**Cryptocurrency**

Cryptocurrency, sometimes called crypto-currency or crypto, is any form of currency that exists digitally or virtually and uses cryptography to secure transactions. Cryptocurrencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units.

**What is cryptocurrency?**

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It’s a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

Cryptocurrency received its name because it uses encryption to verify transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers. The aim of encryption is to provide security and safety.

The first cryptocurrency was Bitcoin, which was founded in 2009 and remains the best known today. Much of the interest in cryptocurrencies is to trade for profit, with speculators at times driving prices skyward.

**How does cryptocurrency work?**

Cryptocurrencies run on a distributed public ledger called blockchain, a record of all transactions updated and held by currency holders.

Units of cryptocurrency are created through a process called mining, which involves using computer power to solve complicated mathematical problems that generate coins. Users can also buy the currencies from brokers, then store and spend them using cryptographic wallets.

If you own cryptocurrency, you don’t own anything tangible. What you own is a key that allows you to move a record or a unit of measure from one person to another without a trusted third party.

Although Bitcoin has been around since 2009, cryptocurrencies and applications of blockchain technology are still emerging in financial terms, and more uses are expected in the future. Transactions including bonds, stocks, and other financial assets could eventually be traded using the technology.

[Link1](https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency)

**Creation of coins :-**

[Link1](https://www.geeksforgeeks.org/how-are-cryptocurrencies-created/#:~:text=The%20units%20of%20cryptocurrency%20are,mathematical%20problems%20that%20generate%20coins.) [Link2](https://www.investopedia.com/how-to-make-a-cryptocurrency-5215343) [Link3](https://www.datadriveninvestor.com/how-to-create-your-own-cryptocurrency/)

**Double Spending**

Although Blockchain is secured, still it has some loopholes. Hackers or malicious users take advantage of these loopholes to perform their activities.

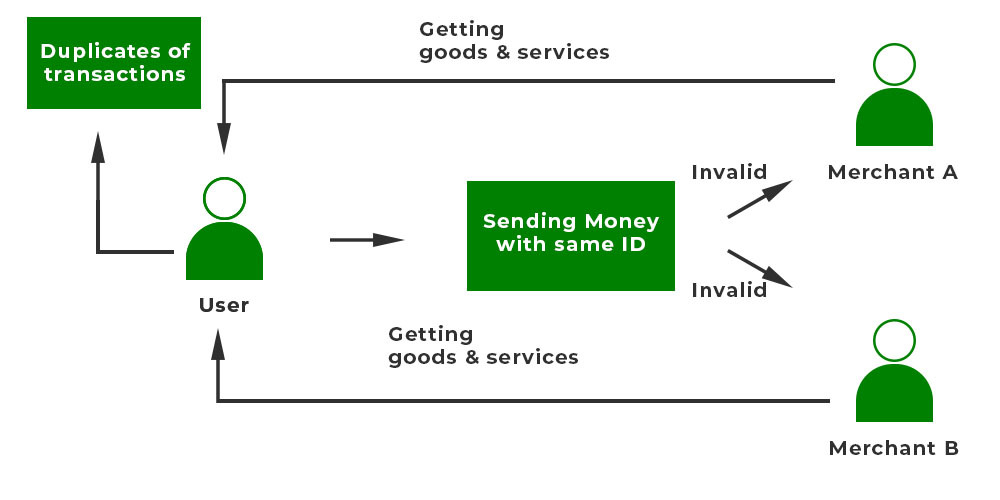
* [Double spending](https://www.geeksforgeeks.org/solutions-to-prevent-double-spending-of-bitcoins/) means the expenditure of the same digital currency twice or more to avail the multiple services. It is a technical flaw that allows users to duplicate money.
* Since digital currencies are nothing but files, a malicious user can create multiple copies of the same currency file and can use it in multiple places.
* This issue can also occur if there is an alteration in the network or copies of the currency are only used and not the original one.
* There are also double spends that allow hackers to reverse transactions so that transaction happens two times.
* By doing this, the user loses money two times one for the fake block created by the hacker and for the original block as well.
* The hacker gets incentives as well for the fake blocks that have been mined and confirmed.

