A Detailed Review on Blockchain Consensus Mechanisms/Algorithms

-Satwik Hosamani(shosaman@syr.edu)

# Abstract:

In order to synchronize the nodes and compromise on which nodes need to be added to the network, consensus is a very critical part of preserving the nodes of the blockchain. In order to work properly, these consensus structures are important for a blockchain. They make sure that the same blockchain is used by everybody. Everyone can apply items to be added to the blockchain, but it is important that all transactions are reviewed continuously and that all nodes are constantly audited by the blockchain. Blockchains are at risk of multiple threats without a strong consensus process.

There are several methods of reaching consensus and as such, through its blockchain consensus system, each bitcoin implementation is distinct from each other in one way. Many methods such as Proof of Work, Practical Byzantine Fault Tolerance, Proof of Stake, Delegated Proof of Stake, Proof of Capacity, Elapsed Time Proof and several others will be evaluated I can also evaluate the underlying algorithms behind these processes and compare the various approaches for different attributes and contrast them. I will go into the properties and the value of the characteristics such as cooperation, coordination, equal rights, consensus, engagement and activity and how these aims are accomplished by each process. Either asynchronous or semi-synchronous network forms would be the bulk of the mechanisms addressed here.

The key aim of this study will be to dig deep into the heart of consensus-based blockchain maintenance and discuss multiple ways in which consensus can be effectively accomplished. I will also report on the most common consensus processes/algorithms currently used and other mechanisms currently under review. Some of the subjects may need illumination on promoting consensus-building hardware or applications that will also be part of this study.

# What and Why of Consensus

## What is consensus?

Only decentralized structures which do not have a common source of control or a central administration of the system's functioning require agreement. All modifications to the database in a centralized structure, such as a database, either by inserting, modifying or removing information from the database, are made by an administrator or a central authority. The authority has full authority on how the rules and procedures in the database are defined. Since blockchain is a decentralized framework, we need some kind of way to control or ensure that the blockchain operates safely and maintains reliable data in the sense that no central authority is managing the blockchain. We need a way for all block users to apply to blockchain decision-making.

In other words, for the blockchain to function accurately, there has to be a consensus among the users. This accurate, equitable, real-time functional, reliable and secure process is called a consensus mechanism to ensure that all transactions happening on the network are legitimate and that all members agree on a consensus on the status of a blockchain. It is a very significant component of the blockchain that determines on the inputs of the separate blockchain members.

# Achieving Consensus – An Example

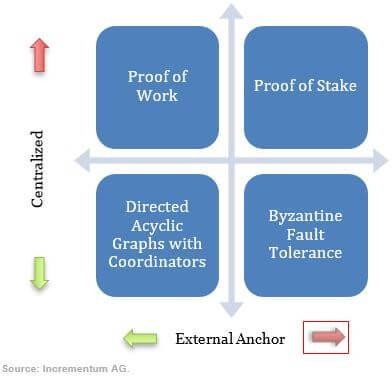
Let me take an instance of the dilemma of the famous Byzantine Generals.

Imagine that there is a king surrounded by his troops in a fortress. The castle is under assault from the enemy, with five armies circling the castle’s hills and camps. And army has a few of its own men and a general who runs them. To enter the fortress, the generals need to coordinate with one another and come up with an assault plan. The way the generals will engage is by sending a messenger with their message on a horse. However there is a question here. As there are traitors among them and intelligence in the wrong hands will lead to a failed assault, the generals should not trust each other. In order to initiate a successful assault on the fortress, the signals should reach all uncompromised generals. As it can clearly be interpreted and altered, a plain written message can not work here. We may equate this to a contemporary situation where calls or emails that can be intercepted and modified are used to connect.

We can use a consensus algorithm which relies on one main principle to solve this question. In order to ensure his allegiance, we need to know how invested the general is in destroying the fortress. One way we can guarantee this is by allowing the generals to deposit a huge amount of money into a stable escrow account. The general must sign his message before sending the message, so we know it is genuine. Because of the signature, we will instantly figure out the difference if some other general wants to tamper with this message or sends a new message. The general who wanted to foul play loses all his money he invested in the escrow account in such a situation. Since there is a stake in the accomplishment of compromise, this form of consensus is called Proof of Stake.” With a network of computers too, the same can be done. Another way to find unity is to help the generals solve an extremely complex mathematical challenge by signing the letter cryptographically so that any changes to the initial message can be detected automatically. To solve the mathematical dilemma, which indicates that they are invested in the attack, the generals will have to devote energy on recruiting mathematicians and a huge amount of time and money. Since there is a lot of effort involved in reaching consensus, this method of achieving consensus is called Proof of Work”.

