46. Staking and proof of stake

Yusuf Ozdemir and Arthur Carvalho

Introduction

The innovation and growth of Bitcoin have reshaped the landscape of digital finance, marking a revolutionary shift in how value is stored and transferred. At the heart of Bitcoin's success lies the technology now known as *blockchain*—a decentralized ledger system that ensures transparency, security, and immutability in digital transactions. Bitcoin's blockchain operates on a consensus mechanism called *proof of work* (PoW), where network participants, often called *miners*, continuously compete to solve computationally intensive mathematical problems. The first miner to solve the puzzle gets the right to create and add a new block of transactions to the blockchain and is rewarded with newly minted cryptocurrency and transaction fees. The difficulty of the puzzle adjusts over time to ensure that new blocks are added at a consistent rate, which is about ten minutes at the time of writing. This process makes it extremely difficult and costly to alter the blockchain, thereby providing security and preventing some fraudulent activities.

While PoW has been pivotal in establishing the reliability and integrity of blockchain technology, it has also drawn significant criticism for its scalability issues and energy-intensive nature. Regarding the latter, at the time of writing, the annual energy consumption of the Bitcoin network is estimated to be almost 145.38 terawatt-hours (Cambridge Centre for Alternative Finance, n.d.). This consumption is slightly below the annual energy usage of Malaysia, which is ranked as the 26th most energy-intensive country in the world. The issue of energy consumption has led to the exploration and adoption of alternative consensus mechanisms, such as *proof of stake* (PoS), which aim to provide similar security benefits while reducing environmental impact.

PoS is an alternative consensus system that some blockchains use to validate transactions without relying on computationally demanding work. In this system, network participants (nodes) offer their cryptocurrency as collateral—a process called *staking*—for the chance to validate blocks and earn rewards. Although there are different implementations of the PoS mechanism, a node (now called a *validator*) is typically chosen randomly to create a new block, with the likelihood of selection directly proportional to the amount of staked cryptocurrency. Similar to PoW, when a block of transactions is successfully produced, the node proposing the block is rewarded with newly minted cryptocurrency. While the staking process incentivizes network participants to invest in the network, it can also be used to penalize potentially fraudulent or erroneous activities. For example, a node can have its staked cryptocurrency *slashed* if it validates fraudulent transactions or fails to propose a block when required, leading to a loss of the deposited funds.

Besides energy efficiency, PoS networks improve scalability by enabling faster consensus and higher transaction throughput compared with PoW systems. By decoupling transaction validation from intensive computational work, PoS systems allow a larger number of transactions to be processed per second, making it easier for blockchains to handle growing user demands. In contrast, PoW networks rely on miners solving complex puzzles, which inherently limits throughput and introduces latency. This dependency often leads to congestion during periods of high demand, driving up transaction costs and causing delays. PoS networks, by eliminating the need for computationally intensive processes, address these limitations and present a more scalable solution for blockchain technology.

Currently, Ethereum is the most popular blockchain network utilizing proof of stake. Launched around 2015, Ethereum is a decentralized platform that enables developers to build and deploy *smart contracts*, which are software programs running and stored on the blockchain. In other words, Ethereum extends blockchain functionality beyond simple transaction storage and validation by offering a flexible, programmable environment through its Ethereum Virtual Machine. In terms of market capitalization, Ethereum is currently the second largest blockchain technology, behind only Bitcoin (CoinMarketCap, n.d.). Like Bitcoin, Ethereum initially used PoW as its underlying consensus mechanism to validate transactions. However, the high energy consumption and scalability issues associated with PoW led to the development of Ethereum

2.0, a major upgrade with the goal of transitioning Ethereum to the PoS mechanism. The full transition, known as "The Merge," was completed in September 2022, significantly reducing energy consumption by approximately 99.95% (Beekhuizen, 2021) and laying the groundwork for future scalability improvements. While Ethereum 2.0 is more energy efficient and significantly improves the network's ability to handle more transactions, issues related to inclusivity have arisen. Specifically, nodes must stake at least 32 cryptocurrency units (over 83,000 USD currently) to be able to join the pool of validators/block proposers, which is prohibitively expensive for many.