**How Does Double Spending Happen?**

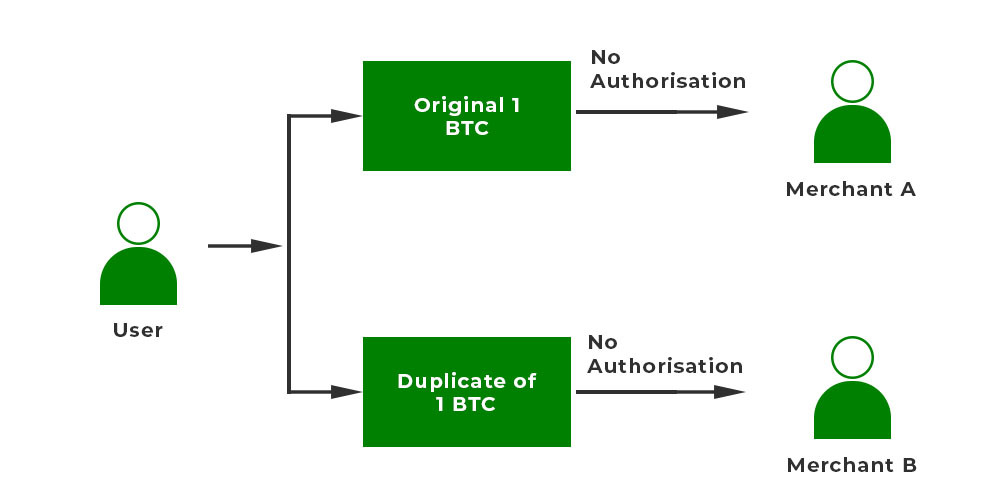
Double spending can never arise physically. It can happen in online transactions. This mostly occurs when there is no authority to verify the transaction. It can also happen if the user’s wallet is not secured. Suppose a user wants to avail of services from Merchant ‘A’ and Merchant ‘B’.

* The user first made a digital transaction with Merchant ‘A’.
* The copy of the cryptocurrency is stored on the user’s computer.
* So the user uses the same cryptocurrency to pay Merchant ‘B’
* Now both the merchants have the illusion that the money has been credited since the transactions were not confirmed by the miners.

This is the case of double spending.



**Example:**Suppose a user has 1 BTC. He/She wants to avail of services from merchant A and merchant B. The user creates multiple copies of the same BTC and stores it. The user first sends the original BTC to Merchant A and gets the service. Simultaneously, the user sends the copied version of 1 BTC to Merchant B. Since the second transaction was not confirmed by other miners, the merchant accepts the bitcoin and sends the service. But the cryptocurrency that was sent is invalid. This is the case of Double Spending.



### Types Of Double Spending Attacks

There are different types of Double Spending attacks:

* **Finney Attack:** Finney Attack is a type of Double spending Attack. In this, a merchant accepts an unauthorized transaction. The original block is eclipsed by the hacker using an eclipse attack. The transaction is performed on an unauthorized one. After that, the real block shows up and again the transaction is done automatically for the real block. Thus the merchant loses money two times.
* **Race attack:**is an attack in which there is a ‘race’ between two transactions. The attacker sends the same money using different machines to two different merchants. The merchants send their goods but transactions get invalid.
* **51% Attack:**This type of attack is prevalent in small blockchains. Hackers usually take over 51% of the mining power of blockchain and therefore can do anything of their own will.

**How Bitcoin Handles Double Spending?**

[Bitcoin](https://www.geeksforgeeks.org/what-is-bitcoin/) is one of the most popular blockchains. To combat Double spending it uses some security measures. There are two types of examples of double spending in BTC.

