

Hybrid Secure Proof of Stake

August 27, 2021

By

Wulf Kaal¹

Abstract

In conventional Proof of Stake (PoS), the nodes with higher stake would have a higher probability of being selected for the block rewards. Block rewards are constant regardless of the node reputation. In Secure Proof of Stake (SPoS), the nodes with higher reputation have a higher probability of being selected for the rewards.

The main concept in Hybrid Secure Proof of Stake (HSPoS) is to separate the block consensus from the block rewards. HSPoS proposes that the rewards become a function in the reputation of the node. Thus, while the node probability of being selected is based on the fungible stake, the rewards for the block is adjusted by the non-fungible reputation multiplier which is a function of the node's reputation.

HSPoS enables a transitioning process in which traditional PoS consensus algorithms, can be used and maintained while being supplemented with SPoS characteristics and node reputation. This enables enhanced experimentation and allows a slow transitioning from PoS to SPoS.

Key Words: Proof of Work (PoW), Secure Proof of Stake (SPoS), Hybrid Secure Proof of Stake (HSPoS), Blockchain, Canary Network, Decentralized Autonomous Organization, Decentralized Governance, Consensus Algorithm, Reputation Staking

JEL Categories: K20, K23, K32, L43, L5, O31, O32

¹ The Author is grateful to Muhammet Kara for his helpful insights into the history of the Casper Testnets. The author is also very grateful to Dr. Adel Elmessiri for delightful discussions on possible hybrid and phase transitioning consensus algorithm models that allow moving from PoS to SPoS.

Table of Contents

Consensus Algorithm Experimentation	3
Case Study – Casper Network	3
Platform Centralization	3
Testnets as remedies to platform centralization	4
Canary Network	6
Benefits for Developers	6
SDAO	7
Reputation Governance	7
Technology Upgrades	8
Migrating from PoS to SPoS	9
Hybrid Secure Proof of Stake (HSPoS)	9
Toy Model	10
Conclusion	11

Consensus Algorithm Experimentation

The blockchain community has been experimenting with consensus algorithms since the early days of Bitcoin's Proof of Work (PoW) consensus algorithm. Proof of Stake (PoS) has become the main body of research in the 2020s. The next phase of consensus algorithm experimentation extends the research on PoS.

In conventional PoS, the nodes with higher stake would have a higher probability of being selected for the block rewards. Block rewards are constant regardless of the node reputation. In SPoS, the nodes with higher reputation have a higher probability of being selected for the rewards.

The main concept in Hybrid Secure Proof of Stake (HSPoS) is to separate the block consensus from the block rewards. HSPoS proposes that the rewards become a function in the reputation of the node. Thus, while the node probability of being selected is based on the fungible stake, the rewards for the block is adjusted by the non-fungible reputation multiplier which is a function of the node's reputation.

HSPoS enables a transitioning process in which traditional PoS consensus algorithms, can be used and maintained while being supplemented with SPoS characteristics and node reputation. This enables enhanced experimentation and allows a slow transitioning from PoS to SPoS.

Case Study – Casper Network

The development of HSPoS requires an examination of the needs of PoS network experimentation.

The Casper network PoS provides a prominent example of a 3rd generation blockchain with a PoS consensus algorithm that is subject to experimentation.

Platform Centralization

Developers have lost the ability to influence the direction of what they are building. Platform centralization is one of the key factors in this context. Platform centralization is particularly detrimental in the developer community because it is the developer community that brings information in from the edges of the system/society and helps form a consensus on emerging technologies for society. With only a limited ability to influence the direction of

product/technology development, the developer community is less able to deploy its unique talents and skills in creating technology solutions for the greater good of humanity.

The lack of developer liberalization has negative societal ramifications. If the developer community is restrained from building technology it sees as cutting edge and beneficial for society, societies' ability to experiment with such new technology solutions is severely hampered. Without societal experimentation with cutting-edge technology, and increasing mainstream adoption, in turn, it is more problematic to increase innovation for the greater good of society. In other words, if the developer community does not receive the support it needs in developing decentralized infrastructure solutions, society at large suffers.

