MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of University of California, Berkeley School of Law, Georgetown University Law Center, University of Chicago Law School, and Placeholder Venture Capital

---

On June 23, 2025, Crypto Task Force Staff met with representatives from University of California, Berkeley School of Law, Georgetown University Law Center, University of Chicago Law School, and Placeholder Venture Capital.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. University of California, Berkeley School of Law, Georgetown University Law Center, University of Chicago Law School, and Placeholder Venture Capital representatives provided the attached documents, which were discussed during the meeting.

Agenda for Committee Meeting with the SEC on Staking Regulation

1. Introductions
    a. Introduction of BLAB committee members: background and experience
2. Current Staking Landscape
    a. Key distinctions between blockchain-level staking, protocol-level staking, and financial-instruments associated with staking
    b. Importance of decentralization and open-source infrastructure in blockchain level staking for the stability and long-term success of the public infrastructure technology
3. Regulatory Framework and Recommendations
    a. Definition
        i. Proposal for a narrow and qualified definition of "staking" aligned with SEC goals
        ii. Discussion on labeling rules for staking products (akin to the 80% "names rule")
        iii. Framework for pre-approval and certification of staking-related product labels
        iv. Differentiation between custodial and non-custodial staking for regulatory treatment
    b. Economic Safeguards
        i. Proposal for a cap on advertised staking yields tied to protocol-native base rates
        ii. Discussion of intermediary fee limitations and justification requirements
        iii. Importance of transparent disclosures on gross yield, net yield, and fee structures
        iv. Call for minimum standards for slashing risk disclosure and liability allocation
    c. Disclosure and Transparency Enhancements
        i. Real-time, interactive, in-interface disclosure requirements for validator performance and rewards
        ii. Participatory platforms for collaborative disclosure updates (developer and community involvement)
        iii. Support for developer tools and incident-reporting interfaces
    d. Infrastructure Centralization and Control
        i. Risks associated with reliance on centralized relayers, sequencers, and infrastructure providers
        ii. Recommendation for disclosure mandates for validator influence and licensing thresholds
        iii. Enforcement of open-source requirements for validator clients and critical staking software
4. Feedback from the SEC and the Crypto Task Force on the letter and thoughts about next steps in the regulation of staking
    a. Anything else that BLAB can do to be involved with the development of this regulation

Berkeley Law Students
Kiyan Mohebbizadeh (kmohebbizadeh@berkeley.edu)
Jana Krahforst (janakrahforst426@berkeley.edu)
Shreeyash Mittal (shreeyash@berkeley.edu)
Yae Lin Lee (erincita_2024@berkeley.edu)
Giovana Grupenmacher (g.grupenmacher@berkeley.edu)
Varsha Jhavar (varshajhavar@berkeley.edu)

Industry Partners and Berkeley alum: Gurnoor Narula (gurnoor@placeholder.vc)

Georgetown Law Student: Joey Yu (zy299@georgetown.edu)

U Chicago Law Student: Yi Qu (yiqu@uchicago.edu)

Blockchain and Law at Berkeley (BLAB): Kiyan Mohebbizadeh (kmohebbizadeh@berkeley.edu), Gurnoor Narula (gurnoor@placeholder.vc), Joey Yu (zy299@georgetown.edu), Jana Krahforst (janakrahforst426@berkeley.edu), Yi Qu (yiqu@uchicago.edu), Shreeyash Mittal (shreeyash@berkeley.edu), Yae Lin Lee (erincita_2024@berkeley.edu), Giovana Grupenmacher (g.grupenmacher@berkeley.edu), Varsha Jhavar (varshajhavar@berkeley.edu)

Re: Comment in Response to Commissioner Hester Peirce's Request for Information on Staking and Related Services

Submitted to the Office of Commissioner Hester M. Peirce: U.S. Securities and Exchange Commission

May 2025

Dear Commissioner Peirce and Members of the Security and Exchange Commission:

On behalf of Blockchain and Law at Berkeley (BLAB), we respectfully submit this comment in response to Commissioner Hester Peirce's request for input regarding the regulatory treatment of staking and related services within the digital asset ecosystem. We commend the Commission for initiating an open dialogue around the future of staking in U.S. financial markets. Staking plays an essential role in securing blockchain networks by incentivizing investors and network participants to contribute to decentralized public ledgers. However, we also recognize that staking carries significant risks, particularly in the way it is marketed to retail participants and the counterparty and agency risks posed by intermediating institutions that offer staking services.