Staking innovations

The rise of *staking pools* has played a crucial role in democratizing access to PoS networks, especially in ecosystems like Ethereum, where the barrier to entry can be prohibitively high. Staking pools allow multiple users to combine their cryptocurrencies to meet the minimum staking requirement, thereby increasing their collective chances of being selected as validators. In a generic staking pool implementation, users delegate their funds to a central pool operator who manages the validator nodes, and rewards are distributed proportionally based on the amount each participant has staked. Staking pools can be categorized into various types, each offering different levels of decentralization and control. For instance, *decentralized staking pools* like Lido operate through smart contracts, allowing users to retain ownership of their staked assets while participating in the network's validation process. As we discuss later when talking about liquid staking, these pools may issue derivative tokens that represent staked assets, which can be used in other applications, further enhancing the utility and liquidity of the staked funds. On the other hand, *centralized exchanges*, such as Coinbase, also offer staking services, providing a more user-friendly experience at the cost of increased custodial risk, as users must trust the exchange with their assets.

The emergence of *staking-as-a-service* platforms represents an alternative to staking pools and marks the next evolution in the ecosystem. These platforms provide a streamlined and often fully managed staking experience, catering to both individual investors and institutional clients. The service providers handle the technical complexities of setting up and maintaining validator nodes, allowing clients to stake their cryptocurrencies with minimal effort. This service is particularly appealing to those who may lack the technical expertise or resources to manage their own staking infrastructure. However, as with staking pools, users must carefully consider the trade-offs, such as potential fees and the risks associated with entrusting their assets to third-party providers.

In addition to the standard PoS system discussed thus far, other staking-based consensus mechanisms have been developed to address specific challenges and optimize various aspects of blockchain networks. One such alternative is called *delegated proof of stake* (DPoS). While DPoS shares the foundational concept of staking with PoS, where network participants commit their cryptocurrency to validate transactions and reap the rewards, DPoS introduces a more democratic approach. In DPoS, stakeholders use their staked cryptocurrencies to vote for a select group of validators, now known as *delegates*, who are entrusted with the responsibility of validating transactions and producing new blocks. The number of delegates is fixed and typically small, which allows for faster block production and, consequently, a higher number of processed transactions per unit of time compared with both PoW and PoS. For example, the DPoS-based blockchain EOS has around 600 potential validators in its network; however, only 21 active block producers are elected by stakeholders to operate at any time (EOS Authority, n.d.), whereas Ethereum had over one million (James, 2024). The aforementioned speed and efficiency make DPoS particularly attractive for applications requiring rapid transaction processing. However, the benefits of DPoS come with notable trade-offs. For example, the delegation of voting power to a limited number of validators raises concerns about centralization. In particular, a small group of delegates, if collusive, could exert disproportionate influence over the network, potentially undermining the decentralization that blockchain systems aim to preserve. Moreover, the voting system itself may be prone to voter apathy or manipulation, where influential stakeholders can sway delegate selection in ways that do not necessarily reflect the broader community's interests.

Liquid staking represents another innovation within the staking ecosystem, offering a solution to the liquidity constraints typically associated with PoS. In traditional PoS, staked cryptocurrencies may be locked, meaning they cannot be transferred or utilized in other financial activities until they are unstaked, a process that may take considerable time depending on the network's design. Liquid staking addresses this limitation by providing users with liquid staking tokens, which are derivative assets that represent the staked value. These tokens can be freely traded or used in other applications, enabling stakers to earn rewards without sacrificing liquidity. The introduction of liquid staking offers significant advantages, particularly in terms of capital efficiency and flexibility. However, liquid staking also introduces new risks. In particular, the derivative nature of the tokens may lead to complex dependencies and exposure to smart contract vulnerabilities, particularly if the protocols issuing the tokens are not rigorously audited. Additionally, the creation of liquid markets for staking derivatives can lead to price volatility or speculative behavior, potentially destabilizing the underlying network.

Staking benefits, issues, and future

As previously discussed, a primary advantage of PoS systems over PoW mechanisms is that PoS eliminates the need for energy-intensive computations, leading to a substantial reduction in overall energy consumption. This efficiency arises because network participants are no longer competing for rewards based on computational power; instead, rewards are determined by the size of their stake. Moreover, despite the lower energy demands, PoS still allows validators to generate passive income. Finally and more broadly, staking may give users a say in the governance of a blockchain network. Specifically, participants who stake their assets may gain voting rights in a network's decision-making processes, enabling them to influence protocol upgrades, governance proposals, and other critical aspects of the network's development. This democratized approach to governance empowers users to directly impact the direction and policies of the network, aligning the incentives of stakeholders with the long-term success and stability of the blockchain. However, this increased governance role also introduces potential challenges, such as the risk of centralization if large stakeholders dominate voting power.