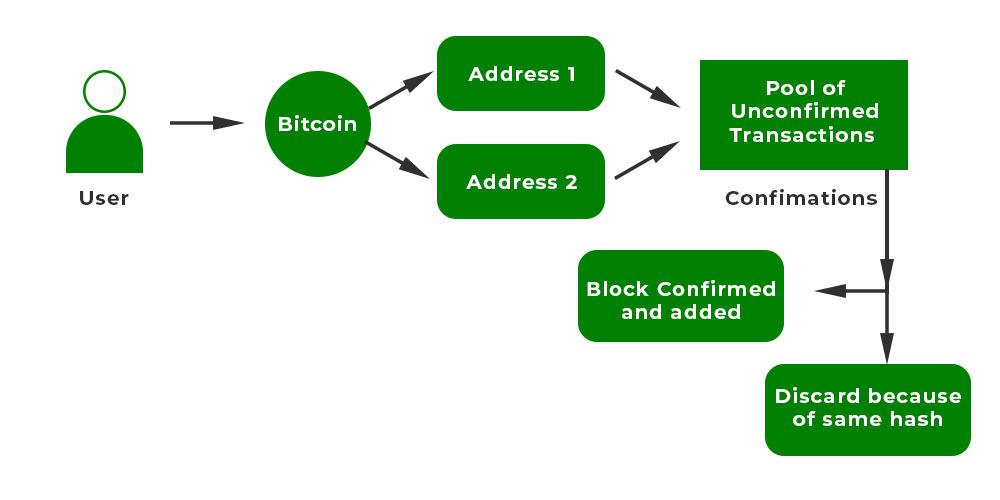
1. The first case is making duplicates of the same bitcoin and sending it to multiple users.
2. The second case is performing the transaction and reversing the already sent transaction after getting the service.

To tackle these double-spending issues, some security measures are taken. They are:

* **Validation:**Validation of transactions by a maximum number of nodes in the network. Once a block is created, it is added to a list of pending transactions. Users send validation for the block. If the verifications are done then only the block is added to the blockchain.
* **Timestamp:**The confirmed transactions are timestamped, therefore they are irreversible. If a transaction is involved with a bitcoin it is verified and done. But in the future, if other transactions are made with the same bitcoin, the transactions will be canceled.
* **Block Confirmations:** Merchants get block confirmations so that they are assured that there was no case of double spending. In bitcoin, a minimum of 6 confirmations are done.
* **Saving copies:** A copy of each transaction is kept at each node so in case of network failure the whole network does not go down.

These security features have reduced double spending to a large extent. Let us discuss a detailed example of how bitcoin handles double-spending.

* A user wants to spend 2 BTC. He/She can create multiple copies of the same cryptocurrency.
* The user can send the same cryptocurrency to two different addresses say ‘Bob’ and ‘Alice’.
* Both of these transactions are sent to the pool of unconfirmed transactions.
* The first transaction T1 would be approved via the confirmation mechanism.
* The confirmation mechanism states that a minimum of six confirmations by miners should be done for block validation. The block is added to the network.
* However, the second transaction T2 didn’t get sufficient confirmation so it would be recognized as invalid by the confirmation process. The block with the highest number of confirmations is accepted and the other one is rejected. So transaction T1 is valid, and Alice received the bitcoin.



### **Solutions To Prevent Double Spending**

Double Spending can be prevented using two approaches: Centralized and Decentralized

* **Centralized Approach:**In this case, a secured third party is employed to verify the transactions. The third-party can track each of the user’s balances. Suppose a user makes a transaction. The third-party identifies the transaction with a unique identity. Then it verifies the transaction and allows the transaction. The problem is that suppose we want to make transactions with other countries where a third party is not required. So in such cases, decentralized systems come into play. another drawback is if the whole system fails, the users cannot have access.
* **Decentralized Approach:**This approach is used by Bitcoin. In this, there is no involvement of central authority. Each transaction is verified using powerful algorithms. The decentralized approach proved to be more secure than the centralized approach. Protocols are established and each protocol does its job at each step. Therefore this also promotes transparency.

### **How to Combat Double Spending?**

Double spending has been minimized to a large extent as companies are using many security features. But we as users also have some responsibility so that such attacks don’t happen.

* Any user should wait for a minimum of six confirmations of the transaction before performing another transaction. In the blockchain, more the confirmations by different users, lesser will be double spending attacks.
* Users should keep their hardware resources safe so that hackers do not misuse them for their own purposes. Often hackers target the hardware part because the hardware is costly. If they somehow steal the hardware, they can roll back any transaction or alter information.
* Users should delete spam mails and avoid phishing to avoid unnecessary malware attacks Phishing is a very common attack by hackers as hackers target login credentials.
* Software should be updated regularly with the latest antivirus installed. If the software is not up to date then the bugs present can cause major damage.