As crypto and staking continue to grow in scale and significance, so too does the need for a comprehensive regulatory framework that protects investors, ensures transparency, and promotes market integrity without stifling innovation. In Part I of our letter, we draw on technical, economic, and legal analysis to offer a comprehensive assessment of the current staking landscape, including consensus layers, protocols, and emerging staking-based financial instruments. Part II of our letter outlines our policy recommendations for the SEC. We urge the Commission to adopt regulatory guidance that recognizes the critical functional differences between blockchain layer staking, protocol custodial and non custodial staking, and related financial instruments. Without such tailored regulation, innovation will be stifled, and investors remain vulnerable to hidden risks including yield opacity, and unclear counterparty obligations. These risks not only threaten individual investor protection but also undermine the transparency, resilience, and decentralization that are foundational to blockchain ecosystems. Clear, informed regulation is therefore not just beneficial but necessary to safeguard market integrity and support the responsible growth of this sector.

I. Staking in the Present Landscape

In this comment letter, we address questions 3, 4, 28, 31 and 32 relating to staking and regulation, with a particular focus on the regulatory treatment of staking as a financial instrument and security class. [1]

The SEC's policy goals are to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital flows by ensuring that investors have access to material information necessary to make informed decisions, thereby promoting transparency and reducing the risk of fraud.[2] In the context of staking, this translates to monitoring that staking programs are transparent and compliant with risk-minimizing practices, as well as making sure that investors are made aware of possible risks associated with staking as an investment.

We start by examining staking's role in incentivizing consensus mechanisms, the role of decentralization in blockchain networks, and the impact of open-source software on this technology. Then we outline the current staking landscape by differentiating between staking as a validator for a blockchain, protocol token staking, and the financial instruments built around staking.

Blockchains and Consensus

A blockchain is a decentralized digital ledger that records transactions across a distributed network of participants. To ensure the ledger remains accurate and tamper-proof, blockchain systems rely on a process called consensus, which allows the network to agree on the validity and order of transactions without relying on a central authority. This is achieved through the participation of validators, specialized network actors who are responsible for proposing, verifying, and confirming new blocks of transactions. Validators are incentivized through rewards, typically issued in the network's native currency, to perform this work honestly and efficiently. These rewards motivate participants to contribute computational resources, maintain continuous uptime, and follow the network's rules, ensuring the blockchain remains secure, operational, and trustworthy.[3]

Incentivization Mechanisms: Distinguishing Between Proof of Work and Proof of Stake

Proof of Work (PoW) and Proof of Stake (PoS) represent two predominant paradigms for decentralized consensus in blockchain networks, each embodying distinct operational principles with implications for security, scalability, energy consumption, and economic incentives. PoW

---

[1] *There Must Be Some Way Out of Here*, https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125

[2] *SEC*, https://www.sec.gov/about

[3] *Bitcoin and Cryptocurrency Technologies*, Arvind Narayanan

requires miners to expend considerable computational effort to solve cryptographic puzzles, thereby validating transactions and securing the blockchain. This process entails significant energy consumption and hardware investments, which act as a resistance mechanism by imposing tangible costs on would-be attackers and by incentivizing honest participation through block rewards.[4] In contrast, PoS eschews energy-intensive computations and selects validators proportional to the amount of cryptocurrency they commit as stake, incentivizing network loyalty through the risk of slashing staked tokens upon misbehavior.[5]

Operationally, PoW secures the network through verifiable resource expenditure, thereby deterring attacks via high upfront and ongoing costs. PoS achieves network security through economic bonding, where validators have their own capital at risk, aligning incentives for honest behavior while reducing energy requirements dramatically. Notwithstanding shared objectives of decentralized validation and irreversibility of transactions, PoS differs markedly in its energy profile, reliance on stake-weighted influence, and validator selection mechanics.[6] These differences result in distinct trade-offs concerning decentralization, scalability, and attack vectors, as well as the nature of validation incentives.

Motivations for the Adoption of Proof of Stake

The transition from PoW to PoS in several blockchain networks, including Ethereum's recent migration, is motivated principally by concerns regarding energy efficiency, transaction throughput, scalability, and broader participation inclusivity. The environmental critique of PoW protocols is particularly salient; PoW networks like Bitcoin consume energy at a magnitude comparable to entire nations, engendering regulatory and societal pressures to pursue sustainable alternatives.[7] PoS addresses these concerns by drastically lowering energy consumption; Ethereum's move to PoS resulted in over 99% reduction in energy use through the elimination of mining's computational race.[8]