The last observation represents one of the main criticisms of PoS, which was previously hinted at. Specifically, validators who stake more money have a higher chance of being selected as block proposers, leading to increased earnings that can be reinvested in staking. This cycle can lead to the centralization of power as the rich get richer, thereby defeating the basic decentralization premise of blockchain and leading to an uneven distribution of wealth. Such an accumulation of wealth can lead to other significant issues, such as the possibility of a *51% attack*. In a 51% attack, an entity or coalition that controls more than half of the total staked cryptocurrency could, in theory, exert undue influence over the network, enabling it to manipulate transaction histories, double-spend coins, or prevent other participants from validating transactions. While safeguards such as staking limits, slashing, and bonding periods might exist to make such attacks less practical or economically unfeasible, it can still be theoretically possible for large stakeholders to accumulate a majority stake in PoS networks. For example, it has been reported that, at a certain point, 64% of the staked cryptocurrencies on Ethereum were controlled by only five entities (Jenkinson, 2022).

Regulatory considerations are also increasingly relevant for PoS systems as governments and financial regulators seek to address the unique challenges posed by staking-based networks. PoS introduces questions about compliance, particularly regarding taxation, anti-money laundering (AML) measures, and securities laws; for example, staking rewards may be subject to taxation, yet the treatment varies widely across jurisdictions, creating potential legal ambiguities for participants. Additionally, regulatory bodies may view staking pools or staking-as-a-service platforms as financial services, which would subject them to strict financial regulations. For example, the US Securities and Exchange Commission (SEC) recently charged the exchanges Kraken (US Securities and Exchange Commission, 2023a) and Coinbase (US Securities and Exchange Commission, 2023b) for their unregistered staking-as-a-service programs.

As blockchain technology continues to evolve, the future of proof of stake appears bright, driven by innovations that promise to address current limitations and unlock new opportunities. For example, the advent of *cross-chain staking* is particularly exciting, where users can stake an asset on one blockchain and receive (tokenized) rewards on another blockchain or participate as validators and earn rewards from multiple networks, thus broadening the scope of staking. Innovations like cross-chain staking foster greater interoperability between blockchain networks, enhancing liquidity and enabling more sophisticated applications across ecosystems. Moreover, the integration of staking mechanisms with decentralized finance protocols is poised to catalyze further growth and innovation within the cryptocurrency space, offering users novel ways to earn rewards, participate in governance, and engage with financial services directly, without intermediaries. Finally, as staking continues to gain traction within the blockchain ecosystem, there is a natural expectation for clearer legal frameworks and regulatory guidance to support its development. Proper regulations will help mitigate risks, protect participants, and foster a more secure and sustainable environment for staking innovations to thrive. While challenges such as centralization, legal, and security risks remain, the ongoing development and refinement of PoS systems suggest that these hurdles can be mitigated, paving the way for a more sustainable, inclusive, and interconnected blockchain future.

References

Beekhuizen, C. (2021). *Ethereum's energy usage will soon decrease by ~99.95%*. Retrieved August 21, 2024, from https://blog.ethereum.org/2021/05/18/country-power-no-more.

Cambridge Centre for Alternative Finance. (n.d.). *Cambridge Bitcoin Electricity Consumption Index*. Retrieved August 21, 2024, from https://ccaf.io/cbnsi/cbeci.

CoinMarketCap. (n.d.). *Today's Cryptocurrency Prices by Market Cap*. Retrieved August 21, 2024, from https://coinmarketcap.com/.

EOS Authority. (n.d.). *EOS Explorer*. Retrieved August 21, 2024, from https://eosauthority.com/.

James, A. (2024). *Ethereum's 13,900 nodes are running 1 million validators, with 26% of the supply staked*. Retrieved August 21, 2024, from https://www.theblock.co/post/285262/ethereum-one-million-validators.

Jenkinson, G. (2022). *64% of staked ETH controlled by 5 entities—Nansen*. Retrieved August 21, 2024, from Cointelegraph: https://cointelegraph.com/news/64-of-staked-eth-controlled-by-five-entities-nansen.

US Securities and Exchange Commission. (2023a). *Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay $30 Million to Settle SEC Charges*. Retrieved October 10, 2024, from SEC: https://www.sec.gov/newsroom/press-releases/2023-25.

US Securities and Exchange Commission. (2023b). *SEC Charges Coinbase for Operating as an Unregistered Securities Exchange, Broker, and Clearing Agency*. Retrieved October 25, 2024, from SEC: https://www.sec.gov/newsroom/press-releases/2023-102.