

Who decides if a new blockchain block is valid? Every protocol has its pros and cons, and experts in the field frequently come up with and test out new consensus mechanisms. In our previous articles, we looked at two methods for a blockchain network to reach consensus and agree on the validity of a new block.

- **Proof of work** makes nodes of a network compete against each other, expending energy to solve cryptographic puzzles. The winner validates the new block and receives a reward.
- **Proof of stake** makes nodes of a network put up a monetary stake in order to be eligible to validate new blocks. Validators are picked pseudo-randomly, and nodes with a higher stake are more likely to be selected. The selected node validates the new block and receives the transaction fees.

In this article, we will look at yet another – proof of authority.

What is proof of authority?

Proof of Authority is another consensus mechanism for a blockchain to validate new blocks. Instead of requiring a majority of all nodes in a blockchain network to agree in order to add a block to the chain, a select group of nodes are selected to validate new transactions and add blocks.

Unlike proof of work, which is energy-intensive by design, proof of authority requires very little energy to validate new blocks. Unlike proof of stake, which requires all validating nodes have a monetary ‘stake’ to validate, proof of authority does not tie up capital to operate.

Both proof of work and proof of stake require a majority of nodes on the network to reach consensus – for large blockchains like Bitcoin and Ethereum, this could be many thousands of nodes. As proof of authority only requires a small number of nodes to validate a block, transaction processing times and fees can be much lower.

So we can see proof of authority has some advantages as a protocol, with the potential of increased scalability compared to proof of work and proof of stake. However, the protocol has a clear weakness – power to validate is concentrated in the hands of just a small number of actors.

Is proof of authority vulnerable to bad actors?

Blockchains were originally introduced as a way to authorise transactions securely **without** relying on a central authority. By only allowing ‘authority’ nodes to validate transactions, this blockchain protocol by design moves away from decentralisation. Additionally, there is no financial penalty imposed for bad behaviour or incentive for good behaviour.

With fewer nodes required for validation of a new block, a proof of authority blockchain is more vulnerable to takeover from bad actors than a blockchain where the majority of all nodes on the network must reach consensus. Proof of authority systems must have stringent vetting procedures in place for selecting validators – typically this involves confirming a

trustworthy, real identity. Vetting procedures should be difficult in order to weed out bad actors, and apply equally to all potential validators.

Use cases for proof of authority

While more centralised than proof of work or proof of stake blockchains, proof of authority blockchains may still be the best option in some circumstances. This type of blockchain-based platform is especially advantageous for private (single organisation) or consortium (multiple organisations - but not public) blockchains.

Multiple known stakeholder parties, who have no reason to trust one another, but must work together, may find their best option is a proof of authority consortium blockchain. This would allow low-cost, scalable validation of transactions – especially relevant for the financial sector. When all authorised validators are known to each other, the scrutiny of the other validators on their real identities incentivises good behaviour. Another advantage of the protocol is increased privacy compared to a public blockchain.

The centralised nature of a proof of authority blockchain makes it unsuitable for applications where the identity of users is not known. With this in mind, it is very unlikely that any use cases involving large public blockchains will turn to proof of authority to validate new transactions.

Ultimately, each consensus mechanism has its advantages and disadvantages. Proof of authority keeps many blockchain benefits – an immutable ledger shared between multiple parties, reduced paperwork and errors, elimination of third party middlemen. However, it sacrifices decentralisation for increased energy efficiency, faster processing and lower costs. While public adoption is unlikely, proof of authority is an elegant solution for large corporations or corporation networks.