# Cryptographic consensus mechanisms

A consensus mechanism is a fault-tolerant mechanism used in a blockchain to reach an agreement on a single state of the network among distributed nodes. These are protocols that make sure all nodes are synchronized with each other and agree on transactions, which are legitimate and are added to the blockchain. Their function is to ensure the validity and authenticity of the transactions.

A consensus mechanism refers to any number of methodologies used to achieve agreement, trust, and security across a decentralized computer network. In the context of blockchains and cryptocurrencies, **proof-of-work (PoW) and proof-of-stake (PoS)** are two of the most prevalent consensus mechanisms.

Proof of work -

* Proof of work (PoW) is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system.
* Proof of work is used widely in cryptocurrency mining, for validating transactions and mining new tokens.
* Due to proof of work, Bitcoin and other cryptocurrency transactions can be processed peer-to-peer in a secure manner without the need for a trusted third party.
* Proof of work at scale requires huge amounts of energy, which only increases as more miners join the network.
* Proof of Stake (POS) was one of several novel consensus mechanisms created as an alternative to proof of work.

Proof of work (PoW) describes a system that requires a not-insignificant but feasible amount of effort in order to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks. The concept was subsequently adapted to securing digital money by Hal Finney in 2004 through the idea of "reusable proof of work" using the SHA-256 hashing algorithm.1

2

Following its introduction in 2009, Bitcoin became the first widely adopted application of Finney's PoW idea (Finney was also the recipient of the first bitcoin transaction).3 Proof of work forms the basis of many other [cryptocurrencies](https://www.investopedia.com/terms/c/cryptocurrency.asp) as well, allowing for secure, decentralized consensus.

*Proof of work was initially created as a proposed solution to the growing problem of spam email.*

## Understanding Proof of Work

This explanation will focus on proof of work as it functions in the [bitcoin](https://www.investopedia.com/terms/b/bitcoin.asp) network. Bitcoin is a digital currency that is underpinned by a kind of [distributed ledger](https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp) known as a "[blockchain](https://www.investopedia.com/terms/b/blockchain.asp)." This ledger contains a record of all bitcoin transactions, arranged in sequential "blocks," so that no user is allowed to spend any of their holdings twice. In order to prevent tampering, the ledger is public, or "distributed"; an altered version would quickly be rejected by other users.4

The way that users detect tampering in practice is through [hashes](https://www.investopedia.com/terms/h/hash.asp), long strings of numbers that serve as proof of work. Put a given set of data through a hash function (bitcoin uses SHA-256), and it will only ever generate one hash. Due to the "avalanche effect," however, even a tiny change to any portion of the original data will result in a totally unrecognizable hash. Whatever the size of the original data set, the hash generated by a given function will be the same length. The hash is a one-way function: it cannot be used to obtain the original data, only to check that the data that generated the hash matches the original data.1

Generating just any hash for a set of bitcoin transactions would be trivial for a modern computer, so in order to turn the process into "work," the bitcoin network sets a certain level of "difficulty." This setting is adjusted so that a new block is "[mined](https://www.investopedia.com/terms/b/bitcoin-mining.asp)"—added to the blockchain by generating a valid hash—approximately every 10 minutes.5 Setting difficulty is accomplished by establishing a ["target" for the hash](https://www.investopedia.com/terms/t/target-hash.asp): the lower the target, the smaller the set of valid hashes, and the harder it is to generate one. In practice, this means a hash that starts with a very long string of zeros.

*Proof of work was initially created as a proposed solution to the growing problem of spam email.*

## Special Considerations

Since a given set of data can only generate one hash, how do miners make sure they generate a hash below the target? They alter the input by adding an integer, called a [nonce](https://www.investopedia.com/terms/n/nonce.asp) ("number used once"). Once a valid hash is found, it is broadcast to the network, and the block is added to the blockchain.6

Mining is a competitive process, but it is more of a lottery than a race. On average, someone will generate acceptable proof of work every ten minutes, but who it will be is anyone's guess.7 Miners pool together to increase their chances of mining blocks, which generates transaction fees and, for a limited time, a reward of newly-created bitcoins.

Proof of work makes it extremely difficult to alter any aspect of the blockchain, since such an alteration would require re-mining all subsequent blocks. It also makes it difficult for a user or pool of users to monopolize the network's computing power, since the machinery and power required to complete the hash functions are expensive.

