**Blockchain Technology**

**Introduction to Blockchain**

The world of crypto is full of technical jargon that can confuse even the savviest technology ninja. Bitcoin introduced the concept of crypto-economics and paved the way for the creation of many blockchain platforms. Before we dive deep into how a blockchain works, let’s understand what cryptoeconomics is and the underlying concepts behind a blockchain

* **Encryption**: Encryption is a process of converting your message into code so that only authorized parties can access it.
* **Decryption**: Decryption is reversing the encryption process so that the message can be converted to the original message.
* **Cryptography**: This is using the techniques of encryption and decryption to send and receive messages.
* **Cryptocurrency:** This is using cryptography the same way as the earlier SSL or video example but specifically to fit the needs of a digital asset
* **Cryptoeconomics**: This is the combination of cryptography and economics to provide a platform to pass digital assets.

**Blockchain Explained**

Bitcoin was the first successful open source digital cash. Blockchain is the core technology, or the heart behind bitcoin and in fact behind all cryptocurrency platforms.

But what is blockchain?

In short, a *blockchain* is a shared digital ledger. Think of a database that instead of storing all the database entries on one computer it stores the data on multiple computers. A fancier definition would be that a blockchain is a decentralized and distributed global ledger.

**Blocks + Chain = Blockchain**

Each block contains records and transactions; these blocks are shared across multiple computers and should not be altered absent an agreement (consensus) of the entire network. The network is ruled according to a specific policy. The computers are connected on one network and called *peers* or *nodes*.

(no financial institutions involved) and distributed ledger. in layperson’s terms, it is a database that stores records and transactions on multiple computers without one controlling party and according to an agreed policy. the data that is stored is a block, and the blocks are linked (chained) together to form a blockchain.

**Linked Blocks**

A blockchain consists of a collection of data (a *block*) linked to the previous block. How are they linked? A block contains data, and each block references the block preceding it, so they are linked just as a chain link would be connected to the chain link before it. Take a look at Figure 1-2; as you can see, each block is referencing the previous block.

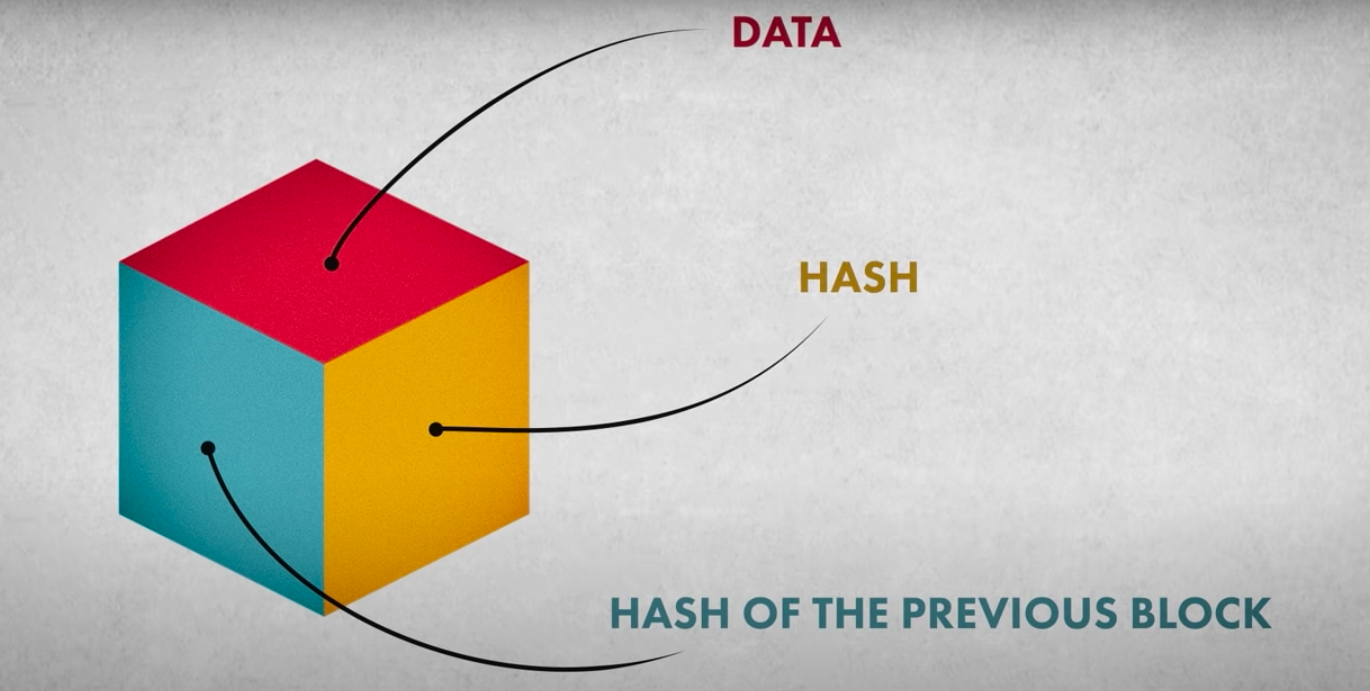
So, a blockchain contains blocks, which hold records of transactions. The private keys are held by the owner to show proof of ownership (this is the digital signature), so no one without the private key can decrypt the string and claim ownership. This combination of public keys and private keys represents electronic cash.