### **How Successful Double Spending is Administered?**

With the increasing dependency on the blockchain, double spending attacks have also become a major problem. Many companies have adopted security features.

* Features like confirmation of the transaction by the nodes have been adopted. A minimum of six confirmations is required to approve the transaction.
* The blocks once created are immutable. They are made irreversible so that no transaction is reverted back.
* The network’s distributed ledger of transactions autonomously records each transaction. Each node has a copy of all transactions that are being done in the network.
* Verification of each transaction’s authenticity is done by Blockchain protocols to prevent double-spending. The concept of hashing is adopted. Here each block has a unique hash.

### **Disadvantages of Blockchain Concerning Double Spending**

There are many disadvantages of blockchain concerning Double Spending:

* **Control of the blockchain:**The biggest disadvantage is if the hackers manage to take control of 51% computation power, they can do any transaction of their own will and can steal other users’ money. Therefore there is a threat to security as millions and millions of money are involved in transactions.
* **Alteration of information:** Transaction information can also be altered by hackers. They can mine blocks and hide the original blocks using attacks like Eclipse attack, Finney Attack, etc.
* **No authority:**The third major problem is no central authority is present to verify the transactions. But these problems will be eliminated if companies take proper security measures and users are also aware of the measures.

[Link1](https://www.geeksforgeeks.org/what-is-double-spending-in-blockchain/#:~:text=Double%20spending%20means%20the%20expenditure,allows%20users%20to%20duplicate%20money.) [Link2](https://www.javatpoint.com/blockchain-double-spending)

**Bitcoin Script :-**

Bitcoin’s scripting language is simply called Script. All Bitcoin scripts are written in Script. It is a simple language that is not Turing complete, meaning it lacks several logical functions, including loops. This is done to ensure that no Bitcoin script can consume inordinate computing power and harm nodes on the network.

Script is used almost exclusively to lock and unlock bitcoin, not to build applications or run programs. Script’s simplicity also gives Bitcoin security and makes it easier for developers to avoid losing money while designing wallets or applications on top of Bitcoin.

All Bitcoin transactions use Script to define how outputs can be spent. In other words, the script of a Bitcoin transaction determines to whom the bitcoin was sent. Bitcoin has a few different scripts, with [Pay-to-Public-Key-Hash (P2PKH)](https://river.com/learn/terms/p/p2pkh/) being the most popular. P2PKH is a simple script which pays bitcoin to an address.

[Link1](https://river.com/learn/terms/s/script-bitcoin/#:~:text=All%20Bitcoin%20transactions%20use%20Script,pays%20bitcoin%20to%20an%20address.) [Link2](https://komodoplatform.com/en/academy/bitcoin-script/) [Link3](https://en.bitcoin.it/wiki/Script)

**P2P Network :-**

A peer-to-peer network is a simple network of computers. It first came into existence in the late 1970s. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server in the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.

### **Types of P2P networks**

1. **Unstructured P2P networks:** In this type of P2P network, each device is able to make an equal contribution. This network is easy to build as devices can be connected randomly in the network. But being unstructured, it becomes difficult to find content. For example, Napster, Gnutella, etc.
2. **Structured P2P networks:**It is designed using software that creates a virtual layer in order to put the nodes in a specific structure. These are not easy to set up but can give easy access to users to the content. For example, P-Grid, Kademlia, etc.
3. **Hybrid P2P networks:**It combines the features of both P2P networks and client-server architecture. An example of such a network is to find a node using the central server.

