Powered by Gemini

Cryptopedia®

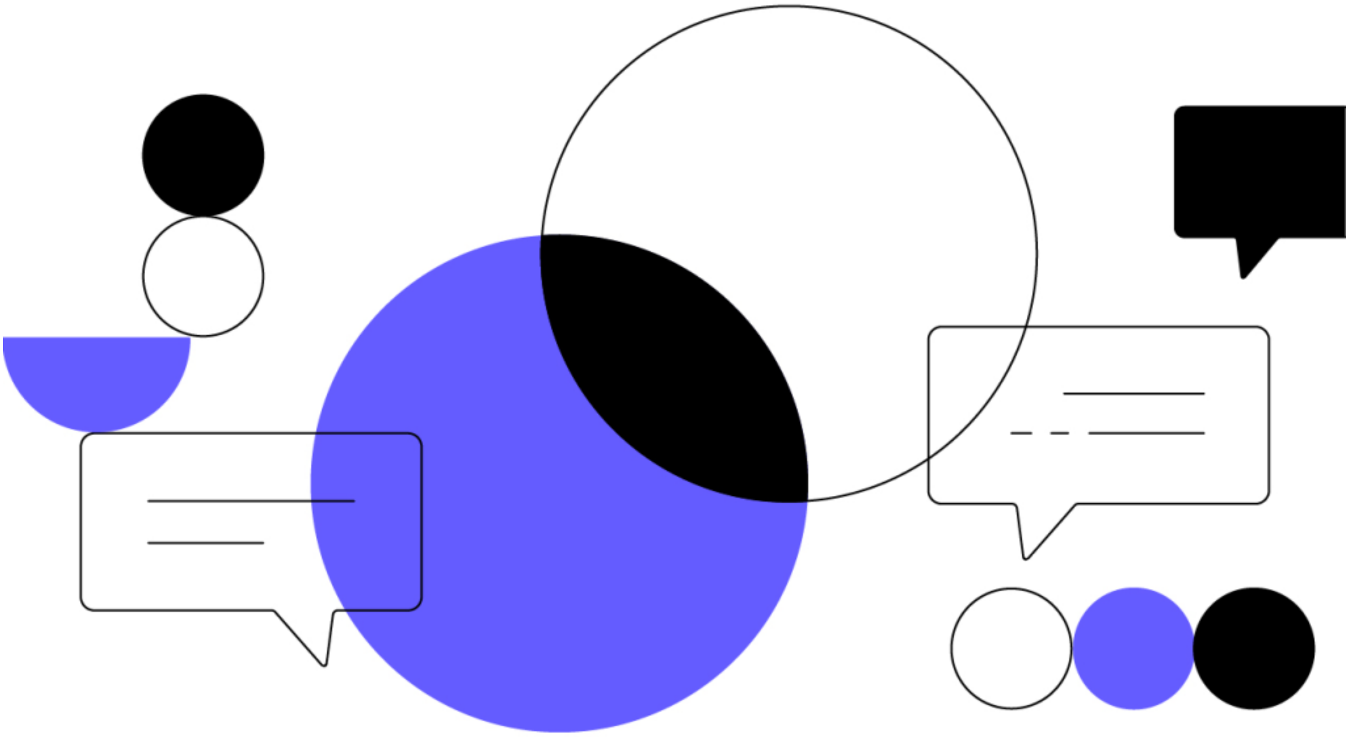
Security > Consensus Mechanisms

Blockchain Consensus Mechanisms Beyond PoW and PoS

PoW and PoS are the most well-known thanks to Bitcoin and Ethereum, but there are many other consensus mechanisms powering the blockchain ecosystem.

By Cryptopedia Staff

Updated March 11, 2023 • 9 min read



Summary

W
th
w
cc

and evolving, and here you can learn about some of the notable iterations in blockchain consensus types.

Contents

Blockchain and Consensus: A Single Source of Truth

In essence, blockchains are distributed databases designed to record, communicate, and transact information without the need for a central authority. Most blockchains are built on a network of distributed individual nodes that work together to furnish the transactions that take place upon the network they all share. Therefore, it’s necessary for every blockchain network to have a mechanism that helps ensure all of its nodes are synchronized with one another and in agreement on which transactions are legitimate and should be added to the blockchain. This decentralized system for determining the blockchain’s true state is called a consensus mechanism. In addition to ensuring the core operations of a blockchain, consensus mechanisms can directly impact the financial parameters and security of the network they underpin.