Beyond environmental considerations, PoS offers scalability advantages through streamlined validator selection and reduced computational bottlenecks, facilitating faster consensus finality and higher transaction throughput.[9] Economically, PoS lowers the barrier to participation compared to PoW, which necessitates specialized, costly mining hardware; staking requires only capital allocation in the native cryptocurrency, potentially democratizing consensus involvement and enhancing network decentralization. By assigning a financial cost to participation, PoS also mitigates Sybil attacks (where malicious actors attempt to gain influence by generating numerous

[4] *What Is Proof of Work or Proof of Stake?*, https://www.coinbase.com/en-gb/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake
[5] *Proof of Stake (PoS) and Ethereum Energy Efficiency*,https://nano-ntp.com/index.php/nano/article/view/4219
[6] *Proof of Work vs. Proof of Stake in Cryptocurrency*, https://www.researchgate.net/publication/369870684
[7] *Bitcoin Electricity Consumption Index*, Cambridge Centre for Alternative Finance, https://ccaf.io/cbeci/index
[8] *Proof of Stake (PoS) and Ethereum Energy Efficiency*, https://nano-ntp.com/index.php/nano/article/view/4219 ; *The Merge and Beyond*, https://blog.ethereum.org/2022/09/15/the-merge-and-beyond
[9] *Proof of Work vs. Proof of Stake in Cryptocurrency*, https://www.researchgate.net/publication/369870684

fake identities) by making such behavior economically unfeasible.[10] The economic model of PoS anticipates reduced token inflation rates due to more efficient issuance policies, improving long-term sustainability. While PoS introduces new considerations, such as potential stake centralization and novel attack vectors (e.g., long-range attacks), ongoing empirical evaluation from deployments on Ethereum and other platforms informs risk assessment and protocol maturation.[11] Today and for the foreseeable future, PoS has emerged as the most widely adopted consensus mechanism, with investors increasingly leveraging staking to generate stable, predictable returns.

However, as a new form of generating investor returns, PoS introduces a new class of regulatory challenges particularly concerning staking yield disclosures, intermediary fee extraction, and asymmetric risk allocation. Without targeted intervention, staking risks evolving into a structurally opaque and extractive layer within the blockchain economy.[12] As Vitalik Buterin has emphasized, decentralization is not only architectural but also political. PoS systems, while efficient, risk undermining political decentralization and exacerbating economic inequality and systemic risk if staking power becomes concentrated in the hands of a few.[13]

The Role of Decentralization

Decentralization is a foundational principle in distributed ledger technology. It refers to the distribution of control across a wide network of independent participants rather than being concentrated in a central authority.[14] Without decentralization, this trustless system would fail as it would no longer be a peer-to-peer system, but an intermediated transaction, exactly as we have today.[15] A decentralized model eliminates single points of failure, promotes inclusivity, and fosters a trustless environment in which no single actor wields overarching influence. In such systems, decisions are made collectively through consensus mechanisms (a process that enables all nodes in a decentralized network to agree on the validity and order of transactions), enabling the network to remain secure, open, and resistant to manipulation.

When it comes to staking, decentralization becomes especially critical. Staking, being the incentive mechanism for people to participate in operating a blockchain network, involves locking up cryptocurrency to help validate transactions and secure PoS blockchains. Because blockchains are designed as public infrastructures, decentralization in staking ensures wide distribution of validating power. This distribution of validating power is essential to staking and

[10] Sybil Attack, https://www.imperva.com/learn/application-security/sybil-attack/
[11] *Proof of Stake (PoS) and Ethereum Energy Efficiency*, https://nano-ntp.com/index.php/nano/article/view/4219
[12] *Policing Proof-of-Stake Networks: Regulatory Challenges Presented by Staking-as-a-Service Providers and the Need for a Tailored Regime*, https://www.researchgate.net/publication/359582425
[13] *The Meaning of Decentralization*, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.
[14] *Consensus Mechanism*, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
[15] *Bitcoin and Cryptocurrency Technologies*, Arvind Narayanan

the integrity of public blockchains because it ensures security, fairness, and resilience. It prevents any single entity from gaining control over the network, reducing the risk of 51% attacks, censorship, and collusion. Broad participation promotes a more democratic and inclusive system, a requirement of public blockchain infrastructure.[16]