# Types of Consensus

By deciding the degree of centralization and the type of investment or in other words, the external anchor needed, one way of defining the types of consensus is.



The vertical axis corresponds to the necessary degree of centralization and the external anchor corresponds to the horizontal axis. Consensus processes that fall into the upper right quadrant require and are more decentralized with more external anchors. Mechanisms that fall into the bottom left quadrant need less external anchors and are less centralized.

Let us delve into each type of consensus to get a better idea

## Proof of Work (PoW)

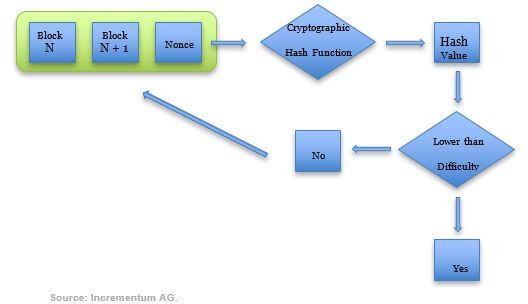
We should regard the Bitcoin Wallets as the Byzantine Generals in the world of bitcoin and blockchain. The way Bitcoin technology describes work is by using miners as the entities who do the work needed to bring a block of transactions into the blockchain. Consider that Adam gives Bob five Bitcoins. To deem it an authentic transaction, the network must ensure that Adam has 5 coins to transfer and the transaction should be digitally signed by Adam. Once this is satisfied, the miners still need to be checked for honesty before the transaction is entered into the block. A hash for the block that serves as an ID for the block has to be computed for the block to be entered into the blockchain.

This is considered a hash-puzzle since the miner has to add the nonce to the hash in the blockchain of the previous node. In contrast to the wide output space of the whole hash function, the numerical output is a number that essentially falls into a target space which is comparatively small. This hash value has to be fixed by the device below a certain value. This number becomes the identification number of that node, which is used in the next block's hash puzzle as an input. It is very difficult to obtain this hash value and requires a lot of computation. The Proof of Work principle guarantees this. To get the transaction right, the miners who are invested in doing right by the scheme spend enough work. If he wants to tamper with the trade, any ill-intentioned miner is more likely to waste resources. The miners' reward here is the processing fee that is part of the transaction. The transaction fee is paid by a miner who correctly measures the hash and sends the transaction into the blockchain. The bigger the transaction fee, the more likely miners are to mine it for the stimulus.

The estimation measures for proof of work are shown below.

The previous block number is all that is needed for the calculation of the subsequent steps. Determine a Nonce for the hash value

1. Apply the Nonce function to the hash and produce a hash value
2. If the hash value is smaller than the system's fixed complexity, then we have a good hash
3. If the value of the hash is greater than the complexity, starting with step 1 by taking a different value of Nonce until
4. Repeat until we have reached a good hash value



The revenue by transaction fees is shown below



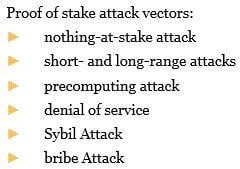
There are, however, several limitations to this mechanism, which includes vulnerability

exploits such as

This mechanism often requires heavy processing capacity that comes with higher hardware and energy costs. The chance of being picked to mine the block as the node will be proportional to the amount of computing power one has. The higher the number of nodes you have the higher your odds of being chosen. For miners with poor computing power, this is a drawback.

## Proof of Stake (PoS)

The person with the largest number of coins is chosen in the Proof of Stake. He/she has the ability to mint a certain amount of coins out of thin air in Bitcoin until the miner mines a transaction. The person with the highest holdings has the potential here. There are several Proof of Stake processes, some of which are Leased Proof of Stake and Assigned Proof of Stake. It has been demonstrated that a better system than Proof of Job is Proof of Stake. But since the largest market capitalizations depend on Proof of Work, Proof of Work is still dominant. However the group is gaining attention with Evidence of Stake. In this or the next year, Ethereum, one of the highest market capitalizations, plans to move from Proof of Work to Assigned Proof of Stake.

Negatives and threats relevant to Proof of Stake are

Most of the reasons why Proof of Stake is not yet dominant is that it has not been well checked yet. This is one of this technique's negatives. Another explanation is that there is a better risk of being chosen by the person with the largest number of coins. This mechanism makes the wealthy wealthier and gives those with smaller network stakes little shot. In comparison, when investors obtain interest in their long positions, evidence of interest allows rather than proof of work to be accrued.