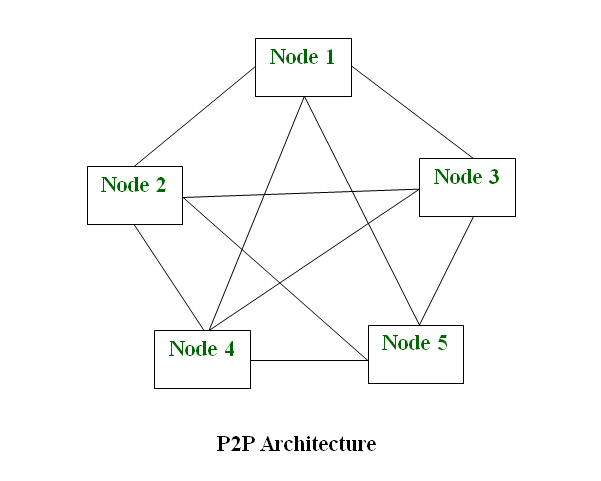
### **Features of P2P network**

* These networks do not involve a large number of nodes, usually less than 12. All the computers in the network store their own data but this data is accessible by the group.
* Unlike client-server networks, P2P uses resources and also provides them. This results in additional resources if the number of nodes increases. It requires specialized software. It allows resource sharing among the network.
* Since the nodes act as clients and servers, there is a constant threat of attack.
* Almost all OS today support P2P networks.

### **P2P Network Architecture**

In the P2P network architecture, the computers connect with each other in a workgroup to share files, and access to internet and printers.

* Each computer in the network has the same set of responsibilities and capabilities.
* Each device in the network serves as both a client and server.
* The architecture is useful in residential areas, small offices, or small companies where each computer act as an independent workstation and stores the data on its hard drive.
* Each computer in the network has the ability to share data with other computers in the network.
* The architecture is usually composed of workgroups of 12 or more computers.



### **How Does P2P Network Work?**

Let’s understand the working of the Peer-to-Peer network through an example. Suppose, the user wants to download a file through the peer-to-peer network then the download will be handled in this way:

* If the peer-to-peer software is not already installed, then the user first has to install the peer-to-peer software on his computer.
* This creates a virtual network of peer-to-peer application users.
* The user then downloads the file, which is received in bits that come from multiple computers in the network that have already that file.
* The data is also sent from the user’s computer to other computers in the network that ask for the data that exist on the user’s computer.

Thus, it can be said that in the peer-to-peer network the file transfer load is distributed among the peer computers.

### **Applications of P2P Network**

Below are some of the common uses of P2P network:

* **File sharing:**P2P network is the most convenient, cost-efficient method for file sharing for businesses. Using this type of network there is no need for intermediate servers to transfer the file.
* **Blockchain:**The P2P architecture is based on the concept of decentralization. When a peer-to-peer network is enabled on the blockchain it helps in the maintenance of a complete replica of the records ensuring the accuracy of the data at the same time. At the same time, peer-to-peer networks ensure security also.
* **Direct messaging:**P2P network provides a secure, quick, and efficient way to communicate. This is possible due to the use of encryption at both the peers and access to easy messaging tools.
* **Collaboration:**The easy file sharing also helps to build collaboration among other peers in the network.
* **File sharing networks:**Many P2P file sharing networks like G2, and eDonkey have popularized peer-to-peer technologies.
* **Content distribution:**In a P2P network, unline the client-server system so the clients can both provide and use resources. Thus, the content serving capacity of the P2P networks can actually increase as more users begin to access the content.
* **IP Telephony:**Skype is one good example of a P2P application in VoIP.

### **Advantages of P2P Network**

* **Easy to maintain:**The network is easy to maintain because each node is independent of the other.
* **Less costly:**Since each node acts as a server, therefore the cost of the central server is saved. Thus, there is no need to buy an expensive server.
* **No network manager:** In a P2P network since each node manages his or her own computer, thus there is no need for a network manager.
* **Adding nodes is easy:**Adding, deleting, and repairing nodes in this network is easy.
* **Less network traffic:**In a P2P network, there is less network traffic than in a client/ server network.

### **Disadvantages of P2P Network**

* **Data is vulnerable:**Because of no central server, data is always vulnerable to getting lost because of no backup.
* **Less secure:**It becomes difficult to secure the complete network because each node is independent.
* **Slow performance:**In a P2P network, each computer is accessed by other computers in the network which slows down the performance of the user.
* **Files hard to locate:**In a P2P network, the files are not centrally stored, rather they are stored on individual computers which makes it difficult to locate the files.

