47. Staking as a service

Arthur Carvalho

Introduction

Bitcoin revolutionized finance by introducing a decentralized digital currency, eliminating the need for intermediaries like banks. At its heart lies what is now called *blockchain technology*, a distributed and immutable ledger that records blocks of transactions across a network of computers (nodes). Integral to blockchain's function is a consensus mechanism, a process that ensures all participants agree on the validity of transactions. Bitcoin employs a proof-of-work (PoW) consensus mechanism, where some nodes—also called *miners*—compete to solve complex mathematical problems. The first miner to solve the problem adds the next block of transactions to the blockchain and is rewarded with freshly minted Bitcoin and transaction fees. This process, while robust, has drawn criticism due to its significant energy consumption, as miners require powerful hardware to perform computationally intensive calculations, raising concerns about environmental sustainability.

The evolution of blockchain technology has led to the emergence of *proof of stake* (PoS) as a viable alternative to the energy-intensive PoW consensus mechanism. In PoS networks, users *stake* their cryptocurrency holdings to validate transactions and secure the network, earning rewards in the process. For example, staking on Ethereum, a prominent blockchain that transitioned from PoW to PoS with its Ethereum 2.0 upgrade, offers a compelling illustration of how this alternative consensus mechanism functions. In Ethereum's PoS system, *validators* replace miners as the key participants in the network. Instead of spending energy on solving complex puzzles, validators are selected to propose and validate new blocks based on the amount of cryptocurrency they have staked or locked as collateral. As of October 2024, validators must stake a minimum of 32 ETH (Ethereum's native cryptocurrency) to participate in the validation process, which is currently equivalent to approximately US$84,000. When selected, a validator is responsible for proposing a new block or attesting to a block proposed by another validator. If the block is accepted and added to the blockchain, the validator earns rewards in the form of additional ETH. The rewards are distributed among all validators who participated in the consensus process for that block, incentivizing honest and active participation.

While PoS offers numerous advantages over PoW, performing *solo staking* can be challenging for many due to technical and financial barriers. This is where innovations such as *pool staking* and *staking as a service* (StaaS) emerge as crucial solutions, the latter being this chapter's main focus.

Staking innovations

PoS offers several benefits over PoW, including enhanced energy efficiency and increased scalability. However, despite its advantages, participating in PoS can pose significant challenges for individual users. For example, setting up and maintaining a validator node requires technical expertise, high-performance computers with ample storage, specific software, constant network connectivity, staying up-to-date with network upgrades and security patches, and, consequently, a substantial initial investment. This upfront investment can be prohibitive for many individuals, especially in the early stages of a PoS network when the value of the staked cryptocurrency might be volatile. Moreover, the risk of "slashing," where a portion of the staked cryptocurrency is penalized for validator misconduct or downtime, can be a deterrent for potential participants. Specifically, slashing occurs when a validator violates the network rules, such as going offline and failing to propose or validate blocks, attempting to double-sign transactions, or rewriting transaction history. This penalty, designed to maintain network integrity, can result in a significant loss of staked cryptocurrency, making it a crucial consideration for potential participants. For example, depending on the severity of the violation, slashed validators on Ethereum may be forcibly removed from the network and lose a portion of their staked ETH (Ethereum Foundation, 2024). For users or organizations lacking technical proficiency, navigating the above-mentioned complexities can be discouraging and time-consuming.

Pool staking is an alternative to solo staking that tackles some of the above issues, where multiple *delegators* combine their cryptocurrency holdings into a single staking pool to increase their chances of being selected to validate transactions and earn rewards. This approach makes staking more accessible and easier for individuals with smaller amounts

of cryptocurrency, as it allows them to participate without needing the large minimum stake often required for solo staking. By pooling resources, participants can share in the rewards more consistently, making it an attractive option for those who might not have the technical knowledge or resources to stake on their own. However, while pool staking reduces the barriers to entry and provides a steady stream of rewards, it has some notorious drawbacks compared with using staking as a service. For example, pool staking may involve higher fees or reduced flexibility, as participants typically have less control over the staking process. Additionally, pools are often subject to governance decisions made by the pool operators, which might not always align with the individual staker's preferences. To address these challenges while helping democratize access to PoS participation, s*taking as a service* (henceforth referred to as StaaS) has emerged as a popular solution. In contrast to pool staking, StaaS offers a more hands-off approach with potentially lower fees and more personalized control. However, unlike solo staking, StaaS comes with its own set of risks, such as reliance on a third party to manage the staking process.

The emergence of StaaS

StaaS relies on third-party providers that offer a user-friendly platform enabling individuals to delegate their cryptocurrency holdings to a professional validator node operator. This process typically involves assistance with initial setup procedures, such as generating cryptographic keys and depositing the required cryptocurrency into a blockchain wallet. Users typically entrust their validator signing keys to the StaaS provider, allowing the provider to operate the validator node on their behalf. This delegation of responsibility eliminates the need for users to manage the previously alluded to technical complexities of running a validator node. In exchange for these services, StaaS providers typically charge a recurring fee, often calculated as a percentage of the staking rewards earned or a fixed monthly payment.

StaaS offers several distinct advantages for individuals seeking to participate in PoS networks. First, StaaS platforms tend to emphasize accessibility and ease of use. In particular, they are designed to be user-friendly, requiring minimal technical expertise, where users can easily delegate their cryptocurrency holdings and begin earning rewards with just a few clicks. Moreover, StaaS providers handle the complexities of node setup, maintenance, and software updates, thus reducing technical barriers by eliminating the need for users to possess specialized technical knowledge. StaaS also has the potential to lower financial commitment. By pooling resources, StaaS providers reduce the individual financial burden associated with running a validator node, making PoS participation accessible to a wider range of users. Part of that process includes mitigating slashing risks since reputable StaaS providers implement robust security measures and best practices to minimize slashing, thus protecting users' staked cryptocurrency from potential penalties. Finally, many StaaS platforms support multiple PoS networks, allowing users to diversify their staking portfolio and potentially enhance their returns due to diversification opportunities.