## Delegated Proof of Stake (DPoS)

This approach is an extension of the current form of stake proof. In truth, it is better in certain respects than the original Proof of Stake method since it achieves faster block production. The main distinction here is that in the conventional Proof of Stake, the maker of a new block is decided by the method that takes into account each particular contestant's stake. This means that there will be a significant number of contestants to decide the maker, which takes more time. A voting system is introduced in the Delegated Proof of Stake. Users will vote on who should become the block's creator and the person with the most votes and most stakes becomes the block's creator. As there are fewer entrants compared to the conventional PoS, this speeds up the process very fast and the process is also quickly tracked. As the voting mechanism means that the maker is trusted considering all the votes he has received, this does not mean a loss of security. Another main distinction here is that DPoS is relatively easier to handle any changes to the legislation and laws because it is the people who vote on it. The techniques are hard coded into the genesis block of a conventional PoS scheme and any modifications to it will enable the protocol to be forked. In this way, DPoS aims to build better incentives and a framework for consensus that is fast, flexible, more dispersed and more effective. Bitshares, ARK.io, EOS, Lisk, STEEM, CaptainALtCoin, among others, are some of the blockchains that allow use of DPoS.

## Practical Byzantine fault tolerant Mechanism (PBFT)

This method is one of the most popular permissioned blockchain platform protocol. This solution was created specifically keeping the Byzantine General’s problem in mind. The main gist of this method is that it achieves consensus by determining the decision of all the nodes analysing it and the most popular opinion is provided as the result. However, for this to work, we need to make sure that the number of malicious nodes on the network are not greater than the number of honest nodes. A statistical limit is calculated to be 1/3 for the number of malicious nodes in the network. If more than 1/3 nodes on the network are malicious in a given vulnerability window, then this protocol would not work correctly. The positive thing about this is that the likelihood of having 1/3 malicious nodes on the network reduces as the number of nodes grows in the network and slowly becomes unlikely. The structure of this system is that in a chain of one node as the main node or the master, all the nodes on the network are ordered and all the other nodes are regarded as the backup nodes. These nodes provide the block with their options and therefore guarantee the block has not been tampered with. The system is a 4-phase operation, as seen below, which follows.

1. A client sends a request to the leader node to invoke a service operation.
2. Multicasts the request to the backup nodes by the leader node.
3. The nodes execute the request and then give the client a response.
4. The client expects f + 1 (f represents the maximum number of nodes that could be defective) to respond with the same result from different nodes. The consequence of the procedure is this outcome.

The benefit of this approach is that as we have discussed in Proof of Work techniques, there is not much computation needed. If it is decided on a proposed block, then it is final. This also suggests that in deciding the outcome, there is considerably less energy consumption needed. For any single block proposed that does not apply to PBFT, a round is required in a PoW or a PoS system. There are also major pitfalls to this strategy, though. This strategy would not work if the network were to have more malicious nodes than truthful ones. Only a small network of highly trustworthy nodes would implement this protocol, and even then, evaluating the legitimacy of the block will entail higher computation that is equivalent to what can be performed in PoW mechanisms. This will negate the very objective of an effective operation.

Despite the pitfalls, many programs, including Zilliqa and IBM's Hyperledger, have made use of their custom PBFT implementations.

## Proof of Capacity

This is a type of PoS scheme where you pay for hard drive space instead of paying for money or coins. The more room you possess on your hard disk, the more chances are that the person will be picked for mining the next block and enjoy the payout. Before a user can start mining, this approach requires some configuration for the nodes on the network. The algorithm produces huge data sets that are stored on the hard drive of the owner, known as plots. This is done to prevent a failed continuous computation as found in the PoW mechanism. The possible list of hash values is stored on the hard disk and the lottery is won by the person who has the most matched hash values within a given amount of time. The process of plotting can take days, even weeks to come up with specific plot files, depending on the size of the hard drive. Generally, plotting makes use of a very sluggish concept known as Shabal.

Compared to PoW and due to inexpensive hardware accessible by standard hard disks and Android-based systems, the advantage of this strategy is reduced costs. The downside to this solution is the risk of malware manipulating the mining process.

Burstcoin is one of the systems that makes use of this process.