**How does Blockchain work?**

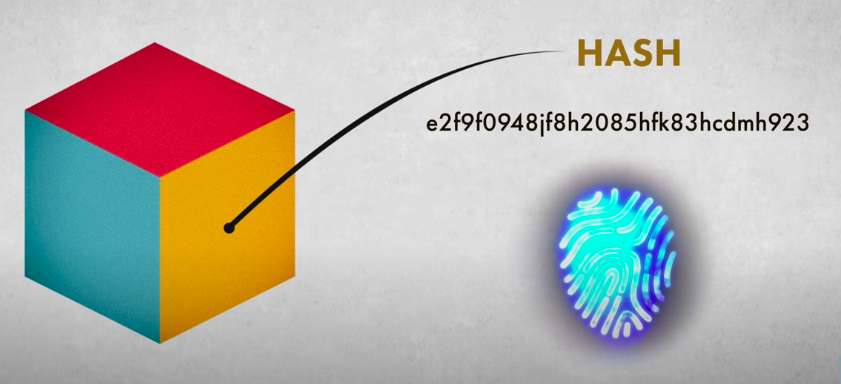
As the name suggests a blockchain is nothing but a chain of blocks with some information.

Each Block has

1. Data
2. Hash
3. Hash of the previous block



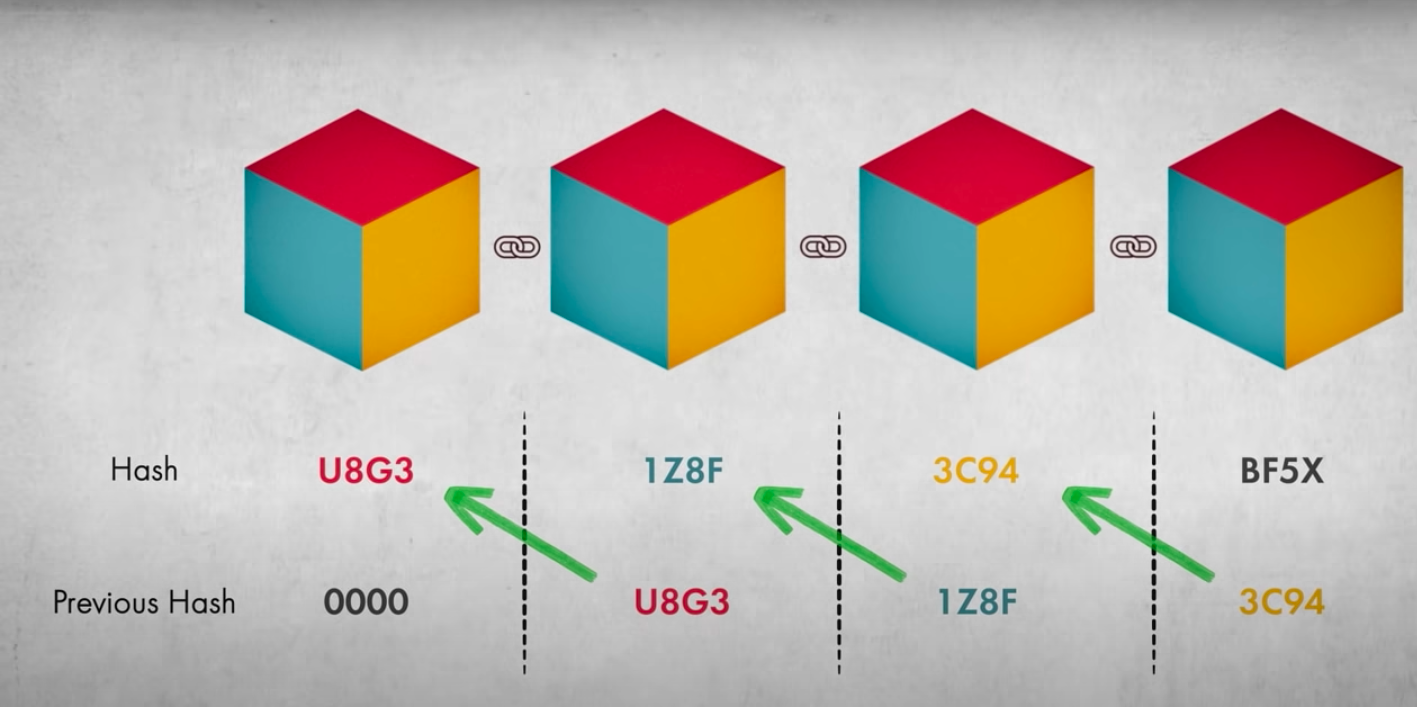
What is Hash?