Most blockchains have three necessary attributes — scalability, decentralization, and security —
w
cc
Et l
th
ha
pr
ar

Proof of Activity (PoA) Consensus Mechanism

Proof of Activity — not to be confused with Proof of Authority, which uses the same "PoA" abbreviation — combines PoW and PoS protocols in a way that can allow participants to both mine and stake their tokens to validate blocks. Under most PoA setups, miners compete to mine new blocks in exchange for token rewards. However, the blocks themselves do not include transactions; rather, they are empty templates embedded with the transaction title and block reward address. The information in the transaction title is used to randomly select a validator node to sign the block and confirm it to the blockchain ledger, and only token holders are eligible to act as validators. From there, the network security fee is split between the miners and validators involved in processing and signing the block.

The PoA blockchain consensus mechanism helps lower the chance of a 51% attack because its structure makes it practically impossible to predict which validators will sign a block in each future iteration, and competition among both miners and transaction signers helps strike an effective balance between different network participants. However, this system is subject to many of the criticisms often aimed at classic PoW and PoS systems, since a significant amount of energy is still required to mine blocks during this protocol's PoW phase, and major token holders still have a disproportionately high chance of signing new transactions and accumulating rewards.

Proof of Activity is used by the Decred and Espers blockchain projects.

Proof of Authority (PoA) Blockchain Consensus

Proof of Authority (PoA) utilizes what's called a reputation-based model to help validate transactions and generate new blocks. In most cases, validators within a PoA consensus blockchain are users that have been selected and approved by other network participants to act as moderators of the system. As a result, validators are typically institutional investors or other strategic partners within the blockchain ecosystem that have a vested interest in the long-term success of the network and are willing to disclose their identities for the sake of accountability.

Therefore, while PoS blockchains force validator nodes to place financial capital on the line to ensure amenable actions, PoA blockchains require validators to place their social capital on the line. That being said, many PoA blockchains also require prospective network validators to invest heavily in the network on a financial level in addition to staking their reputation. This allows the network to filter out would-be validators with lukewarm or dubious motives while financially incentivizing honest nodes that are willing to make a long-term commitment.

Due to their validator selection process, PoA blockchains are often considered relatively centralized
(o
va
re
pe
co

Pr

Proof of Burn (PoB) Consensus and Blockchain

Under PoB, miners intentionally and permanently destroy, or "burn," tokens in order to obtain a proportional right to mine new blocks and verify transactions. The more tokens a miner burns, the higher the chance that miner will be selected as the next block validator. By demonstrating their dedication to the network via intentional token destruction rather than expending computational resources and leveraging powerful mining hardware, miners within a PoB setup are able to operate using far less energy than classic PoW systems often necessitate. The PoB consensus mechanism is utilized by Counterparty, Slimcoin, and Factom.

Proof of Capacity (PoC) / Proof of Space (PoSpace)

Proof of Capacity — also known as Proof of Space — uses the available hard drive space in a miner's device to decide its mining rights and validate transactions rather than expending computational power. Under PoC, a list of possible cryptographic mining solutions is stored in the mining device's hard drive even before the mining activity commences, with larger hard drives capable of storing more potential solution values. As a result, the more storage capacity a miner has, the higher the chance that miner will be able to match the required hash value of a new block generation cycle and win the mining reward. This protocol was designed in order to avoid both the energy inefficiencies of classic Proof of Work (PoW) mechanisms as well as the hoarding incentives brought about by many Proof of Stake (PoS) configurations. This protocol bears several similarities to Filecoin's Proof of Storage consensus mechanism.

The Proof of Capacity consensus mechanism is used by Permacoin, Burstcoin, and SpaceMint.

Proof of Contribution (PoC/PoCo) Consensus Mechanism

Proof of Contribution (PoC or PoCo) protocols rely on specialized algorithms to monitor the contributions of all active nodes within a network during each consensus round, and then award the right to generate the next block to the node(s) with the highest contribution value. Under PoC, every executable action can be assigned a specific confidence threshold that determines the minimum level of confidence required for the calculation tied to that action to be validated by the network.

Within a PoC consensus mechanism, users who wish to perform an on-chain computation must stake a security deposit before performing any computation. Each user's contribution level is a function of that user's historical track record and staking amount, as well as the accuracy of their calculated re

Fc rs
ur
re
re
pl
us

In virtually all instances, multiple users will end up providing the same accurate result to any given calculation. In these instances, these users' confidence levels are aggregated to compute the result's overall confidence score, and the users split the consensus rewards. While not broadly used, PoC has been effectively implemented in projects like iExec, where it's important for the network to validate on-chain actions that are initiated off-chain in a way that is both secure and transparent.