Testnets as remedies to platform centralization

The Casper Network has accomplished significant improvements that address platform centralization and the resulting constraints on the developer community.

Casper has experimented with testnet environments since 2020. The Casper community established a single testnet after the Casper mainnet launch, with two incentivized testnet phases in 2021. The latest incentivized testnet ended in September 2021. The last Casper testnet in September 2021 entailed as its single rewarding requirement the perceived uptime of the participating testnet validator node.

The early testnet days set the ideal foundation for the Shasper Network. In the early testnet days, multiple testnet upgrades had been completed and tested successfully. Importantly, the early testnet community entailed many participants who were actively sharing their knowledge and supporting other validators without expectation of profit or return favors. While some parts of the documentation were verbose and manual on purpose, to educate the operators in the process, the early testnet community created detailed and very easy-to-follow instructions for the testnet node operators, which resulted in around 950 nodes running on the network and around 200 nodes were rewarded each week.

The 2021 Casper testnets had several inevitable shortcomings that originated from early experimentation with testnet validator needs. In the early testnet days, validator participation was volatile with validators joining and others leaving regularly. At some point during 2021, the active Casper testnet nodes fell under 800 after the uptimes/rewarding-status of each validator node was reported to the community on a weekly basis. Other validators shut down their nodes instead of waiting for the end of the incentivization phase when they realized that there was no reward for them.

The initial Casper testnet was subject to inevitable forms of centralization. For example, a small group of core developers determined the testnet validator performance numbers and other rules without broader community input. Moreover, only a rather small group of developers managed the testnet validator community, communicated info/updates from the DEVxDAO (the testnet host), maintained the technical documentation, helped the validators on technical issues both on the testnet and the mainnet, observed the general status/health of the Casper testnet, and reported to the core dev team.

During the first phase of the 2021 Casper Testnet, it was unclear which validators would get rewarded in each week, causing friction and non-productive discussions among the validators. Once the uptime scores and reward eligibility had been shared on a weekly basis the situation improved marginally. Yet, the initial testnet group were hampered by communication shortcomings. For example, only around 680 of the validators were present in the telegram group. Nevertheless, the Casper testnet validator telegram group as the the only/main source of news & updates for testnet validators. Alas, several validators relied on less reliable resources.

The original Casper Testnet was also afflicted by cases of single persons running 15+ validator nodes in an effort to abuse the welcome promotions of certain cloud providers and the rewards policy of the DEVxDAO. Some individuals ran multiple nodes in an effort to get the rewards without any participation/contribution in the validator group. Those individuals had a tendency to present themselves at the times of payment without reading the rules/instructions or caring about them, ruining inter-group dynamics.

Lack of expertise also afflicted the initial Casper testnet. Only around 85% of the testnet nodes were up-to-date, with the rest of the active machines (around 140 machines at the time) not contributing to the network at all. Judging by the discussion and questions in the telegram channel, many testnet participants also did not have the required expertise to run Casper testnet nodes. Questions primarily focused on reward payments, with little to no focus on the technical topics.

Nevertheless, the 2021 Casper testnet fulfilled its purpose. It provided a test bed for dApp developers on Casper mainnet, and tested the node software upgrades before they were deployed on the Casper mainnet. Moreover, testnet upgrades reached the viable percentage much faster than the mainnet upgrade. And, some issues are detected on the testnet, causing some minor releases being skipped on the mainnet. Thus, the testnet did contribute to creating a more stable environment on the Casper mainnet.

The combination of positive and negative factors explored above suggests that the Casper testnet can be upgraded significantly, which will help it fulfill its mission and purpose for the Casper mainnet.

Canary Network

In 2021, parts of the Casper and DEVxDAO communities have proposed, not by consensus, the Shasper Network as a canary network that runs parallel to the Casper testnet and the Casper Mainnet.

The Shasper Network was introduced to provide technological, innovation, and community solutions for the evolution of the Casper Network infrastructure environment.

The Shasper Network infrastructure improves most of the applications and uses of the Casper Network for the greater good of the Casper Community and society at large. Through its technological infrastructure designs, the Shasper Network creates, improves and expands well-functioning and well-governed blockchain networks. Dev teams can launch their own custom blockchains, DApps, parachains, and parathreads on the Shasper Network.