A Hash can be understood as a fingerprint which is unique to each block. It identifies a block and all of its contents, and it’s always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.Therefore, the hash

is very useful when you want to detect changes to intersections. If the fingerprint of a block changes, it does not remain the same block.

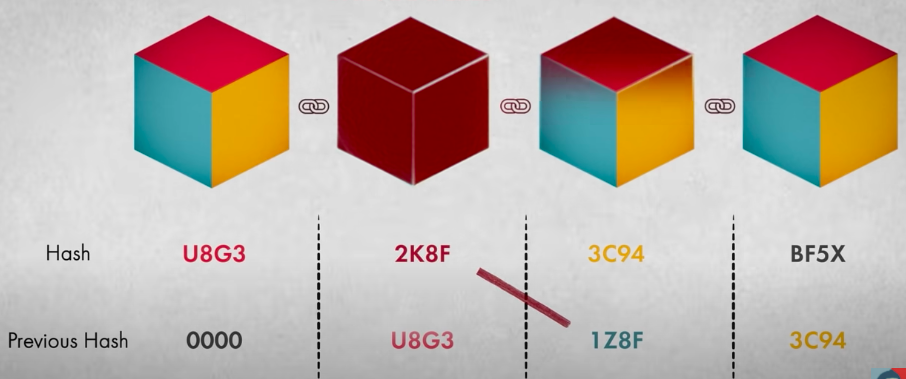
Consider the following example, where we have a chain of 4 blocks. The 1st block has no predecessor. Hence, it does not contain the previous block. Block 2 contains a hash of block 1. While block 3 contains Hash of block 2 and Block 4 contains a hash of block 3.

Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure.

****

But what happens when someone tries to tamper the transaction?

Assume an attacker is able to change the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have the correct hash of the previous block.



Therefore, changing a single block can quickly make all following blocks invalid.

**Types of Blockchain**

There are different types of blockchains possible in the ecosystem.

1. **Public –**  
   A public blockchain is also known as permission-less blockchain. Here, everyone can be a part of this blockchain and can participate by running as a node, by mining a block or by making transactions in the blockchain. Bitcoin and Litecoin are examples of public blockchains.
2. **Private –**  
   A private blockchain is also known as permissioned blockchain. Here, there are restrictions on the participation as only selected individuals or member of an organisation can be a part of the blockchain. Multichain and Hyperledger projects (Fabric, Sawtooth) are examples of private blockchain.
3. **Consortium –**  
   A consortium blockchain are said to be partially-decentralised or semi-decentralised. It is controlled by a group of organisations unlike one organisation as in private blockchain. The member organisations has the authority to participate by running as a full node, by mining etc. R3 and EWF (Energy Web Foundation) are examples of consortium blockchain.

**Double Spending Problem**

A digital signature (public keys and private keys) securely ensures a party’s identity is kept private and electronic cash is stored.

This concept of a private-public key combo enables you to encrypt and decrypt strings and keep a string safe, However, it is still not enough to solve the biggest problem of digital currency—double spending.

When you use fiat money (a paper money made legal by a government) such as U.S. dollars or euros, the paper is inconvertible, which means that once you gave the paper away, you cannot spend it again. In cryptocurrency, what happens if you prove ownership and send your digital asset twice at the exact same time? This could lead to *double spending*.

Hackers can try to reproduce digital assets as well as potentially double spend them, which cryptocurrency had to solve before it could be used as a digital currency.

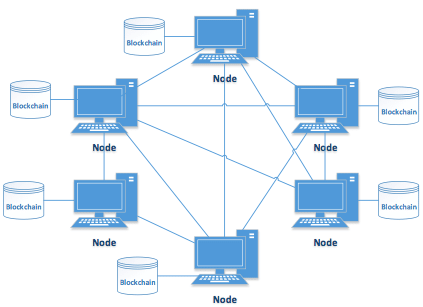
Blocks that hold keys are not enough to provide security and solve the double-spending potential issue to form a digital currency.

Bitcoin solves this problem by creating a network of computers and proving that no attempts of double spending have occurred. This is done by having all the computers on the network aware of every transaction. All the transactions are shared with all the computers in the network.

This network is called P2P Network

**Double Spending Solution: P2P Network**

In cryptocurrency, using a peer-to-peer network provided the solution to solve the double-spending problem.



## **Introduction to P2P Network and its Types**

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.

Today, P2P networks are the foundation of most of the cryptocurrencies, thus making up a significant portion of the blockchain industry. Want to get in-depth knowledge about Blockchain technology? Check out the best blockchain certification courses now.

