**Bitcoin Consensus**

**Bitcoin Consensus :-**

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

[**Proof of Work (PoW)**](https://www.geeksforgeeks.org/blockchain-proof-of-work-pow/) **:-**

[**Link1**](https://www.geeksforgeeks.org/blockchain-proof-of-work-pow/)

**Hashcash PoW :-**

"Hashcash is a proof-of-work system used to limit email spam and denial-of-service attacks, and more recently has become known for its use in bitcoin (and other cryptocurrencies) as part of the mining algorithm. Hashcash was proposed in March 1997 by Adam Back."

The idea is that a message, like an email, "proves" that it is a legitimate message by including hashing some string in such a manner that it proves that a computer spent some time/energy on a particular algorithm -- in particular, computing a [SHA-1](https://en.wikipedia.org/wiki/SHA-1) hash such that the first 20 bits of the hash are 0. Because this takes a certain amount of computational time to find such a qualifying hash through brute force, it costs the sender a small amount to find the hash, which is seen as prohibitive for spammers that send large number of emails. A hashcash can be viewed as "a white-listing hint to help hashcash users avoid losing email due to content based and blacklist based anti-spam devices."

This "proof of work" concept is primarily used nowadays as the bitcoin mining function. These "act as a vote in the blockchain evolution and validate the blockchain transaction log." Or, to put it another way: "Bitcoin uses Hashcash to provide security from malicious alterations of the Blockchain, by imposing a cost for alteration that a miner must hope to recoup through rewards given for cooperation... In Bitcoin, the difficulty of the Hashcash problem is varied over time depending on the recent history of solution times, targeting a ten minute solution on average."

**How does HashCash work?**

It is based on the idea that if a certain user has used their processor to generate this stamp, it is unlikely that they are a spammer. Receivers with a very low almost negligible computational cost can verify this. In this way we can guarantee that it is not spam.

Decrypting the seal and ensuring it is not spam requires brute computing force. Or what is the same, we need the processor to find the answer by trial and error. Basically, the processor will test combinations according to certain criteria until it finds the correct answer. This would demonstrate that it is not spam.

Spammers base their business model on sending hundreds, thousands, and even millions of emails quickly. All this with a low cost of resources per message. For example; If a 5-second job is requested before sending an email, the cost of sending thousands of emails would be unbearable by the spammer. For its part, the receiver can quickly verify if there is a verification work prior to receiving the mail. With this, you can quickly filter and classify legal emails from spam attempts.

[Link1](https://en.wikipedia.org/wiki/Hashcash#:~:text=Hashcash%20is%20a%20proof%2Dof,part%20of%20the%20mining%20algorithm.) [Link2](https://www.codeproject.com/Articles/1172340/Hashcash-or-Proof-of-Work) [Link3](https://paybis.com/blog/what-is-hashcash/)

**Attacks on PoW:-**

As we know, the idea of Proof of Work was by Cynthia Dwork and Moni Naor. This permissionless consensus uses double SHA 256 which makes it secure from hackers. With proof of work, miners compete with each other to complete the transaction and get the bounty. Even it has many advantages like solving the double-spending problem and very difficult to tamper it, but it is not impossible to tamper if the hacker has high computational power.

In this article, we will see two major attacks by which PoW based systems can crash. They are :

1. Sybil Attacks
2. Denial of Service(DOS) Attacks

These are explained as following below with their solutions.

**1. Sybil Attacks :**  
In Sybil attacks, the attacker attempts to fill the network with the clients under its control. When this thing happens the attacker can actually control or get a monopoly over the network and these clients can do different kinds of actions based on the instruction from the attacker. They can refuse to relay the valid blocks or they can only relay the blocks which are generated by the attackers and those blocks can lead to double-spending.

In Simple language, The attacker can include multiple nodes in the network who can collectively compromise the Proof of Work mechanism.

**Solution –**  
To prevent Sybil attacks we have to diversify the connections i.e allowing outbound connection to one IP per / 16 IP address. So by diversifying the network it is expected that if the attacker generates multiple false miners the attacker will generate them within the same clustered network or subnet.

**Note :**  
Although this solution makes hard to launch sybil attacks but it doesn’t make it impossible.

**2. Denial of Service (DOS) Attacks :**  
In this attack, the attacker sends a lot of data to a particular node so that node will not able to process normal [Bitcoin](https://www.geeksforgeeks.org/what-is-bitcoin/) transactions. As a result, the metabolism of the mining procedure will get delayed which wastes the power for computation and in that meantime, the attacker can also send new nodes to the network resulting in a monopoly which is nothing but a Sybil attack.