The ICON Network uses a modified version of Proof of Contribution, known as Delegated Proof of Contribution (DPoC). In DPoC, elected entities can validate blocks on a delegate's behalf (on a Proof-of-Contribution basis), and earn token rewards accordingly.

Proof of History (PoH) Blockchain Consensus

The Proof of History protocol operates via a built-in historical record that proves the specific moment in time at which every on-chain event occurred. While most other blockchains require multiple validators to collectively agree on when each transaction has taken place, each individual Solana validator maintains its own internal clock by encoding the passage of time in a simple SHA-256, sequential-hashing verifiable delay function (VDF).

Each time Solana's validators communicate, a cryptographic proof of the relative order and time of each message is recorded onto the network ledger, allowing the network to ignore local clocks and accommodate all potential network delays on their own time. This allows for the efficient delivery and reassembly of all involved transaction data without needing to wait for sequential block confirmations across the entire network. By achieving blockchain consensus via PoH, Solana is able to achieve remarkably fast confirmation times without sacrificing security and still maintaining a relative degree of decentralization.

Proof of Importance (PoI) Consensus and Blockchain

Proof of Importance (PoI) is a spinoff of PoS that strives to take a more holistic approach to evaluating nodal contributions rather than focusing solely on capital requirements for participation in consensus. While traditional PoS consensus mechanisms only consider the amount of capital a node has vested when determining its proportional governance capabilities, Proof of Importance (PoI) mechanisms incorporate additional factors when weighing each node's respective level of on-chain influence.

While the exact scoring criteria used in PoI varies, many of these consensus mechanisms borrow features from the consensus algorithms used in network clustering and page ranking. Common factors include the number of transfers a node has participated in over a set period of time, and the
de

Po
si
nc
di e
or

mechanisms, in which the marginal cost of creating a block is zero and users can continue effortlessly validating blocks in the event of a fork.

The PoI consensus mechanism was first introduced by the New Economy Movement (NEM) project.

Proof of Storage (PoStorage), Proof of Replication (PoRep) & Proof of Spacetime (PoSpacetime)

Proof of Storage relies on data instead of on financial staking. Due to the way Proof of Storage operates, this protocol is mainly used in networks where decentralized data storage capabilities play a prominent role. Under Proof of Storage, the probability of a node being selected to mine new blocks is determined by the amount of data storage that node has actively contributed to the network. Therefore, this protocol is similar to Proof of Stake, but instead of using staked tokens to determine on-chain clout, Proof of Storage achieves consensus by proving that each network participant is actually providing the specific data storage services they claim to be — and rewarding them accordingly.

Filecoin — a leading blockchain-based data storage provider — uses two unique forms of Proof of Storage: Proof of Replication (PoRep) and Proof of Spacetime (PoSpacetime). Proof of Replication allows a node to verify that a specific piece of data has been replicated to its own uniquely dedicated physical storage. With Proof of Spacetime, the Filecoin network randomly selects miners from which data is read for verifications and compressed into a PoSpacetime proof. From there, miners must publicly provide the corresponding proof that the given data encoding has remained in physical storage continuously over a specified period of time, thereby verifying whether it has fulfilled its duties during any given timeframe. As a result, PoRep is used to prove that a miner has stored a unique copy of a piece of data at the moment that data was sealed, while PoSpacetime is used to spot-check random nodes and verify that they are continuously dedicating storage space to that same data over time.

In addition to Filecoin, Storj is another notable project relying on the Proof of Storage consensus mechanism.

Blockchain Consensus Is a Process

There are countless ways for decentralized networks to agree on a single source of truth. As the blockchain sector continues to mature and establish more industry conventions, the design of these consensus mechanisms will have varying and significant implications on each network's security, accessibility, and sustainability.

Th
im ch
co
th m

has its own strengths and weaknesses which must be assessed within the context of the respective network's intended use.

Cryptopedia does not guarantee the reliability of the Site content and shall not be held liable for any errors, omissions, or inaccuracies. The opinions and views expressed in any Cryptopedia article are solely those of the author(s) and do not reflect the opinions of Gemini or its management. The information provided on the Site is for informational purposes only, and it does not constitute an endorsement of any of the products and services discussed or investment, financial, or trading advice. A qualified professional should be consulted prior to making financial decisions. Please visit our Cryptopedia Site Policy to learn more.

Author

Cryptopedia Staff

Is this article helpful?

Yes | **No**

Topics in article

Consensus Mechanisms