## **P2P vs. Traditional Client-Server Systems**

Before understanding the role of these networks in blockchain, let’s distinguish between P2P and traditional client-server architecture. The critical difference between both the systems is that in Client-Server, there is a dedicated server and specific clients whereas, in P2P, it is maintained by a distributed network of users, where each node can act both as a server and a client.

## **Role of P2P in Blockchain**

P2P is a technology that is based on a very simple principle, and that is the concept of decentralization. The peer-to-peer architecture of blockchain allows all cryptocurrencies to be transferred worldwide, without the need of any middle-man or intermediaries or central server. With the distributed peer-to-peer network, anyone who wishes to participate in the process of verifying and validating blocks can set up a Bitcoin node.

Blockchain is a decentralized ledger tracking of one or more digital assets on a peer-to-peer network. When we say a peer-to-peer network, it means a decentralized peer-to-peer network where all the computers are connected in some way, and where each maintains a complete copy of the ledger and compares it to other devices to ensure the data is accurate. This is unlike a bank, where transactions are stored privately and are managed only by the bank.

Want to implement blockchain on business applications? Get started with blockchain certification courses now.

## **P2P: Pros & Cons**

Let’s talk about the advantages first. Here are few undeniable benefits of the P2P network in the blockchain.

* As blockchain is a decentralized system of peer to peer network, it is highly available due to decentralization.
* Because of P2P networking capability, even if one peer gets down, the other peers are still present. Thus nobody can take down the blockchain.
* P2P networks offer greater security compared to traditional client-server systems.
* When you are using cloud computing to store your data, you need to trust AWS and Google drives, but with the blockchain, because it utilizes a peer to peer network you don’t need to trust any third parties which can modify your crucial data. These are non-resistant to censorship by central authorities.
* These networks are virtually immune to the Denial-of-Service (DoS) attacks.
* The distributed peer-to-peer network, when paired with a majority consensus requirement, gives blockchains a relatively high degree of resistance to malicious activity.

P2P network in blockchain, however, raises few concerns. As in blockchain, instead of a central server, distributed ledgers must be updated on every single node, adding transactions requires a considerable amount of computational power. Although this provides an increased level of security, it significantly reduces efficiency, and this acts as one of the main hindrances in terms of scalability and mass adoption.

# **Consensus Algorithms in Blockchain**

We know that Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency. There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified. This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network.

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

Now, we will discuss various consensus algorithms and how they work.

1. **Proof of Work (PoW):**  
   This consensus algorithm is used to select a miner for the next block generation. Bitcoin uses this PoW consensus algorithm. The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution. This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block.
2. **Proof of Stake (PoS):**  
   This is the most common alternative to PoW. Ethereum has shifted from PoW to PoS consensus. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stake. After that, all the validators will start validating the blocks. Validators will validate blocks by placing a bet on it if they discover a block which they think can be added to the chain. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets and their stake increase accordingly.  
   In the end, a validator is chosen to generate a new block based on their economic stake in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.
3. **Proof of Burn (PoB):**  
   With PoB, instead of investing into expensive hardware equipment, validators ‘burn’ coins by sending them to an address from where they are irretrievable. By committing the coins to an unreachable address, validators earn a privilege to mine on the system based on a random selection process. Thus, burning coins here means that validators have a long-term commitment in exchange for their short-term loss.  
   Depending on how the PoB is implemented, miners may burn the native currency of the Blockchain application or the currency of an alternative chain, such as bitcoin. The more coins they burn, the better are their chances of being selected to mine the next block.  
   While PoB is an interesting alternative to PoW, the protocol still wastes resources needlessly. And it is also questioned that mining power simply goes to those who are willing to burn more money.
4. **Proof of Capacity:**  
   In the Proof of Capacity consensus, validators are supposed to invest their hard drive space instead of investing in expensive hardware or burning coins. The more hard drive space validators have, the better are their chances of getting selected for mining the next block and earning the block reward.
5. **Proof of Elapsed Time:**  
   PoET is one of the fairest consensus algorithms which chooses the next block using fair means only. It is widely used in permissionned Blockchain networks. In this algorithm, every validator on the network gets a fair chance to create their own block. All the nodes do so by waiting for random amount of time, adding a proof of their wait in the block. The created blocks are broadcasted to the network for others consideration. The winner is the validator which has least timer value in the proof part. The block from the winning validator node gets appended to the Blockchain. There are additional checks in the algorithm to stop nodes from always winning the election, stop nodes from generating a lowest timer value.

There also exist other consensus algorithms like Proof of Activity, Proof of Weight, Proof of Importance, Leased Proof of Stake, etc. It is therefore important to wisely choose one as per the business network requirement because Blockchain networks cannot function properly without the consensus algorithms to verify each and every transaction that is being committed.