[Link1](https://www.geeksforgeeks.org/what-is-p2ppeer-to-peer-process/) [Link2](https://www.investopedia.com/terms/p/ptop.asp#:~:text=Peer%2Dto%2Dpeer%20refers%20to%20the%20direct%20exchange%20of%20some,the%20most%20widely%20used%20cryptocurrency.)

**Transaction in Bitcoin Network :-**

[Link1](https://www.geeksforgeeks.org/how-bitcoin-transaction-works/#:~:text=Bitcoin%20transaction%20means%20sending%20bitcoin,present%20in%20the%20blockchain%20network.) [Link2](https://river.com/learn/how-does-a-bitcoin-transaction-work/#what-is-a-bitcoin-transaction) [Link3](https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/)

**Bitcoin Mining :-**

[Link1](https://www.geeksforgeeks.org/how-does-bitcoin-mining-work/) [Link2](https://www.geeksforgeeks.org/bitcoin-miners-and-bitcoin-mining/)

**Block propagation and Block relay :-**

It’s an average time that is needed for the new block to reach the majority of nodes in the network. In a large decentralized network like Bitcoin, whenever the new block is generated, it is broadcasted according to the Gossip protocol. If some node has got the new valid block, it informs nodes connected to it about its new possession.

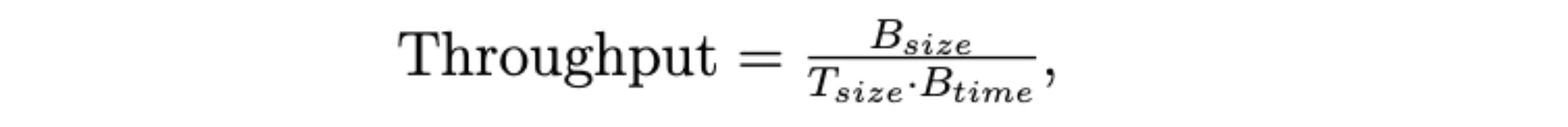
Then the node transfers this block to those nodes which asked it to do that. Before the block reaches each full-node in the network, it passes through 7 intermediary nodes. It’s important that every honest node verifies the block before relaying it to other peers.

It’s important that even in the worst-case scenario, the propagation delay should be reasonable so that miners will keep their nodes synchronized most of the time, and will always verify proposed blocks.

Whenever people talk about the scalability of the blockchain, they mention the transaction throughput of the system. However, people forgot that improvements in transaction throughput shouldn’t compromise the network’s security, or raise data storage requirements for nodes desiring to participate in the network.

These modifications could decrease the number of independent transaction validators in the network, thereby reducing decentralization.

Transaction throughput in Bitcoin could be easily calculated using the formula:



where

*Bsize is the block size in bytes,*

*Tsize is the average size of transaction record in the block,*

*Btime is the average time between consecutive blocks in the blockchain.*

[Link1](https://hackernoon.com/understanding-the-block-propagation-problem-in-blockchains-1t2s3x9b) [Link2](https://www.youtube.com/watch?v=ZXhouRy0VXQ)(Video)

**Consensus introduction:-**

 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.

Types:-

1. **Proof of Work (PoW)**
2. **Proof of Stake (PoS)**
3. Practical Byzantine Fault Tolerance (PBFT)
4. **Proof of Burn (PoB)**
5. **Proof of Capacity**
6. **Proof of Elapsed Time**

[Link1](https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/)[link2](https://www.techtarget.com/whatis/definition/consensus-algorithm#:~:text=Blockchain%20networks%20rely%20on%20consensus,users%20from%20validating%20bad%20transactions.)

**Distributed consensus in open environments :-**

[Link1](https://notepub.io/notes/blockchain-technology/bitcoin/bitcoin-consensus-in-an-open-system/) [Link2](https://www.alibabacloud.com/blog/from-distributed-consensus-algorithms-to-the-blockchain-consensus-mechanism_595315)

**Consensus in a Bitcoin network:-**

[Link1](https://notepub.io/notes/blockchain-technology/bitcoin/bitcoin-consensus-in-bitcoin/)

**Remaining Notes of Blockchain 🡪** [**Link**](https://github.com/Bandhan-singh-katoch/Blockchain/tree/main/Blockchain%20Notes)