While decentralization is a foundational strength of blockchain networks, its benefits can be undermined when staking power becomes concentrated. When a few entities control large amounts of the staked cryptocurrency, they gain disproportionate influence over transaction validation and governance. This concentrated power introduces central points of control into what is intended to be a trustless, peer-to-peer system, leading to vulnerabilities such as censorship of transactions, preferential treatment, collusion, and diminished user trust. The economic consequences of validator centralization are similarly significant. Concentrated staking power can create oligopolistic market dynamics, where a small number of validators extract outsized rewards and reinforce their dominance through preferential network treatment. This dynamic exacerbates wealth inequality within the network and discourages smaller participants from engaging, ultimately weakening network security and resilience. Moreover, centralized validators may prioritize short-term profit maximization over the protocol's long-term health, increasing the risk of governance capture and stifling innovation. Validator concentration can also undermine confidence in a network's neutrality and fairness, leading to reduced demand for the native token and greater price volatility. Over time, these effects can destabilize blockchain ecosystems that depend on broad participation for their economic sustainability and security, emphasizing the need for protocol-level incentives that promote and preserve decentralization.[17]

The blockchain protocols attempt to deal with bad actors by using a mechanism called slashing. Slashing is used to deter malicious or negligent behavior by validators by forfeiting a portion of the staked tokens when a validator engages in harmful activities such as double-signing blocks, going offline for extended periods, or otherwise violating consensus rules. For staking providers, especially those managing large pools of user-delegated assets, slashing poses significant financial and reputational risks. A slashing event can lead to direct losses for customers, trigger mass unstaking, and undermine confidence in the provider's reliability. As such, proper validator management, infrastructure redundancy, and protocol compliance are critical responsibilities for any entity offering staking services. However, slashing does not pose any sort of barrier to the centralization of staking providers, thus not limiting the consequences of allowing such institutions to prevail. In addition to punitive mechanisms like slashing, several protocols have adopted active governance and policy measures to maintain decentralization. Strategies such as delegation programs, decentralization incentives, minimum validator thresholds, and community

[16] *The Decentralized Finance Crisis*, https://arxiv.org/abs/2002.08099

[17] *Workshop on Trusted Smart Contract*, https://fc20.ifca.ai/wtsc/; *Examining Attacks on Consensus and Incentive Systems in Proof-of-Work Blockchains,* https://arxiv.org/html/2411.00349v2

grants have helped prevent the concentration of power, and preserve the openness, trustlessness, and resilience of blockchain networks.[18]

The Importance of Open Source Technology for Staking

Open-source software is a critical foundation for ensuring the security, auditability, and decentralization of staking ecosystems. In staking, where participants delegate or lock their assets to secure blockchain networks, the underlying validator software and staking infrastructure must be transparent and verifiable by the community. Open-source validator clients allow independent experts to inspect, audit, and improve the code, identifying vulnerabilities and reducing the risk of critical failures or malicious behaviors. Public access to the source code ensures that the network's core infrastructure remains accountable to its users rather than reliant on a centralized entity's assurances.[19]

In open-source staking environments, the community can verify that the validator implementations correctly follow consensus rules, that slashing conditions are enforced fairly, and that no hidden mechanisms exist to prioritize certain transactions or entities. This transparency not only strengthens security through peer review but also fosters greater trust among network participants. By contrast, reliance on closed-source staking software introduces risks of hidden vulnerabilities, arbitrary code changes, and centralization of control all of which could undermine the decentralization that PoS systems aim to preserve.[20]

Moreover, open-source staking infrastructure enables quicker discovery and resolution of bugs, promotes client diversity to avoid systemic risks from a single point of failure, and supports resilience through community maintenance and upgrades. Multiple validator clients developed from open specifications allow networks to remain operational even if one client faces a critical issue. In contrast, closed-source models can slow down emergency response and lock users into vulnerable systems without alternative options.[21]

If staking infrastructure becomes reliant on closed-source or privately maintained clients, it introduces unacceptable concentrations of power: single entities can control validator behavior, dictate protocol upgrades, or conceal vulnerabilities. This undermines the trustless, peer-to-peer architecture that public blockchain networks are designed to maintain. Open source enables community-driven governance, allowing multiple independent teams to review, maintain, and

---

[18] *Proof of Stake*, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#slashing; *What is Decentralization in Blockchain*, https://www.starknet.io/glossary/what-is-decentralization-in-blockchain/; *Base Layer Neutrality*, https://cryptoforinnovation.org/base-layer-neutrality/

[19] *Open Source Security Audit,* Sentinel One https://www.sentinelone.com/cybersecurity-101/cybersecurity/open-source-security-audit/

[20] Guide to Open Source: Importance of Open Source Technology in Cryptocurrency, https://masterthecrypto.com/open-source-technology-in-cryptocurrency/

[21] Validator Client Diversity on Solana, https://stakin.com/blog/validator-client-diversity-on-solana

fork validator software as necessary to enforce consensus norms and recover from governance failures.