## Proof of Elapsed Time (PoET)

This method tries to make the odds of winning the chance to create a block as even as possible. The networks using this identify the participants before they can participate. Each node has exactly the same chance to be the winner of the block. The PoET mechanism is based on spreading and fairly distributing the odds for the largest possible number of participants. At first, the users show an intent to mine transactions and create a block to its local enclave. The system then identifies this user and asks the user to wait a specific amount of time which is different for each user. The user can ask for his/her hold up time in the system to determine how long they need to wait. The user with the shortest hold up time wins the chance to create the block. The resource at stake here is time and as we know, time is money. Once the node knows how long it needs to wait, it can go to sleep for the specified amount of time and can be woken up by the system once the winner is declared. The good thing about this is that the node does not need to waste its resources when it is waiting for the specified amount of time. The user can use this time to do other computations and tasks. Once a winner has been declared, the winner can then create the block and spread the information across the network so the other nodes can update their local blockchain.

One of the blockchain systems that make use of this method is Intel’s Hyperledger. However, Intel has a modified version of this algorithm and they use it as their choice of consensus for the Intel’s Hyperledger Sawtooth. This is a very unique implementation but the network will have to rely on intel for the policies and the rules of the system which means a third party is involved. This defeats the whole purpose of decentralization especially since Intel controls how the network operates.

## Proof of Activity

This approach is a combination of consensus mechanisms such as Proof of Work and Proof of Stake. It was designed specifically for the purpose of beating 51% of attacks. A 51 percent attack is a form of attack where, whether a party or entity has 51 percent or more network nodes, they will influence how the blockchain mechanism operates on a blockchain network. The 51 percent attack is vulnerable to both the Proof of Function and the Proof of Stake. If a malicious entity gets more than half of the nodes on the network in Proof of Work, they get to compute very easily and therefore win the lottery most of the time. In Proof of Stake, they get to dictate any single element on the network if the company owns the most currency with a high number of nodes. By applying both strategies, Proof of Operation beats this. If a consumer wishes to mine a block, the contestant must first succeed in applying the policies of Proof of Work. The consumer will let the machine know he is complete and can mine the block after computing the hash. This generates a transaction with only the header of the block and the contestant's address. If this user still confirms the policies of the Proof of Stake, so the user earns the possibility of making the block and mining. As there is no data and just headers in the transaction, this helps the user to construct headers before the transaction ever happens. However, this suggests that the device is vulnerable to spamming. There is a time limit imposed by the method during which the header must be generated to prevent this. This means that the amount of headers produced is much lower and avoids flooding.

Using this approach, the 51 percent attack becomes almost impossible since it is very difficult to succeed with 51 percent of network nodes, both Proof of Work and Proof of Stake. This is one of the methods of extremely stable consensus currently in operation. Decred and Espers are the blockchain applications that make use of this mechanism.

# Usage of Consensus mechanisms in the real world

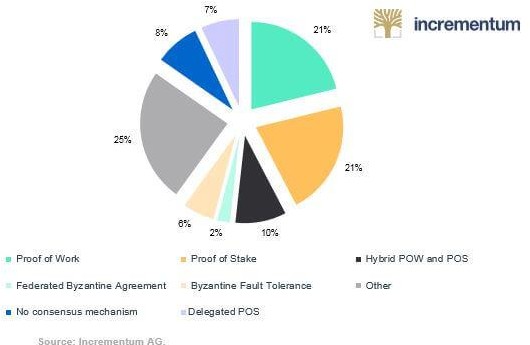
In this article, we have addressed some consensus structures and some more exist. None of them are fine, though. The most stable and popular consensus process so far is still the original one used by Bitcoin: job proof. Evidence of work, however, depends on miners, which can contribute to centralization. Developers are always trying to beat proof of work so the ICO market will splash massive waves with a coin that excludes miners and their energy consumption.

Let us look at several data on the use of consensus structures that we have addressed and some others across the globe.

There are 17 separate consenåsus mechanisms and systems that use them in the table shown.



The chart below shows the most popular consensus mechanisms used



# References

* <https://cryptoresearch.report/crypto-research/consensus-mechanisms/>
* [https://medium.com/datadriveninvestor/blockchain-consensus-mechanisms- 7aa0176d488a](https://medium.com/datadriveninvestor/blockchain-consensus-mechanisms-7aa0176d488a)
* Practical Byzantine Fault Tolerance Miguel Castro and Barbara Liskov Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, MA 02139 castro,liskov @lcs.mit.edu (<http://pmg.csail.mit.edu/papers/osdi99.pdf>)
* <https://blockonomi.com/practical-byzantine-fault-tolerance/>
* <https://www.investopedia.com/>
* [https://hackernoon.com/the-difference-between-traditional-and-delegated-proof- of-stake-36a3e3f25f7d](https://hackernoon.com/the-difference-between-traditional-and-delegated-proof-of-stake-36a3e3f25f7d)