The Shasper Network creates an experimental development environment for dev teams who want to move fast and innovate on Shasper or prepare for deployment on Casper. The Shasper Network provides the Casper Community with a testing ground for applications and smart contracts that can be directly transferred to the Casper Network.

Shasper is a network that is built as a risk-taking, fast-moving canary network for the Casper Blockchain. Shasper is a living platform built for developers to take initiative, spark innovation, and experiment with the limits of what was hitherto seen as possible.

Shasper is a scalable network of specialized blockchains and uses nearly the exact same codebases as the Casper Blockchain.

Benefits for Developers

Cutting-edge Technology

Shasper always enables the newest features of the Casper blockchain before they go live on the Casper Network. The advanced technology built into Shasper entails sharded next-generation multichain networks.

Speed

Blinky's nimble environment enables risk-taking for dev teams who wish to move quickly through the governance and upgrade process, which in turn enables accelerated growth and scaling of experimentation.

Experimentation

Dev teams can launch their own custom blockchains, DAppss, parachains, and parathreads on the Shasper Network at low [or no] cost [without the need to get governance/network approval].

Synergies

Dev teams building on the Shasper Network have the ability to leverage the global developer community and the brand of the Casper Network.

Community Governance

Developers on the Shasper Network can participate directly in the evolution of the Shasper Network through participation in the Shasper DAO (SDAO). The SDAO follows a decentralized framework of governance that was developed by the DEVxDAO. SDAO members get paid to participate in the governance of the Shasper Network.

SDAO

The Shasper DAO (SDAO) is the collective of Shasper Network validators. Any testnet environment depends on proper governance to allocate power fairly and equitably at equilibrium in a sustainable fashion. The Shasper Network accomplishes the need for proper decentralized governance through its decentralized governance design for network validators in the SDAO. Shasper validators in the SDAO vote on the design of the Shasper Network and are an integral part of its evolution.

Reputation Governance

The Shasper Network provides a hardcoded solution for the funding of its governance framework via the SDAO. Each validator who produces a block in the Shasper Network follows the Casper Proof of Stake (PoS) Consensus algorithm and is compensated for block propagation accordingly.

However, in addition to the Casper PoS Consensus algorithm allocation, each validator who succeeds in propagating a block allocates [__]% of the block reward, denominated in SHAS, into a separate SDAO wallet.

That [__]% of the block reward in SHAS token also mints reputation in the SDAO for said validator. The reputation minting process follows the DEVxDAO MVPR protocol and the SHAS token that are allocated to the SDAO are shared among the SDAO members following the DEVxDAO MVPR protocol. Accordingly, the SHAS in the SDAO wallet are distributed to the SDAO VAs in proportion to their SDAO reputation score. After each block is produced and reputation is produced for both validation services and policing of validation services in the SDAO,

the SHAS % fee is paid out immediately according to the new reputation state after the block is produced. The respective SDAO reputation score of each VA, in turn, is determined by their respective merit, level of activity, and engagement in the SDAO.

NFTs owners are onboarded via vote into SDAO. Shasper Testnet validators who, in addition to evidence of the NFT ownership, post evidence of their performance record as Shasper Network validators will be considered as candidates for the SDAO.

While the Shasper Network is permissionless, in an effort to encourage validator participants to educate themselves about network requirements etc. and to pay more attention to the network and the documentation, the SDAO runs the program with a prior registration requirement. This performance based onboarding process and metric goes way beyond the criterion of validator node uptime. In the SDAO preregistration workflow, validator candidates apply for a position in the SDAO program, and have guaranteed reward allocation for a period of time, provided that they meet the following criteria, including but not limited to:

1. Uptime
2. Node performance
3. Running a dApp / protocol on the network
4. Response time to upgrades
5. Technical background
6. Adherence to the instructions and best-practices
7. Adherence to the hardware specs
8. Community-behavior
9. Other contributions

An initial group of [3] SDAO VAs decide on a scheduled onboarding process to add more testnet validators into the SDAO.