Staking in Foundational Blockchain Layers

Staking on the blockchain layer serves as a fundamental incentive mechanism for validators and investors to participate in securing decentralized networks. As Ethan Buchman put it, "a reliable system from unreliable parts." In PoS blockchains, validators are required to lock up a certain amount of cryptocurrency as a stake to gain the right to propose and attest to new blocks. This system replaces the computational cost of PoW with a financial cost, deterring Sybil attacks by making identity replication economically prohibitive. This is required to create it sustainable in permissionless systems (where anyone can join the network without prior authorization). Each slot on the blockchain selects a validator to propose a new block based on their proportion of stake. This block is then disseminated across the network through a gossip protocol. By aligning economic incentives with protocol rules, staking ensures network liveness and encourages honest participation, even in an environment built on inherently unreliable infrastructure, as noted by Ethan Buchman's idea of building "a reliable system from unreliable parts."[22]

Despite its benefits, staking carries several risks that can affect both validators and delegators. One of the most prominent concerns is the "nothing-at-stake" problem, where validators may attempt to validate multiple conflicting chains simultaneously since they incur no inherent cost for doing so. This behavior undermines the integrity of the blockchain by threatening consensus and finality.[23] To mitigate this, PoS networks implement slashing to limit malicious or negligent behavior. While this strengthens security, it introduces financial risk for stakeholders, especially in cases of accidental misbehavior or software faults. Furthermore, since PoS emphasizes liveness over absolute consistency, there remains an inherent trade-off in maintaining a fully safe and decentralized system over an unreliable network like the Internet.

Ethereum

Ethereum uses a chain-based PoS consensus mechanism to keep the network secure and up-to-date. In this system, validators must stake a fixed amount of ETH to participate in proposing and attesting to blocks. This economic commitment deters malicious behavior by putting the validator's funds at risk. In every time slot, one validator is randomly selected (based on their stake) to propose a new block, which is then shared with the rest of the network using a gossip protocol. The consensus process has two main components: LMD GHOST and Casper FFG. LMD GHOST (Largest Message Driven Greedy Heaviest Observed Sub-Tree) ensures

[22] *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains*, https://www.imperva.com/learn/application-security/sybil-attack/
[23] *Understanding Proof of Stake: The Nothing at Stake Theory*, https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027

liveness (the ability of the network to keep making progress) by guiding validators to choose the most supported branch of the chain. It uses validator attestations, submitted every 32 slots (an epoch), to determine which block has the most backing and should be considered the "head" of the chain.

Casper FFG (Friendly Finality Gadget) provides *safety* by finalizing blocks and making them extremely difficult to reverse. It does this by requiring a two-thirds majority of validators to vote on specific checkpoints rather than every single block. Once a checkpoint receives enough support, it becomes finalized, helping protect against long-range attacks or chain reorganizations. Because validators risk having their staked ETH slashed (in this case partially burned/destroyed) if they act maliciously or incorrectly, they are incentivized to follow the protocol honestly. Together, staking, LMD GHOST, and Casper FFG form a robust mechanism that balances progress and security in Ethereum's decentralized network.[24]

Cosmos

Cosmos uses the Tendermint Proof-of-Stake consensus mechanism. The big insight with Tendermint: if the chain is highly fault-tolerant, you can trust the chain to make good decisions about who can produce blocks. If you compromise on safety/consistency and you are choosing your next leader on a canonical chain with less than 100% confidence it is correct, you could go down the wrong path and not recover. While Ethereum prioritizes liveness over safety/consistency, Cosmos chains are non-forking and finalize after every block slot. The only concern here though, is that if there is no consensus reached per slot, block production could theoretically stop.[25]

Solana

In Solana, validators are chosen to produce blocks based on the amount of SOL they have staked, with voting power proportional to stake and a two-thirds supermajority required for finality. The core innovation is Proof of History (PoH), a cryptographic clock that timestamps and orders transactions using a verifiable delay function. This allows Solana to sequence transactions efficiently without requiring validators to synchronize their clocks, enabling high throughput and parallel processing. Block production is organized through a leader schedule, where validators are assigned slots in advance to propose blocks. Each block contains a hash chain from PoH, proving both the order of transactions and the time elapsed. Validators then submit stake-weighted votes to confirm blocks, and a block is optimistically confirmed when it receives two-thirds of the votes, achieving absolute finality after 32 subsequent confirmations. Fork resolution is handled by selecting the heaviest branch based on stake-weighted votes, and once

