Blockchain Consensus Algorithm: Proof of Authority (POA) Overview

By Arbin Chhatkuli

In a blockchain network, the design of a consensus mechanism is essential due to its nature as a distributed ledger. It ensures that all participants agree on the state of the network. Each running node in the network should maintain the same logs, ensuring consistency and accuracy. For instance, if Alice has 2 ethers and Bob has 4 ethers, and Alice sends 1 ether to Bob, Alice should have 1 ether, and Bob should have 5 ethers. This transaction should be publicly announced across the entire network. However, an inactive node with outdated logs, such as Adam, could mistakenly believe that Alice still has 2 ethers and Bob still has 5 ethers. This discrepancy could lead to serious problems. To prevent such issues, a consensus mechanism is required to establish a universal truth agreed upon by all network participants. Additionally, consensus mechanisms address various challenges, including Byzantine faults common in distributed systems.

Proof of Authority (POA)

In Proof of Authority (POA), only specific trusted nodes have the authority to produce blocks at their discretion. These trusted nodes act as validators for the blocks, and only they possess the rights to propose blocks for inclusion in the blockchain. POA offers a solution for achieving high transaction rates and fault tolerance. This consensus mechanism is primarily intended for small-scale or private networks where all participants are known to each other or for lower-stake networks, such as testnets or networks storing a trivial amount of value.

POA in Ethereum

Before the official launch of Ethereum's main network, Ethereum had several testnets, including Olympic and Morden Classic, during the frontier release. Notably, Ropsten served as the last public Proof of Work (POW) testnet until its abandonment due to stability concerns. Nevertheless, Ropsten is still maintained as the primary platform for testing smart contracts and decentralized applications (dApps) on both Geth (Go-Ethereum) and Parity Ethereum (written in Rust). Since Ropsten is only a testnet, no actual funds are involved, alleviating concerns about the cost and implications of transactions on the mainnet.

An important event related to Ropsten was the occurrence of spam attacks that increased the block gas price by submitting transactions with excessively high gas prices. This resulted in higher transaction costs, with lower gas transactions receiving less attention.

The Ropsten testnet no longer receives updates, prompting Ethereum developers to transition to other testnets like Sepolia and Goerli,where Sepolia is based on POW & Goerli is based on POA consensus mechanisms.

Several alternative testnets were established to replace Ropsten:

1. **Kovan**: Kovan was the first Proof of Authority (POA) testnet launched as a response to the spam attacks on Ropsten. A consortium utilized Parity's Aura POA engine to operate this testnet.

2. **Rinkeby**: Rinkeby was the second Proof of Authority (POA) network introduced in response to Ropsten's spam attacks. Instead of Aura, Geth's Clique POA engine is employed for this network.

3. **Goerli**: Goerli serves as the testnet version of the Ethereum cryptocurrency. Launched in January 2019 by the Ethereum research team, its primary purpose is to provide a testing environment for developers and researchers to experiment with new features and improvements before their implementation on the main Ethereum network. Users of both Parity and Geth engines can function as validators on this single testnet, simplifying testing and development processes for Ethereum-related projects.

In a Nutshell

The Proof of Authority (POA) consensus is a special way to make blockchain networks secure and fast. It works great for small private networks, test networks, or networks with not much at stake. If you're a developer or researcher or a learner like me in the Ethereum world, it's important to know how test networks have changed over time. For example, Ropsten was used a lot, but it had some problems, so now there are better ones like Kovan, Rinkeby, and Goerli. You can use Goerli Faucet to get the testnet token required in Goerli Testnet , which is easy to get.These test networks are super important for building and testing smart contracts and apps on Ethereum, making Ethereum better.