**Solution –**  
To prevent DOS attacks there are several rules bitcoin have which are:

* No forwarding of orphaned blocks.
* No forwarding of double-spend transactions.
* No forwarding of same block or transactions
* Disconnect a peer that sends too many messages
* Restrict the block size to 1 MB (1mb according to Satoshi Nakamoto)
* Limit the size of the bitcoin script up to 10000 bytes.

As we have seen above there are 2 major attacks that can alter transactions in Proof of Work (PoW) based systems and we also discussed the solution for that. Now the question comes Can we break Bitcoin PoW?

The answer would be YES, even after taking care of all types of attacks Bitcoin PoW is computationally difficult to break, but not impossible. Because attackers can deploy high power servers to do more work than the total work of the [blockchain](https://www.geeksforgeeks.org/blockchain-technology-introduction/). There is a known case of successful double-spending.

[Link1](https://www.geeksforgeeks.org/types-of-attacks-on-pow-proof-of-work-based-systems/#:~:text=In%20this%20article%2C%20we%20will,Denial%20of%20Service(DOS)%20Attacks) [Link2](https://syssec.kaist.ac.kr/~yongdaek/courses/ee817/Presentation/BWH&FAW.pdf)

**The Monopoly Problem :-**

Proof of Work depends on the computing resources available to a miner. If a miner can possess a huge amount of computational resources, then there is a possibility that the miner can control the entire network or gain control over the network. It may happen that a minor can gradually generate a lot of blocks in the current blockchain. If a huge number of blocks in the blockchain go from a particular miner, then that particular miner can control the entire flow of transactions in the blockchain. This particular problem is called the monopoly problem in the bitcoin network.

A statistical theory called the “Tragedy of the Commons” says that such a monopoly can increase over time from an economic perspective.

Consider the methodology of bitcoin generation and rewarding mechanism in the network. Whenever the miner mines a new block, they get a reward. But, there is a limit on the generation of bitcoins from the mining procedure in the system’s entire life span. Whenever there is a limit on the generation of bitcoins from the mining procedure with time, the amount of reward given to the miners will drop. The number of bitcoins that can be generated will also gradually drop to make it saturated. Moreover, if the minors get fewer rewards, they will get discouraged from participating or joining as miners. If they get discouraged from participating as miners, the system will be left with few miners with enormous computing resources, and they may control the entire network.

The above practical problem is not there in today’s bitcoin network. However, with time it is expected that this kind of problem may arise. This is the shortcoming of the “Proof of Work” based system such as Bitcoin Cryptocurrency.

### **Proposed Solutions**

To reduce the monopoly problem, other consensus mechanisms came into practice. The most popular is the “Proof of Stake” (PoS) mechanism, and the bitcoin forum proposes it.

The idea was to make a general transition from a PoW to PoS based system when the bitcoins are getting widely distributed. It means the number of bitcoins is not under to control of one individual, and it is normally distributed amongst the bitcoin cryptocurrency users. The broad difference between these two are as follows:

* PoW: The probability of mining a block depends on the work done by the miner. So the amount of work to be done is totally depends on the computing resource possessed by the miner.
* PoS: The amount of bitcoin that the miner holds, instruct which miner can generate the next block. So if a miner holds one percent of the total bitcoins, then the miner can mine one percent of PoS blocks.

By putting this kind of restriction on the number of bitcoins that the miner holds and proportional to that, the miner will generate the Proof of Stake block. This reduces certain kinds of monopoly problems and makes the monopoly problem a difficult problem for a “Proof of Stake” based system. The inherent assumption is that the bitcoin is widely distributed by the “Proof of Work” based system. So every miner will participate in the mining procedure proportional to the amount of bitcoin the individual possesses.

[Link1](https://notepub.io/notes/blockchain-technology/bitcoin/what-is-the-inherent-problems-of-bitcoin-network-and-what-is-the-solution-pow-pos/#The_Monopoly_Problem)

**Proof-of-Stake :-**  
As understandable from the name, nodes on a network stake an amount of [cryptocurrency](https://www.geeksforgeeks.org/what-is-a-cryptocurrency/) to become candidates to validate the new block and earn the fee from it. Then, an algorithm chooses from the pool of candidates the node which will validate the new block. This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age based selection, randomization process) to make the selection fair to everyone on the network.