[24] *What is Gasper*, https://medium.com/@jamaltheatlantean/what-is-gasper-20f6697d3dc6
[25] *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains*, https://www.imperva.com/learn/application-security/sybil-attack/

finality is reached, votes cannot be retracted. Solana's approach prioritizes liveness and scalability, allowing for extremely high transaction throughput-thanks to PoH's decoupling of transaction ordering from consensus-while Tower BFT ensures network safety by requiring a supermajority for finality.[26]

Staking in a Protocol

While staking within a consensus mechanism is directly tied to providing crypto-economic security to the blockchain itself, staking at a protocol or app layer is centered around liquidity, stability, user retention, and active governance participation. Akin to how investors are able to purchase stock within a company and (technically) hold the right to participate in future decisions for said company, onchain investors are able to purchase protocol/app tokens, stake them, and earn benefits for doing so, such as governance rights and a share of profits. It's a win-win situation, as the protocol now gains a more loyal and stable user base that is actively involved in the protocol, and also doesn't face volatile sell and buy pressure for their token from opportunistic short-term investors.

While the stakes for staking activity at the consensus layer are more pronounced than at the protocol/app layer, this activity doesn't come without risks of its own. With a lack of industry-standard auditing standards and a sense of pseudo anonymity onchain, the largest risk is purchasing and staking tokens in a project that is built to be rugpulled. The information asymmetry between opportunistic onchain investors who want to capture revenue share and voting power in a protocol versus ill-intentioned project founders can lead to the misuse or outright theft of locked funds. A more common consequence of staked tokens is the relative capital inefficiency of locked protocol/app tokens, and the illiquidity that leaves for said token in secondary markets, making it prone to unassuming volatility.

UniSwap

Uniswap, a leading decentralized exchange (DEX) on the Ethereum blockchain, enables users to swap ERC-20 tokens without intermediaries. Central to its ecosystem is the UNI token, which grants holders governance rights over protocol decisions, including fee structures and upgrades. While Uniswap doesn't offer traditional staking, it incentivizes liquidity provision through its Uniswap V3 Staker contract. Liquidity providers (LPs) can deposit token pairs into pools, receiving non-fungible token (NFT) representations of their positions. These NFTs can be staked in specific incentive programs to earn additional rewards, promoting liquidity and active participation in the protocol.[27]

---

[26] *Proof Of History: How Solana Brings Time to Crypto*, https://solana.com/news/proof-of-history
[27] *Uniswap V3 Staker Contract*, https://docs.uniswap.org/contracts/v3/reference/periphery/staker/UniswapV3Staker?utm_source=chatgpt.com

However, participating in Uniswap's liquidity pools carries inherent risks. One significant concern is impermanent loss, where LPs may experience reduced returns if the prices of their deposited tokens diverge significantly.[28] Additionally, the decentralized nature of Uniswap allows for the listing of any ERC-20 token, which can expose investors to malicious tokens designed to exploit users, such as "trapdoor" tokens that prevent selling after purchase.[29]

MakerDAO

MakerDAO enables decentralized governance of the DAI stablecoin through the participation of MKR token holders. To vote on protocol proposals (e.g. adjusting stability fees or onboarding new collateral) users must hold MKR tokens and lock them in the MakerDAO governance contract via the official governance portal. The MKR token lock-up serves to enable voting rights and ensure that those influencing the protocol have a vested interest in its long-term stability. This mechanism is critical to maintaining MakerDAO's decentralized ethos and in stabilizing the MKR token value.[30]

Staking-Based Financial Instruments: Liquid Staking & Restaking

When an investor stakes a token through a liquid staking provider such as Lido, Rocket Pool, or Coinbase, they receive a liquid staking token (LST). An LST is a tradable, on-chain representation of their staked token and the rewards it accrues. This token, such as stETH or rETH, reflects the investor's claim on the underlying staked asset and can be freely transferred or used in DeFi applications. The core utility of an LST lies in its liquidity and composability. For example, rather than locking ETH in the Ethereum staking contract and forfeiting its usability, an investor can use the LST as collateral in lending protocols, or trade it on secondary markets while still earning staking rewards from the base Ethereum layer. Essentially, the LST represents a claim on the underlying staked token and any rewards it earns.[31]

Building on this innovation, restaking protocols such as EigenLayer allow investors to redeploy their LSTs to secure infrastructure layers beyond Ethereum, such as middleware networks, rollups, oracles, and data availability layers. From a technical standpoint, the restaked LSTs are deposited into smart contracts that impose additional slashing conditions, enabling the LST to serve as collateral for multiple networks simultaneously. This layered staking approach increases

