to the database.

Every transaction is attached to the previous transaction in sequential order, creating a chain of transactions (or blocks). A transaction cannot be deleted or edited, thereby creating an immutable audit trial. A transaction can only be changed by adding another transaction to the chain.

**History of Blockchain**

* First proposed as a research project in **1991**, the blockchain concept predated its first widespread application in use: Bitcoin, in 2009.
* 
* **Satoshi Nakamoto**
* The blockchain was popularized by a person (or group of people) using the name in **2008** to **Satoshi Nakamoto** serve as the public transaction ledger of the **Cryptocurrency Bitcoin** based on work by Stuart Haber, **W. Scott Stornetta, and Dave Bayer**.
* The identity of Satoshi Nakamoto remains unknown to date. The implementation of the blockchain within bitcoin made it the first digital currency to solve the Double-spending spending problem without the need of a trusted authority or central server.
* Bitcoin's **Genesis Block** was the first instance of a proof-of-work blockchain system and is the template for all other blocks in its blockchain. In 2009, Bitcoin's pseudonymous developer, Satoshi Nakamoto, created the Genesis Block, which launched the cryptocurrency boom that is ongoing today.

**What is Blockchain?**

****

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as bitcoin for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

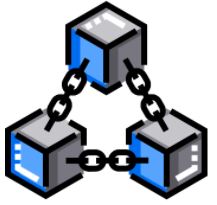
One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.

A database usually structures its data into tables, whereas a blockchain, like its name implies, structures its data into chunks (blocks) that are strung together. This data structure inherently makes an irreversible time line of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this time line. Each block in the chain is given an exact time stamp when it is added to the chain.

**Why is Blockchain Important and Why Does it Matters**

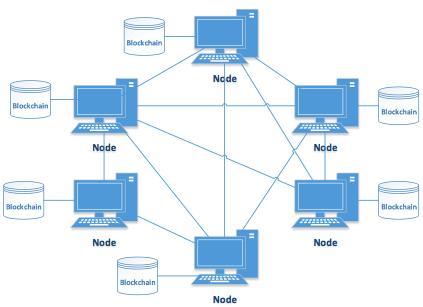


Blockchain helps in the verification and traceability of multistep transactions needing verification and traceability. It can provide secure transactions, reduce compliance costs, and speed up data transfer processing. Blockchain technology can help contract management and audit the origin of a product. It also can be used in voting platforms and managing titles and deeds.



Note: The data is recorded in chronological order. Also, once the data is recorded, it cannot be changed.

**Distributed P 2 P Network**

****

The underlying blockchain technology leverages the power of P2P networks and provides a shared and trusted ledger of transactions. As a distributed ledger technology, blockchain records transactions as an immutable timestamped digital block that indicates senders and receivers. No centralized authority manages the blockchain networks and only the participants can validate transactions among each other. The technology allows people and institutions to trust the output without trusting the participants. This new form of distributed data storage and management acts as a digital ledger that publicly records all transactions and activities.

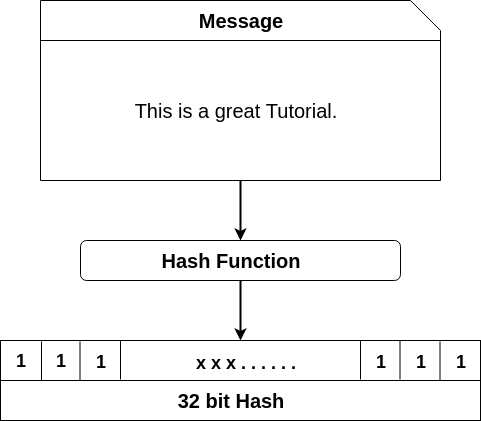
Peer to peer network, commonly known as P2P is a decentralized network communications model that consists of a group of devices (nodes) that collectively store and share files where each node acts as an individual peer. In this network, P2P communication is done without any central administration or server, which means all nodes have equal power and perform the same tasks.