* **Coin-age based selection:**  
  The algorithm tracks the time every validator candidate node stays a validator. The older the node becomes, the higher the chances of it becoming the new validator.
* **Random Block selection:**  
  The validator is chosen with a combination of ‘lowest hash value’ and ‘highest stake’. The node having the best weighted-combination of these becomes the new validator.

**A typical PoS based mechanism workflow:**

1. Nodes make transactions. The PoS algorithm puts all these transactions in a pool.
2. All the nodes contending to become validator for the next block raise a stake. This stake is combined with other factors like ‘coin-age’ or ‘randomized block selection’ to select the validator.
3. The validator verifies all the transactions and publishes the block. His stake still remains locked and the forging reward is also not granted yet. This is so that the nodes on the network can ‘OK’ the new block.
4. If the block is ‘OK’-ed, the validator gets the stake back and the reward too. If the algorithm is using a coin-age based mechanism to select validators, the validator for the current block’s has its coin-age reset to 0. This puts him in a low-priority for the next validator election.
5. If the block is not verified by other nodes on the network, the validator loses its stake and is marked as ‘bad’ by the algorithm. The process again starts from step 1 to forge the new block.

**Features:**

* **Fixed coins in existence:**  
  There is only a finite number of coins that always circulate in the network. There is no existence of bringing new coins into existence(as in by mining in case of bitcoin and other PoW based systems). Note that the network starts with a finite number of coins or ‘initially starts with PoW, then shifts to PoS’ in some cases. This initiation with PoW is meant to bring coins/cryptocurrency in the network.
* **Transaction fee as reward to minters/forgers:**  
  Every transaction is charged some amount of fee. This is accumulated and given to the entity who forges the new block. Note that if the forged block is found fraudulent, the transaction fee is not rewarded. Moreover, the stake of the validator is also lost(which is also known as **slashing**).
* **Impracticality of the 51% attack:**  
  To conduct a 51% attack, the attacker will have to own 51% of the total cryptocurrency in the network which is quite expensive. This deems doing the attack too tedious, expensive and not so profitable. There will occur problems when amassing such a share of total cryptocurrency as there might not be so much currency to buy, also that buying more and more coins/value will become more expensive. Also validating wrong transactions will cause the validator to lose its stake, thereby being reward-negative.

**Advantages of PoS:**

* **Energy-efficient:**  
  As all the nodes are not competing against each other to attach a new block to the blockchain, energy is saved. Also, no problem has to be solved( as in case of Proof-of-Work system) thus saving the energy.
* **Decentralization:**  
  In blockchains like Bitcoin(Proof of Work system to achieve distributed consensus), an extra incentive of exponential rewards are in place to join a mining pool leading to a more centralized nature of blockchain. In the case of a Proof-of-Stake based system(like Peercoin), rewards are proportional(linear) to the amount of stake. So, it provides absolutely no extra edge to join a mining pool; thus promoting decentralization.
* **Security:**  
  A person attempting to attack a network will have to own 51% of the stakes(pretty expensive). This leads to a secure network.

**Weakness of a PoS mechanism:**

* **Large stake validators:**  
  If a group of validator candidates combine and own a significant share of total cryptocurrency, they will have more chances of becoming validators. Increased chances lead to increased selections, which lead to more and more forging reward earning, which lead to owning a huge currency share. This can cause the network to become centralized over time.
* **New technology:**  
  PoS is still relatively new. Research is ongoing to find flaws, fix them and making it viable for a live network with actual currency transactions.
* **The ‘Nothing at Stake’ problem:**  
  This problem describes the little to no disadvantage to the nodes in case they support multiple blockchains in the event of a blockchain split(blockchain forking). In the worst-case scenario, every fork will lead to multiple blockchains and validators will work and the nodes in the network will never achieve consensus.

**Blockchains using Proof-of-Stake:**

* Ethereum(Casper update)
* Peercoin
* Nxt

[Link1](https://www.geeksforgeeks.org/proof-of-stake-pos-in-blockchain/)

**Proof of Burn (PoB):**With PoB, instead of investing in expensive hardware equipment, the validators follow the following approach:

* They 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 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 validators 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. It is also questioned that mining power simply goes to those who are willing to burn more money.

**Why Proof of Burn Required?**

There were some drawbacks in the PoW consensus algorithm which made researchers work towards a new consensus algorithm i.e PoB.