---

[28] *Assessing Staking Risks: Illiquidity and Price Volatility*, https://figment.io/insights/assessing-staking-risks-illiquidity-and-price-volatility/?utm_source=chatgpt.com
[29] *From Programming bugs to Multimillion Dollar Scams: An Analysis of Trapdoor Tokens*, https://arxiv.org/abs/2309.04700?utm_source=chatgpt.com
[30] *Understanding the MakerDAO Governance Process for StableCoins*, https://blockapps.net/blog/understanding-the-makerdao-governance-process-for-stablecoins-insights-and-mechanisms/
[31] *A Developer Theory of Disclosure*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5137972

the total yield potential for the investor: they continue to earn Ethereum staking rewards through the LST, while also earning additional rewards through the restaking tokens.[32]

Liquid staking and restaking introduce significant risks due to investor reliance on largely unregulated third-party custodians who manage staked assets and issue LSTs. These providers often operate with limited transparency and minimal disclosure requirements, leaving investors exposed to potential mismanagement or failure without adequate recourse or insight into how their funds are used. The risk is further compounded in restaking protocols, where LSTs are reused as collateral across multiple networks. This creates layered rehypothecation risk, as the same underlying staked asset may be pledged to secure obligations in several protocols simultaneously. In the event of stress or failure in one protocol, this entanglement can trigger a contagion effect that spreads across the ecosystem, threatening the solvency or performance of unrelated platforms. Without standardized accountability or regulatory oversight, investors face complex, opaque risks that are difficult to assess and may not be accurately priced into the market value of LSTs.[33]

Lido

Lido is a liquid staking protocol that allows users to stake assets like ETH, SOL, and MATIC while maintaining liquidity through derivative tokens called liquid staking tokens (LSTs)—for example, stETH on Ethereum. When users stake through Lido, their tokens are pooled and delegated to professional validators, while the staker receives an equivalent amount of LST that reflects their staked position and yield. LSTs accrue staking rewards and can be traded, used in DeFi, or transferred, allowing stakers to preserve capital efficiency. The core innovation of Lido lies in its tokenization of staked positions, abstracting away the complexities of validator selection, slashing risks, and lockup periods. However, this also centralizes risk within the Lido protocol: validator selection is governed by the DAO, and the underlying assets are effectively custodied by smart contracts governed by the Lido governance mechanism. The growing dominance of Lido has raised concerns about staking centralization and protocol-level systemic risk because of the growing proportion of staked ETH that it controls. If Lido's smart contracts or governance processes were compromised, the effects could propagate across Ethereum and multiple DeFi protocols that integrate stETH as a base asset.[34]

EigenLayer

---

[32] *What is Restaking in Crypto and How does it Enable Capital Efficiency*, https://www.coinbase.com/learn/advanced-trading/what-is-restaking-in-crypto-and-how-does-it-enable-capital-efficiency

[33] *Liquid Staking: Understanding the Risks*, https://www.ankr.com/blog/liquid-staking-risks/; *A Hitchhikers Guide to Restaking and its Risks*, https://hackernoon.com/a-hitchhikers-guide-to-restaking-and-its-risks

[34] *Liquid Staking and its Benefits*, https://coinmarketcap.com/academy/article/liquid-staking-and-its-benefits-a-deep-dive-by-lido

EigenLayer is a restaking protocol built on Ethereum that allows users to redeploy their staked ETH or liquid staking tokens (such as stETH, rETH, or cbETH) to provide security to additional middleware protocols. This approach creates a new crypto-economic primitive called pooled security, where the same staked asset provides security to Ethereum's consensus and auxiliary services like data availability layers, oracle networks, or bridges. Technically, EigenLayer introduces smart contracts that accept restaked assets and enforce additional slashing conditions for misbehavior across these secondary services. The core innovation is modularity: restakers opt-in to specific services, and those services benefit from Ethereum-grade security without needing their own validator sets. However, the model also introduces significant contagion risk. Restaked ETH is exposed to multiple slashing vectors, a failure or malicious event in one restaked protocol could slash assets used across others. EigenLayer's design thus enhances capital efficiency and security composability but at the cost of increased complexity and interconnected slashing risk. The protocol also raises new governance challenges, such as determining how slashing conditions are enforced, how restaking opt-ins are managed, and how restakers are compensated for layered risks.[35]

II. Policy Recommendations

Defining Staking as a Financial Instrument

Given the increasing diversity of crypto-related financial instruments marketed under the label of "staking," there is a strong regulatory rationale for adopting a narrow and qualified definition of staking consistent with the SEC's mandate and past practice. Since the early 2000s, the SEC has enforced various "names rules," requiring that investment funds whose names imply a particular asset class, sector, or strategy must allocate at least 80% of their assets accordingly.[36] This rule is intended to prevent investors from being misled by misleading or overly broad product labels at first impression. A similar approach could apply in the crypto context, where products labeled as staking vary widely in their mechanics, risk profile, and investor protections. Some of these so-called staking products function more like lending, rehypothecation, or leveraged yield-generating strategies, rather than the protocol-native staking mechanisms typical of proof-of-stake blockchains.