P2P architecture is suitable for various use cases and can be categorized into structured, unstructured, and hybrid peer-to-peer networks. The unstructured peer-to-peer networks are formed by nodes randomly from connection to each other, but they are inefficient than structured ones. In structured peer-to-peer systems, the nodes are organized, and every node can efficiently search the network for the desired data. Hybrid models are actually a combination of P2P and client-server models, and when compared to the structured and unstructured P2P systems, these networks tend to present improved overall performance.

**Hashing algorithm**

**Blockchain Hash Function**

A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic by product of a hash algorithm. We can understand it from the following diagram.



**The hash algorithm has certain unique properties:**

1. It produces a unique output (or hash).
2. It is a one-way function.

In the context of cryptocurrencies like bitcoin

, the blockchain uses this cryptographic hash function's properties in its consensus mechanism. A cryptographic hash is a digest or digital fingerprints of a certain amount of data. In cryptographic hash functions, the transactions are taken as an input and run through a hashing algorithm which gives an output of a fixed size.

## SHA-256

A Bitcoin's blockchain uses SHA-256 (Secure Hash Algorithm) hashing algorithm. In 2001, SHA-256 Hashing algorithm was developed by the National Security Agency (NSA) in the USA.

**For example:** We have type in data section: **This is a preet**.

It will generate the corresponding Hash:

1. 759831720aa978c890b11f62ae49d2417f600f26aaa51b3291a8d21a4216582a

**Immutable ledger**

Immutable ledger in blockchain refers to any records that have the ability to remain unchanged. It cannot be altered and hence the data cannot be changed with ease, thereby making sure that the security is quite tight. Immutability means that it is very difficult to make changes without collusion. The central idea behind the blockchain ledger is the security of data and the proof that data has not been changed or altered. Let us delve a bit deeper into the topic to understand more about blockchain immutability and the benefits it offers.

## Understanding Blockchain Immutability

Immutability is defined as the ability of a blockchain ledger to remain unchanged, unaltered, and indelible. Each of the blocks of information like facts or transaction details is carried out with the help of a cryptographic principle or a hash value. Now, this hash value has an alphanumeric string generated by each block individually. Each of the blocks contains a hash value or digital signature for itself and for the previous one as well. This, in turn, makes sure that the blocks are retroactively coupled together and unrelenting. It is this functionality of blockchain technology that makes sure no one is able to interfere with the system or change the already saved data into the block.

In this regard, it is also quite essential to know that blockchain is distributed and decentralized in nature. Here a consensus is made among the different storing a copy of the data. It is this consensus that makes sure the originality of data is righty maintained. Immutability is undoubtedly one of the most definitive features of blockchain technology and also brings out the that can be deployed. The concept can simply redefine the entire process of auditing of data to make it much more efficient, and cost-effective, along with bringing about more trust as well as integrity into the data.

## How to Achieve Immutability?

As explained above, the hash value helps in securing each block of code in a separate manner. To understand how to achieve immutability, clarification of the concept of cryptographic hashing is essential. Nowadays, the generation of a cryptographic is not quite a dreadful task. It is because of the fact that modern programming languages come with an array of hash functions. With the help of these hash functions, it is just required to pass a set of bytes and the function will be returning a checksum signature. These functions always generate a string of length of 64 characters and we would always be getting the fixed string length regardless of the size of the input, which is referred to as a digital signature.  
  
The digital signature points to the exact data that the users input. But hash cannot be reverse-engineered which means that the users cannot make use of this output string for the purpose of finding the input data. This, in turn, results in the immutability of the blockchain ledger. In this system, each of the transactions is verified with the help of a blockchain network. It includes blocks of information embedded with timestamps and is secured by a hashing process. It links together and incorporates the hash of the last block. This mechanism plays a major role in developing the chronological chain which helps in joining each of the blocks.  
  
The meta-data of the last block is always included by hashing at the time of generating a new hash for it. This, in turn, helps in creating a link between the block and the chain, thereby making it unbreakable. Once this is done, none can alter or delete the data of the block which is placed in the blockchain. It is because whenever anyone would be attempting to make a change, the modification is rejected by the subsequent block since the hash of the block would not be valid anymore.

**References**

🡺https://www.cpajournal.com/

🡺 https://www.investopedia.com/

🡺https://www.javatpoint.com/

🡺https://www.solulab.com/