* The first drawback is that the power consumption of PoW is very high. Miners are awarded by upgrading the ledger under a POW model. Computational power is employed to solve a math problem in exchange for remuneration. Greater the money a miner spends to solve the problem, the greater the chances that they will be allowed to mine blocks.
* PoW requires very high capital investments.

**How PoB Works?**

1. As the name itself suggests, there is something which should be burned. Here as we are talking in the context of virtual currency so it’s obvious that in PoB virtual currency is burned. The more the currencies are burned by miners the more they have the power to create blocks.
2. By burning we don’t exactly mean burning. It means not using that coin. This may be done if it is sent to somewhere where it can’t be spent. So miners send these coins to such addresses from where they can’t be used. It is sent to a public verifiable address where it cannot be accessed and thus can not be used.
3. When the coin is burnt its availability decreases leading to a potential increase in the value of the coin.
4. Now the question is why do we need to burn the coin? The basic explanation for this is that by destroying the currency, the consumer is displaying a big commitment to the currency by foregoing a narrow profit in exchange for a long-term profit.
5. To avoid any undue advantages for early adopters, the PoB has devised a method that allows for the periodic burning of crypto coins in order to maintain mining capacity. Any time a fresh block is mined, the energy of burned coins decreases slightly.
6. It is a deflationary idea in which the quantity of currencies reduces over time, increasing deficiency and, as a result, the currency holders’ value. Coins that grow their quantity over time, on the other hand, tend to lose value.

**Advantages of PoB:**

* It required very little power compared to PoW.
* It reduces energy consumption by wasting insignificant resources when coins are burned.
* It encourages long-term involvement in a project as a consumer is displaying a big commitment to the currency by foregoing a narrow profit in exchange for a long-term profit.
* The coin distribution is more fair compared to all other consensuses.

**Disadvantages Of PoB:**

* It is risky because one doesn’t know that will they gain the wealth they have burnt in the future or not.
* As coins are burnt, so technically if we see then resources are wasted.
* It may suffer from rich getting richer phenomena. In which those who are wealthy are getting wealthier by having more coins.

[Link1](https://www.geeksforgeeks.org/proof-of-burn-consensus-algorithm-in-blockchain/)

**Proof of Elapsed Time :-**

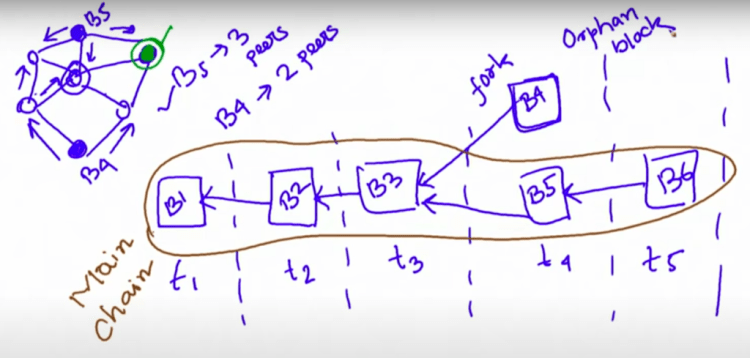
[Link1](https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp) [Link2](https://www.naukri.com/learning/articles/proof-of-elapsed-time-in-blockchain/)

**Bitcoin miners :-**  
Within the bitcoin network there are a group of people which are called miners and their role is to process and confirm transactions. Anybody can apply to be a miner, and you could run the client yourself.

**Role of bitcoin miners:**  
The role of the miners is to process and confirm transactions to chain together the blocks of transactions. Typically these miners use very powerful computers that are specifically designed to mine bitcoin transactions, and the way they do that is by actually solving math problems and resolving cryptography issues, because every one of these transactions need to be cryptographically encoded and secured. These mathematical problems are what actually ensures that the data is secure and nobody is tampering with that data.

