Proof Of Authority (POA)
Technical Document

Enhancing the Performance of the Blockchain

Prepared By
Vegavid Technology

Table of contents

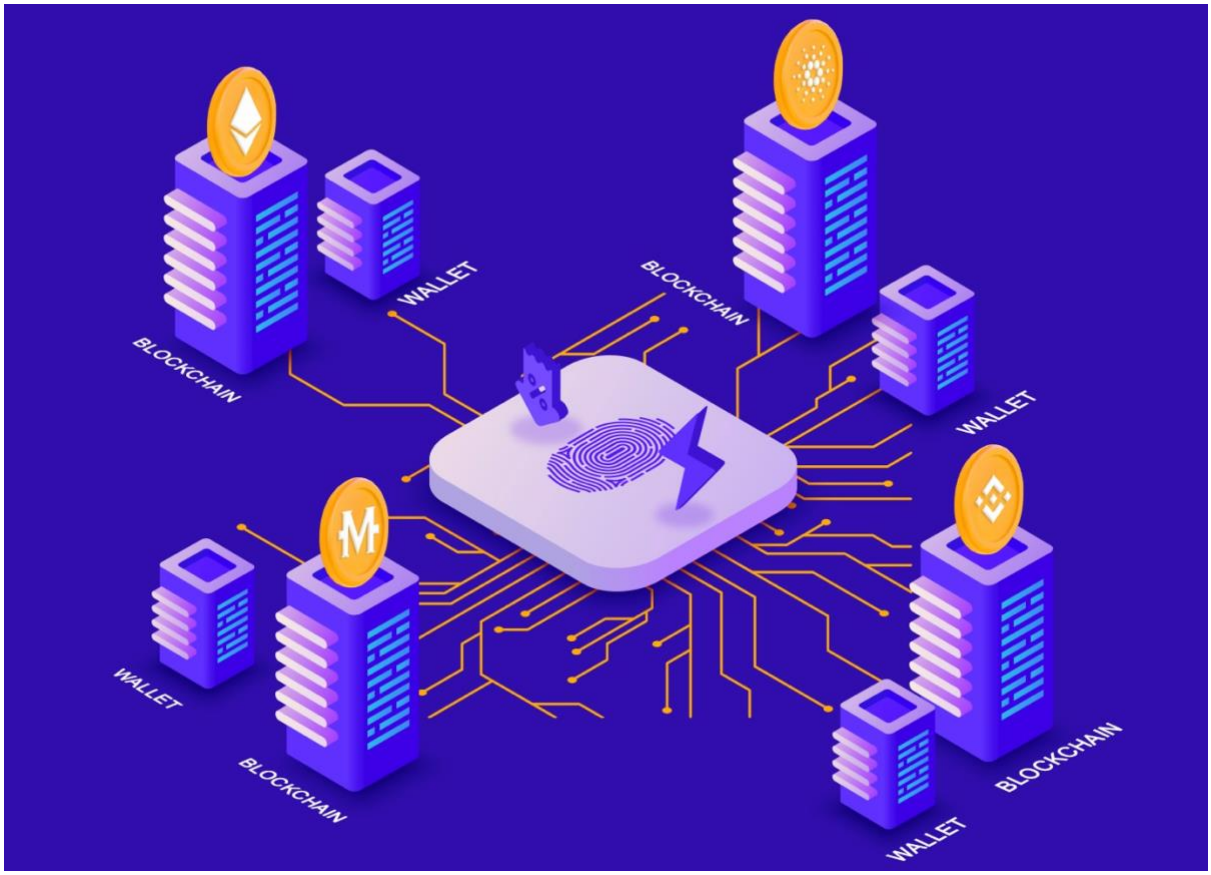
Abstract

MEHH Coin project has moved to a new consensus mechanism that will strengthen its network of master nodes. Currently, we have reached an important milestone of the MEHH blockchain, which is upgrading from ethereum's POW consensus to POA consensus in order to reach higher performance and lower operating costs.

Why do we choose to use the POA consensus algorithm? First, the main reason is that POA offers a high TPS, which is very important for the future of blockchain. Second, the POA consensus algorithm allows only authorised nodes to be part of the network.

With PoA, MEHH has become a social-environment-friendly project, where we listen to our community and constantly try to make it better. Sometimes the changes are big and sometimes they are small. The most recent change to our project is one that we believe will help make our project better and our community stronger.

We have chosen to move away from the Ethereum network and move our tokens to the POA network. We have chosen to upgrade to POA consensus for several reasons, including:



- Lower the cost of running DApps on the POA network.
- Improve the efficiency of smart contracts.
- Forging a more equitable consensus model.

We believe that the main advantage of POA consensus lies in its technological characteristics. This change is going to help us get our project to the next level while staying true to the community that built it. We care about our community, and we are always looking for ways to make their lives easier.

In this technical document, we will discuss more the technical aspect of the MEHH Network POA Consensus algorithm and its benefits.

Introduction

Blockchain is one of the most disruptive technologies of recent years. Initially, while developing Bitcoin, the blockchain technology was used as a decentralised public ledger. But nowadays, it is widely exploited to support integration and federation among companies. Its distinguishing properties of data immutability, integrity, and full decentralisation are key drivers for general-purpose exploitations, ranging from Cloud computing to business-to-business applications.

Essentially, blockchain is a linked data structure replicated over a peer-to-peer network, where transactions are issued to form new blocks. Peers achieve distributed consensus on transaction orders by placing them into new blocks; each block is linked to the previous via its hash. This whole process is carried out by distinguished nodes of the network, named miners.