While StaaS offers numerous benefits, it is essential to consider the potential drawbacks before any delegation. First, there is the natural third-party risk associated with entrusting one's cryptocurrency and cryptographic keys to a StaaS provider. For that reason, as we discuss later, it is crucial to choose a reputable provider with a proven track record and robust security measures. Second, StaaS providers typically charge a commission or fee for their services, which can impact the overall profitability of staking. Hence, there is a need to compare fees across different providers to ensure one is getting a competitive rate. Third, some StaaS platforms may impose lock-up periods or restrictions on withdrawing staked cryptocurrency, potentially limiting liquidity and access to funds. Finally, the growth of StaaS could potentially lead to increased centralization within PoS networks, as a significant portion of staked cryptocurrency might be concentrated with a few dominant providers. Due to fears of increased vulnerability to collusion, governance manipulation, and reduced network security, centralization concerns have been recurrent in Ethereum since it transitioned to PoS. For example, it was reported that only two entities accumulated 42% of the network's stake immediately after Ethereum's upgrade (Luo, 2022).

Key platform considerations

As of October 2024, there are several StaaS providers on the market, such as Kiln, P2P.org, RockX, Stakefish, Ethpool, and Consensys. The above discussion suggests that there are key considerations one must contemplate when selecting a StaaS partner. We elaborate and expand on these considerations next. First, one of the most important aspects is the *open-source* nature of the provider's essential code. A commitment to 100% open-source code means that the underlying software is fully transparent and accessible to the public. This transparency allows the community to independently verify, audit, and even improve the code, fostering trust and collaboration within the blockchain ecosystem. Moreover, open-source software can be forked and adapted for other uses, ensuring that the technology remains adaptable and resilient to future changes or challenges.

Second and equally important is whether the essential code and underlying hardware of a StaaS platform have undergone formal *auditing*. Audits are ideally conducted by independent third-party firms specializing in cybersecurity and blockchain technology. These audits thoroughly review a StaaS provider's code and hardware for vulnerabilities, ensuring they are free from critical flaws that could compromise the security of users' funds or the integrity of the network. To foster trust, the results of these audits should be published and made publicly available, offering additional assurance that the platform operates safely and transparently. To complement the audit process and boost community involvement within an open-source project, a robust *bug bounty* program may be another critical consideration. Bug bounty programs incentivize the broader community of developers and security experts to identify and report vulnerabilities in the platform's code. By offering rewards for these discoveries, StaaS providers can preemptively address potential security issues before they can be exploited, thus enhancing the overall security of the service.

In addition to the technical robustness of the platform, the concept of being *battle-tested* is vital. Specifically, a StaaS platform that has been available and used by the public for a significant period has had its systems tested under real-world conditions. This longevity naturally correlates with reliability and stability, as the platform has had ample opportunity to refine its processes and respond to any issues that have arisen during its operation. In other words, a well-established track record can be a strong indicator of a platform's capability to handle the complexities and demands of a live blockchain environment. Moreover, the process of *onboarding* users is another key factor. A *permissionless* StaaS service allows users to participate without requiring special permissions, account sign-ups, or Know Your Customer (KYC) processes. This openness is crucial for maintaining the decentralized ethos of blockchain, where anyone can contribute to the network without being subject to centralized authority or gatekeeping. However, this lack of formal user verification can lead to potential legal issues, especially in jurisdictions with stringent regulatory requirements. Without KYC procedures, it becomes more challenging to comply with anti-money laundering laws and other regulatory mandates, potentially exposing both the service provider and users to legal risks. As a result, careful consideration of the legal landscape is necessary.

Conclusion and future outlook

Staking as a service has emerged as a pivotal force in democratizing access to PoS participation, enabling users to earn rewards without the technical complexities and financial burdens of running their own validator nodes. By leveraging the expertise and infrastructure of StaaS providers, users can bypass the complexities of node management, software updates, and security protocols. This streamlined approach enables individuals to participate in PoS with minimal technical knowledge, opening up the opportunity to earn passive income from their cryptocurrency holdings. As the PoS ecosystem continues to mature, StaaS is expected to play an increasingly important role in driving adoption and facilitating broader participation in blockchain networks. At the same time, there are important risks and key considerations one must contemplate before partnering with a StaaS provider, such as the open-source and auditability nature of their technology, as well as the onboarding process and potential legal ramifications.

The future of StaaS is likely to be shaped by ongoing innovation, increased competition, and evolving regulatory landscapes. As the market matures, we can anticipate greater

transparency, enhanced security measures, and a wider range of services catering to the diverse needs of cryptocurrency holders. The continued growth and development of StaaS hold the potential to further empower individuals within the blockchain ecosystem, fostering greater decentralization and financial inclusion.

References

Ethereum Foundation. (2024). *Proof-of-Stake Rewards and Penalties*. Retrieved August 22, 2024, from https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/#slashing.

Luo, X. (2022). *Ethereum Already Showing Signs of Increased Centralization*. Retrieved October 21, 2024, from CoinDesk: https://coindesk.com/tech/2022/09/15/eth-may-already-be-showcasing-increased-signs-of-centralization/.