### **Mining Bitcoin**

* The first and foremost task is to join the network, listen for transactions, and validate the proposed transactions from the network clients.
* Listen for the new blocks proposed by other miners, validate, and re-broadcast to the peer nodes. However, re-broadcast to a node that resides in a subnet of the bitcoin network. This is the standard policy followed by the bitcoin network nodes to avoid the Sybil attack.
* Collect the transactions for a predefined time, and construct a new block that includes all the transactions not included in a block of the main bitcoin blockchain received from the peer nodes.
* Participate in the mining procedure, where the miner task is to find a nonce to make the new block valid by utilizing the predefined difficulty function. That means the proposed new block must have a certain minimum number of zeros at the prefix. This is also called “Proof of Work” for consensus that a miner had done some work quicker than other miners in the bitcoin network.
* Once a miner can generate a valid block and quicker compared to other miners. The miner will broadcast that new block to the peers, and everybody in the peering system will accept that block if it is part of the main chain.
  + In the typical bitcoin network, multiple new valid blocks may be generated together by the different miners, and these blocks may or may not have a list of the same transactions.
  + Flooding rule: If multiple valid blocks are received from the peer nodes to an individual (a node or miner), the individual will accept the valid blocks but rebroadcast the block received from more peers.
  + The bitcoin blockchain always has the main chain and multiple orphans blocks. The main chain is the longest blockchain in the network, and orphans blocks are blocks from the fork chain that come out from the main chain but do not grow longer than the main chain.
* Whenever a miner finds a new valid block and can successfully append it to the main chain, the miner earns a certain reward. However, other mines may be trying to generate a valid block during the same period, but already one of the miners found the valid one. In that case, they will discard the generation process and start collecting all the new transactions that are not there in the new append block of the bitcoin blockchain.



### **Mining Difficulty**

It is a measure of how difficult it is to find a hash below the giving target. The mining procedure says that we are going to generate a 256-bit hash value. And there is mining difficulty, and it is represented in this way. Out of 256-bit hash, at least the first 64 bit should be zeros. This says that you have to generate a hash value wherein the final hash result, at least the first 64 bits, should be zero, and after that, the remaining bits can be zeros and ones.

This is the difficulty of the mining procedure, and based on that, we defined a metric called mining difficulty.  These difficulty parameters change for every 2016 block or every two weeks. The desire rate of generation of a block is every 10 minutes. If the system tries to generate a new block every 10 minutes, then 2 weeks are required to generate 2016 blocks.

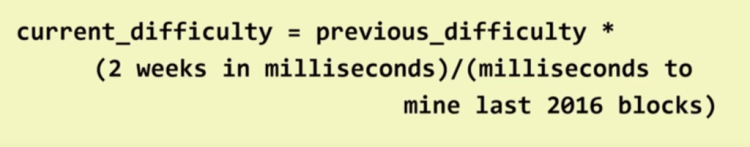
##### **Difficulty level readjustment mechanism (Valid for every 2 weeks or 2016 blocks):**

The difficulty level readjustment works as follows. The system finds out whether miners can generate 2016 blocks within 2 weeks or not.  If they are taking less time, that means the difficulty is too simple for the miners. So the system increases the difficulty parameters for the next round of 2016 blocks. On the other hand, if the miners take more than 2 weeks to generate 2016 blocks. It means that the current difficulty is too hard for the miners. So the system reduces the difficulty parameters for the next round of 2016 blocks.

This way, the bitcoin network dynamically changes the difficulty levels. In general, the change in difficulty is in proportion to the amount of time over or under two weeks the previous 2016 blocks took to find.

### **Difficulty formula**

The difficulty level readjustment happens after every two weeks or 2016 blocks, whichever comes first.  The expectation is that within 2 weeks, 2016 blocks must be generated so that inter-block generation time becomes equal to 10 minutes. The formula to generate or find the current difficulty is as follows:



### **Hash-rate versus Difficulty**

The hash is a random number between 0 and 2^{256}. To find a block, the hash must be less than a given target.

* The offset for difficulty 1 is 0xFFFF * 2^{208}. It means out of 265 bits, the initial 48 bits must be zeros, and the remaining can be either zeros or ones.
* In general, the offset for difficulty D is \texttt0xFFFF * 2^{208}/D. The D tells how many zeros would be there at the beginning. So the expected number of hashes need to be calculated as (D*2^{256})/(\texttt0xFFFF * 2^{208}).

The difficulty level dynamically changes the amount of hash that miners need to generate. If D is a more difficult value, then generate more hashes to get the resulted target well.

[Link1](https://www.geeksforgeeks.org/bitcoin-miners-and-bitcoin-mining/) [Link2](https://notepub.io/notes/blockchain-technology/bitcoin/what-is-the-task-of-miners-in-a-bitcoin-blockchain-network/)

# Bitcoin – Mining Pool

A **mining pool** is a joint group of multiple miners who share the processing power over a network to mine the new blocks and split the reward proportionally to the amount of work they contributed.