***Proof of authority-***

The PoW consensus algorithm used by Bitcoin is the most reliable and secure in existence today. However, it is not really scalable. Bitcoin, as well as other PoW-based blockchains, have limited performance in terms of [transactions per second (TPS)](https://academy.binance.com/en/glossary/transactions-per-second). Such limitation is related to the fact that Bitcoin relies on a distributed network of nodes, which need to reach consensus and agree on the current states of the blockchain. This means that before a new block of transactions gets confirmed it needs to be verified and approved by the majority of network nodes. Therefore, the decentralized aspect of Bitcoin is not only providing a secure and trustless economic system but it is also limiting its potential to be used on a larger scale.

### **What is Proof of Authority?**

Proof of Authority (PoA) is a reputation-based consensus algorithm that introduces a practical and efficient solution for blockchain networks (especially the private ones). The term was proposed in 2017 by Ethereum co-founder and former CTO Gavin Wood.

The PoA consensus algorithm leverages the value of identities, which means that block validators are not [staking](https://academy.binance.com/en/articles/what-is-staking) coins but their own reputation instead. Therefore, PoA blockchains are secured by the validating nodes that are arbitrarily selected as trustworthy entities.

The Proof of Authority model relies on a limited number of block validators and this is what makes it a highly scalable system. Blocks and transactions are verified by pre-approved participants, who act as moderators of the system.

PoA consensus algorithm may be applied in a variety of scenarios and is deemed a high-value option for logistical applications. When it comes to [supply chains](https://academy.binance.com/en/glossary/supply-chain), for example, PoA is considered an effective and reasonable solution.

The Proof of Authority model enables companies to maintain their privacy while availing the benefits of blockchain technology. Microsoft Azure is another example where the PoA is being implemented. In a few words, the Azure platform provides solutions for private networks, with a system that does not require a native currency like the ether ‘gas’, since there is no need for mining.

Although the conditions may vary from system to system, the PoA consensus algorithm is usually reliant upon:

* valid and trustworthy identities: validators need to confirm their real identities.
* difficulty to become a validator: a candidate must be willing to invest money and put his reputation at stake. A tough process reduces the risks of selecting questionable validators and incentivize a long-term commitment.
* a standard for validator approval: the method for selecting validators must be equal to all candidates.

Another common criticism is that the identities of PoA validators are visible to anyone. The argument against this is that only established players capable of holding this position would seek to become a validator (as a publicly known participant). Still, knowing the validators’ identities could potentially lead to third-party manipulation. For instance, if a competitor wants to disrupt a PoA-based network, he may try to influence public known validators to act dishonestly in order to compromise the system from within.

It is well known that decentralization is highly valued within the cryptocurrency community and PoA, as a consensus mechanism, sacrifices decentralization in order to achieve high throughput and scalability. The inherent features of PoA systems are a stark contrast from how blockchains have been functioning until now. Still, PoA presents an interesting approach and cannot be disregarded as an emerging blockchain solution, which may suit well for private blockchain applications.

Proof of stake

The Proof Of Stake algorithm uses a pseudo-random election process to select validators from a group of nodes. The system uses a combination of factors, including [staking](https://academy.binance.com/en/articles/what-is-staking) age, an element of randomization, and the [node's](https://academy.binance.com/en/articles/what-are-nodes) wealth.

In Proof of Stake systems, [blocks](https://academy.binance.com/en/glossary/block) are 'forged' rather than [mined](https://academy.binance.com/en/articles/what-is-cryptocurrency-mining). However, you still might hear the team 'mined' occasionally used. Most Proof of Stake cryptocurrencies launch with a supply of 'pre-forged' coins to allow nodes to start immediately.

Users participating in the forging process must lock a certain amount of coins into the network as their [stake](https://academy.binance.com/en/articles/what-is-staking). The stakes' size determines the chances for a node to be selected as the next validator - the bigger the stake, the larger the chances. Unique methods are added into the selection process to favor not just the wealthiest nodes in the network. The two most commonly used methods are *Randomized Block Selection* and *Coin Age Selection*.

References:

<https://www.investopedia.com/terms/p/proof-work.asp>

<https://www.youtube.com/watch?v=2EabDUGIkBg>

<https://academy.binance.com/en/articles/proof-of-stake-explained>