Once onboarded, Shasper Testnet validators become SDAO voting associates (VA). VA status gives the following rights:

- Receive a salary for VA work and VA participation in SDAO governance - salaries are paid out in SHAS token in proportion to the respective SNGT score.
- Vote on any Shasper Network technology updates
- Vote on applications from other validators to become SDAO VAs
- Vote on any SDAO governance updates
- Vote on which existing projects on the Shasper Network should be promoted to the Casper Mainnet

Technology Upgrades

Through the use of the SDAO, the Shasper Network enables its developer community to determine via community consensus what technology upgrades to the Shasper testnet should be created. Teams of developers can work with the Shasper DAO community to promulgate, design, and obtain support for their respective projects. Rather than convincing legacy technology leaders and their respective platforms, teams of developers can engage directly with their own peers in the Shasper DAO to discuss and vote on proposed technology upgrades and Shasper testnet projects. The community peer review dictates projects, funding, and outcomes and provides feedback mechanisms. The Shasper DAO has the potential to form the foundation for technology development that serves the greater good of society.

Shasper Network governance votes are required to make changes to the codebase. To further facilitate experimentation and innovation for the Casper Network, the Shasper Network will make certain basic changes to the Casper codebase.

Migrating from PoS to SPoS

In order to move PoS towards SPoS (Secure Proof of Stake),² this paper suggests evolving the rewards mechanism in two steps via HSPoS (Hybride Secure Proof of Stake).

Hybrid Secure Proof of Stake (HSPoS)

In conventional PoS, the nodes with higher stake would have a higher probability of being selected for the rewards. Block rewards are constant regardless of the node reputation. In SPoS, the nodes with higher reputation have a higher probability of being selected for the rewards.

The main concept in HSPoS is to separate the block consensus from the block rewards. HSPoS proposes that the rewards become a function in the reputation of the node. Thus, while the node probability of being selected is based on the stake, the rewards for the block is adjusted by the reputation multiplier which is a function of the node's reputation. In other words, rather than using SPoS's block propagation via reputation directly, HSPoS enables a transitioning process in which the traditional PoS consensus algorithm, such as the one in Casper, can be used and maintained while at the same time such PoS consensus algorithm is supplemented with SPoS characteristics and node reputation. This enables enhanced experimentation and allows a slow transitioning from PoS to SPoS.

In HSPoS, two nodes with the same stake would have the same probability of being selected for the rewards. However, the node with the higher reputation would get higher rewards. Nodes can accumulate reputation by:

² https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125827

1. being onboarded into the SDAO and performing well as node validators, and
2. by participating regularly in the governance votes of SDAO.

Furthermore, a node with less stake but high reputation may end up with more rewards than a node with more stake but less reputation.

Through this balancing of validator SHAS stakes and reputation, HSPoS attains an equilibrium of incentives for validators to:

- a. attain economic success as validators, and
- b. participate actively in the decentralized governance of the SDAO (and attain further economic benefits through their participation in governance).

HSPoS emphasizes validator node reputation, which is earned via a reputation-based mechanism that decouples the normal monetary system of incentive rewards. Reputation represents a type of social capital that is earned by participating in the network's ecosystem regardless of the amount of financial capacity.

Toy Model

The multiplier is computed as follows:

Like in the standard PoS system, the rewards are set and can be adjusted (halved or adjusted). HSPoS computes the average reputation per node as defined:

$$AR = \frac{\sum_{i=1}^{i=n} rep(Node_i)}{n}$$

Where

AR: Average Reputation

N: number of nodes

rep(Node): the reputation of the node

The final rewards would be computed by the following equation:

$$RBR(Node_i) = BR * rep(Node_i) / AR$$

Where

$RBR(Node_i)$: Reputation Block Rewards for the i th Node

BR: Block Rewards

Governance decisions, such as network upgrades, among others, follow a simple vote process in which no reputation is minted. However, reputation in the SDAO can be lost as a result of a governance vote as each vote follows the DEVxDAO MVP logic via loosely coupled to tightly coupled voting.

Conclusion

The Shasper network provides a natural extension of the Casper testnet which benefits community experimentation. It creates significant developer incentives which helps retain talent for the Casper network.