In a mining pool, hundreds or thousands of miners may be participating in a pool, and they communicate through some special protocols. The pool hoster can use one of the mining pool methods listed below for work assignment and reward sharing.

### **Mining Pool Methods**

##### Basic Setup:

* B is the per block reward minus the pool fee. It means whenever a miner participates in a block mining pool. Then there is a pool fee that needs to be paid by the miner. Here, B is the effective reward received by an individual miner for mining a block.
* p is the probability of finding a block in a shared attempt. (p = 1/D), where D is the block difficulty. Whenever multiple miners try to do that, and if D is block difficulty, then 1/D is the probability of finding a block.

There are multiple mechanisms for the distribution of share, and these are as follows:

##### **Pay Per Share (PPS)**

In this scheme, there is an instant guaranteed payout to a miner. Whenever a miner joins the mining pool, the miners are paid from the pool’s existing balance, and the miner share is calculated as R = B * p. Here, R is the amount of money given to every individual miner joining the pool. However, the miners get almost equal payment in this architecture, but the risk is at the pool operator. It may happen that the pool is not able to find out any new block, but this scheme follows instant and guaranteed payment to the participant who is participating in this pool. It may always happen that the pool is not getting any reward, but still, the pool operator needs to pay the individual miners.

##### **Proportional Share**

In this scheme, the miners earn the share until the pool finds a block at the end of the mining round. It means every mining round, whenever the pool is finding out a block. The total share will be divided by the individual miners: R = B * n/N, where n is the amount of individual work done, and N is all shared. The payments are made once a pool finds out a block.

##### **Pay per Last N Share (PPLNS)**

This scheme is similar to the proportional sharing method, along with the Miner’s reward is calculated based on N’s last shares, and the Miners get more profit for a short round.

### **Mining Pools – Pros and Cons**

The major advantage of the mining pool is that the small miners can participate in a mining procedure and have a kind of predictable mining like wherever there is a large number of miners who are participating in the mining procedure. There is a high probability that the pool will be able to find out a new block.

The disadvantage is that this kind of architecture leads to centralization, like only a list of mining pools can control the entire network. Gradually, independent miners will be forced to join the mining pool or discourage from participating in the mining procedure because of no guaranteed income from the mining.

[Link1](https://notepub.io/notes/blockchain-technology/bitcoin/what-is-bitcoin-mining-pool-and-what-are-the-different-methods-for-pool-sharing/)

## **Permissioned blockchains :-**

Now, let’s take a closer look at permissioned blockchains. *Permissioned blockchains* are blockchains that are closed (i.e., not publicly accessible) or have an access control layer. This additional layer of security means that the blockchain can only be accessed by users with permissions. Permissioned users are only able to perform blockchain operations within the strict confines of roles assigned to them by the ledger administrators and require that they authenticate themselves through certificates or digital identifier methods. In addition, the roles would dictate what information a user would be able to access.

### Aspects of a permissioned blockchain

**Decisions are authorized by a private group**

Decisions are made by the owners of the network through a central, pre-defined level.

**Security**

Permissioned blockchains provide the operating organization granular control over permissions, data access, and the scope of user roles.

**Decentralization isn’t fixed**

Permissioned blockchains can either be fully centralized or partially decentralized. Its members typically decide on the network’s level of decentralization and the mechanisms for consensus.

**Transparency is not required**

Unlike permissionless blockchains, permissioned blockchains do not need to be transparent. Transparency is optional, as most permissioned blockchain networks are specifically intended to not be transparent for security purposes. Levels of transparency usually depend on the goals of the organization running the blockchain network.  
In the meantime, the ledger maintains a record of every transaction and the identities of the participating parties.

**Lack of anonymity**

Access to the identify of every transactional participant can be crucial information for private entities concerned with accountability and a provable chain of custody. Every change is tracked to a specific user, so network administrators can have instantaneous access to has made a change to the system and when.

### **Advantages of permissioned blockchain**

One of the most significant advantages of permissioned blockchains is the high level of privacy and security they can provide. Without a verified set of credentials and access, no user can access or alter transaction information without permission.

Another advantage is flexibility when it comes to decentralization. It can be incremental or fully centralized, giving businesses more freedom to participate without having to worry about the risks associated with a highly centralized network.

Permissioned blockchains are also highly customizable and can accommodate configurations and integrations based on an organization’s needs. And with knowledge of every user and their actions on the network, a verifiable chain of custody can be established for every transaction.