These miners support cryptocurrency as well as the smart contracts and immutable programs deployed and executed upon blockchain.

Ethereum was the first popularised smart contract framework. Both Bitcoin and Ethereum are permissionless blockchain systems, which means any node on the internet can integrate with them to become miners.

Distributed consensus is here achieved via so-called Proof of Work (PoW), a computational intensive hashing-based mathematical challenge. PoW PBFT vs Proof-of-Authority: Applying CAP Theorem to Permissioned Blockchain De Angelis et al. enjoys strong integrity guarantees and tolerates a sheer number of attacks, but this comes at a huge cost: lack of performance. This has led, together with the absence of privacy and security controls on data, to the so-called permissioned blockchain, where an additional authentication and authorization layer on miners is in place

What is Proof of Authority (POA)?

Proof of Authority (PoA) is a reputation-based consensus algorithm that provides a practical and efficient solution for blockchains (especially private ones). The term was coined by Ethereum co-founder and former technical specialist Gavin Wood in 2017.

The Proof of Authority model is based on a limited number of block validators, which makes it a scalable system. Blocks and transactions are checked by pre-approved participants who act as moderators of the system. Consequently, PoA blockchains are protected by validation nodes that are considered to be trustworthy.

How does it work?

Validators run software to put transactions in blocks. The process is automated and does not require validators to constantly monitor their computers. This, however, requires maintaining the computer (admin site) in good condition.

In order to be a validator, a user must comply with three basic conditions:

1. **The identity must be formally verified** on the network with the possibility of cross-checking the information in the public domain.
2. Obtaining the right to be elected as a validator who is authorised to confirm earned and evaluated blocks should not be easy (for example, **a potential notary is required to obtain a state notarial licence**).
3. There should be **full consistency** in the checks and procedures for establishing authority.

With the PoA algorithm, people get the right to become validators, so they have an incentive to maintain the position that they received. To avoid spoiling their reputation, validators are motivated to maintain a normal transaction process. Thus, most users value their hard-earned role as a validator.

Our Technology

From MEHH Coin's inception, we chose to derive our tailored-to-the-sector blockchain technology from an existing one (i.e., Ethereum), rather than developing our blockchain technology from scratch. That allows us to avoid spending resources reinventing the wheel, and instead focus our software development efforts on functionalities that address the specific pain points of application developers in the technology sector.

Pain Point

Due to the way blocks are created, transaction demand often exceeds available computational supply (i.e., there are too many transactions to fit in a given block), resulting in high transaction costs, delayed settlement, and limited scalability for mass-market applications.

Adjustment made to our fork of Ethereum

Proof-of-Authority consensus: MEHH Coin project replaced the Proof-of-Work (PoW) consensus mechanism used in Ethereum with a Proof-of-Authority (PoA) consensus mechanism. With PoA, the MEHH Coin project has the ability to increase network capacity by 30x compared to Ethereum. Proof-of-Authority Consensus improved functionality and increased technical capability for regulatory oversight while maintaining network trust and security The key criteria for a consensus mechanism compatible with the technology sector are: a) high capacity, b) security, c) resource efficiency, d) regulatability, and e) fidelity. We are using a Proof-of-Authority 2 consensus mechanism for the MEHH Coin, in which a pool of known and trusted computers—called validator nodes—are responsible for validating transactions and creating blocks. This approach offers certain security, regulatory transparency, and considerable capacity benefits, though it does sacrifice a small but not insignificant level of decentralisation.
By limiting the ability to create blocks to a known pool of validators, we can achieve the following benefits without sacrificing the integrity of the chain:

Table: Proof-of-Authority Consensus Mechanism Benefits

Benefit	**Explanation**
Improved resource efficiency and lower energy consumption	The combination of limiting validator status to a defined number of nodes who have passed a vetting process and establishing economic and reputational incentives (validators have something at stake) introduces an inherent level of trust between the participants. Since there is no competition among validators to race each other to create blocks, transaction throughput can be increased (faster block time) while energy consumption and computational complexity are drastically reduced (compared to Proof-of-Work).

Reduced transaction costs	The reduced computing and energy requirements, in turn, reduce the operating cost for validators. In combination with the increased throughput, this makes transaction costs lower and more predictable than those on Ethereum.
Minimal network latency	Validator nodes in the MEHH Coin project are typically run on dedicated hardware in professional server environments with high-speed Internet connections.
Simplified ecosystem upgrades	Limiting validator status to known and legally registered entities simplifies the process for rolling out upgrades to the core protocol (coordinating a vetted group of validators with aligned incentives is easier than a dynamic group of anonymous miners).

We are aware, as well, of the limitations and risks of adopting a Proof-of-Authority consensus and are adopting the following mitigation strategies. While these are our current hypotheses, MEHH Coin project will continue to test and develop new solutions over the next year.

Conclusion

MEHH Coin project is a blockchain platform with the aim of solving global problems by connecting local merchants and consumers to provide more efficient, transparent, and reliable transactions.

MEHH has upgraded its current technology to the Proof of Authority (POA) consensus algorithm which assures the greatest combination of security, efficiency, and decentralisation, available on the Ethereum chain. Efficiency is achieved because the amount of authority-nodes processing transactions is kept relatively low, so block confirmations happen quickly, without the long confirmation times commonly seen in other blockchains.

Security is guaranteed through the fact that authority nodes are distributed among different entities and are numerous enough that they prevent a malicious attack.