Lastly, these types of blockchains are both scalable and highly performant due to the limited number of nodes needed to manage transaction verifications.

### **Disadvantages of permissioned blockchain**

While lack of transparency can be a potential point of concern for permissioned blockchains, the issue is usually mitigated by the implicit trust placed in the governing authority. In a business context, consensus mechanisms and the smart contracts that moderate transactions on the network are agreed upon by the participating parties and maintained in secure, isolated containers. With this additional layer of computational security and measure of implicit trust, a properly provisioned permissioned blockchain can offset the security risk posed by bad actors.

### **Why permissioned blockchains are ideal for business applications**

Many enterprise use cases require performance characteristics that permissionless blockchain technologies are presently unable to deliver because of limitations due to inefficiency and scalability. Additionally, in instances where permissioned blockchains are replacing existing secure, centralized networks, the identity of the participants is an essential requirement, such as in the case of financial transactions where Know-Your-Customer (KYC), Anti-Money Laundering (AML), and supply-chain provenance regulations must be followed.

In general, then, for a blockchain network to be ready for enterprise use, it should possess the following requirements:

* Participants must be identified/identifiable
* Networks need to be permissioned
* High transaction throughput performance
* Low latency of transaction confirmation
* Privacy and confidentiality of transactions and data pertaining to business transactions

### Business value

Let’s quickly review and see how permissioned blockchains stack up against these requirements. In terms of added value, permissioned blockchains:

* Increase business velocity by accelerating transactions, enabling new business models and revenue streams
* Automate multi-party business processes
* Reduce the cost and risk of using intermediaries
* Reduce the cost of fraud and regulatory compliance
* Improve data quality and timeliness by avoiding offline reconciliation and manual exception handling
* Increase auditability and trust; reduce audit costs

Comparing the two, permissioned blockchains are well positioned to achieve all the stated business requirements.

### **Use case examples**

So, how are permissioned blockchains being used by businesses? While still an emerging business model, they have already found a wide variety of applications. Permissioned blockchains have been used to manage supply chains, create contracts, handle claims, verify payment between parties, and administer user identity.

[Link1](https://developer.oracle.com/learn/technical-articles/permissioned-blockchain#:~:text=Use%20case%20examples,-So%2C%20how%20are&text=While%20still%20an%20emerging%20business,parties%2C%20and%20administer%20user%20identity.) [Link2](https://www.investopedia.com/terms/p/permissioned-blockchains.asp) [Link3](https://101blockchains.com/permissioned-blockchain/)

### **Challenges of Permissioned Solutions :-**

Permissioned blockchains are not free from challenges. In fact, implementing permissioned blockchain solutions can be a tough task. So, what makes it so challenging? There are many challenges that it has to go through. Few of them include data storage, messaging and integration, identity, smart contracts management, and so on.

As a business, many decisions need to be made before starting a permissioned network. For example, the company first needs to decide which blockchain platform to use. They also need to determine the blockchain runtime to use. After all, answers to these two questions will give them the development stack on which the development will take place.

Let’s have a look at the challenges that one might come across while developing permissioned solutions:

* **Integration:** One of the biggest challenges that a business or organization has to go through integration challenges, especially when using APIs for communication. To make it easy, you can use Rhombus, Chain Link, and Oraclize. They are great tools that will help you connect and integrate services more efficiently.
* **Data Privacy:** Privacy is a big concern, especially when it comes to regulated industries. To ensure proper privacy, they must meet specific requirements. [Quorum](https://101blockchains.com/quorum-blockchain-tutorial/) and Aztec are a good pick when it comes to developing permissioned blockchains that offer great privacy.
* **Data Access:** Accessing information in a permissioned blockchain can be slow compared. The right solution is to use The Graph which can expose data to the APIs and smart contracts for easy access.
* **Data Storage:** Data can be stored in many ways on a blockchain. However, not all of them are optimal, considering that a huge amount of data is stored on the blockchain. To ensure proper storage, it is advised to use data storage solutions such as IPFS Private Network, Big chain DB, and AWS Quantum Ledger.
* **Identity:** The last challenge that we are going to discuss is the participant’s identity problem. As it is permissioned network, the identity of the peers is already known, which can cause issues during the consensus computations. To simplify the issue, it is advised to use Azure BaaS or uPort that will help your business to better leverage their identity protocols and solutions for decentralized applications.

[Link1](https://101blockchains.com/permissioned-blockchain/) [Link2](https://vedveethi.co.in/eNote/BlkChain/BlkChain_Unit-3/ForwardHTML/Design%20issues%20for%20Permissioned%20blockchains.htm)

### **Consensus mechanisms in permissioned blockchain :-**

Because of the structure of permissioned blockchains, they don’t use the same types of consensus protocols as permissionless ones. Most commonly, organizations that deploy permissioned blockchains use one (or more) of the following three protocols: Practical Byzantine Fault Tolerance (PBFT), federated, or round-robin consensus.

**PBFT –**PBFT is an improved version of the original BFT protocol where all voting nodes much reach a consensus, but one or more parties are considered unreliable. In this model, a network’s safety and stability are guaranteed so long as the required minimum percentage of nodes are behaving honestly and properly.

**Federated (or Federated Byzantine Consensus)**- In a federated consensus, there’s a set of transaction validators trusted by each node in the blockchain that receives and sorts the transactions. Once a minimum number of these validators agree, a consensus is reached.

**Round-robin -** In a round-robin consensus, nodes are selected pseudo-randomly to create blocks. Once chosen, a node must pass through a cooling-off period before it can re enter the pool and be available again for consensus participation.

[Link(for detail)](https://www.researchgate.net/publication/351008008_A_Review_of_consensus_protocols_in_permissioned_blockchains)

**Distributed consensus in closed environment :-**

Link1 Link2

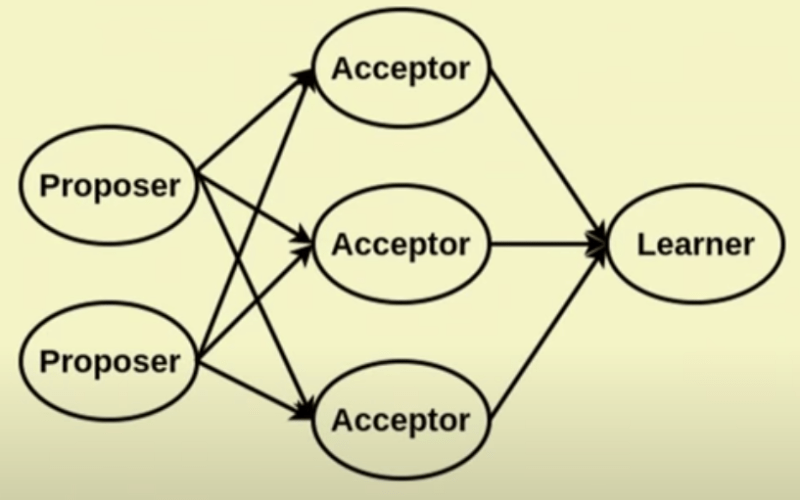
**Paxos :-**

It was the first consensus algorithm proposed by L. Lamport in 1989. The objective was to choose a single value under the crash or network faults. We will look into the Paxos in a simplified view, and later we will try to understand how it can be implemented in a real system to ensure consensus.

The main idea behind the Paxos consensus algorithm is straightforward, and we will understand it with an example. Let us consider that we are at the college and after classes, we are going to hang out all together. We have two options to hang out with classmates after classes: Subway and Coffee Cafe Day (CCD). So after classes, we can either go to Subway or CCD based on the collective decision, but everyone will go to the same place. In this case, there is no central leader. The only way to take a collective decision is that a few of them (in this case, max could be the two students) will propose an option (i.e., CCS or Subway). Others will either accept or reject that proposed option, and the majority count will be the final value, which will be the consensus.

### **Paxos: Types of Nodes**

There is a certain terminology used in PAXOS, and there are as follows: There are three types of nodes, the proposer, acceptor, and learner. However, everyone is a learner in the network who learns what the majority decision is.

PAXOS – Type of nodes

* **Proposer:** The proposer proposes values, and the consensus algorithm should choose that proposed values.
* **Acceptor:** They form the consensus and accept the values. Whenever they hear a certain proposal from the proposer, the acceptors either accept or reject the proposal.
* **Learner:**This learner will determine which value has been chosen by each acceptor and collectively accept that particular value.

[Link1(Video)](https://youtu.be/F1sjeiYNFHs) [Link2(Detailed info)](https://notepub.io/notes/blockchain-technology/permissioned-blockchain/what-is-the-paxos-consensus-algorithm-and-how-it-is-useful-to-achieve-consensus-in-the-permissioned-blockchain-model/)