The SEC has already signaled concern over this ambiguity by initiating enforcement actions against major custodial staking service providers like Kraken and Coinbase. These actions suggest a growing regulatory desire to distinguish custodial staking-as-a-service offerings from non-custodial, protocol-native staking, where users retain control of their assets while participating directly in consensus. A more constructive and transparent regulatory approach could involve the SEC pre-approving the use of the term "staking" for products that meet clearly

[35] *Restaking Overview*, https://docs.eigenlayer.xyz/restakers/concepts/overview
[36] 17 CFR 270.35d-1

defined standards, similar to how the FDA certifies terms like "organic." Labels such as "SEC-approved non-custodial staking product" could help protect consumers from misleading marketing and allow the crypto industry to innovate responsibly within a framework of consistent disclosures and technical oversight.

We therefore urge the Commission to adopt the following regulatory actions regarding staking yield and service fee regulation:

1. Definition Standardization: Develop a formal, narrow definition of "staking" that aligns with protocol-native mechanisms, clearly distinguishing them from lending, rehypothecation, and other yield-generating strategies.

2. Labeling Compliance Rule: Implement a staking names rule analogous to the 80% rule for investment funds, requiring that products marketed as "staking" to satisfy enumerated requirements such as engaging in substantial protocol-native staking activities.

3. Pre-Approval of Product Labels: Require pre-approval from the SEC for the use of "staking" in product names or marketing, ensuring consistency, investor clarity, and alignment with defined standards.

4. Custodial vs. Non-Custodial Disclosures: Mandate clear labeling of staking products as either "custodial" or "non-custodial," with prominent disclosures regarding asset control, custody risks, and reward distribution mechanics.

5. Accreditation of Staking Products: Introduce a labeling framework similar to FDA certification (e.g., "SEC-approved non-custodial staking product") to provide consumers with trustworthy signals of regulatory compliance and risk transparency.

Yield Caps and Fee Regulation in Staking Models

As staking becomes a core infrastructure element of blockchain networks, the absence of standardized safeguards around validator yield and intermediary compensation introduces measurable risks to retail participants, market transparency, and systemic stability. [37] Two distinct regulatory mechanisms are required to address this imbalance: (1) a cap on staking interest rates and (2) a limitation on intermediary fees.

First, uncapped staking yields—particularly when advertised by custodial providers—create asymmetric information environments and invite regulatory arbitrage. Promised returns frequently diverge from protocol-native staking rewards, with service providers either

[37] *Digital Asset Staking Guide (Version 2)*, https://www.hoganlovells.com/-/media/project/english-site/our-thinking/pdfs/digital-asset-staking-guide-v2-070225.pdf

subsidizing returns to attract inflows or concealing variability through opaque accounting.[38] This distorts risk perception, misrepresents the inherently volatile nature of on-chain returns, and undermines informed investor choice. A protocol-aligned cap on advertised interest rates, tied directly to the base reward rate offered by the underlying network, is necessary to restore economic signal fidelity. Such caps would reduce unsustainable reward inflation, prevent subsidized marketing gimmicks, and align investor expectations with protocol-level realities.

Second, even when advertised yields are realistic, custodial staking platforms - ranging from centralized crypto exchanges to traditional financial institutions - often deduct significant, undisclosed fees from the actual network rewards. This is a separate but equally urgent issue. Platforms such as Coinbase, Binance, and Kraken routinely retain 15–25% of staking rewards, with retail users receiving only 3–3.5% APY while the underlying network generates 4.5–5%. These deductions are rarely disclosed clearly, distorting competitive dynamics and disproportionately impacting retail participants. A regulatory cap on fees charged by brokers and exchanges, combined with enforceable disclosure requirements, is necessary to ensure users receive a fair share of the staking rewards they generate.

Moreover, many staking-as-a-service models introduce substantial slashing risks that remain largely unregulated. In practice, these risks are often externalized to retail users without transparent disclosures regarding their likelihood, the allocation of responsibility, or whether any insurance mechanisms are in place. As a result, retail stakers may bear disproportionate risks for operational failures over which they have no control.[39] Effective regulation must therefore establish minimum standards for slashing-related risk disclosure, liability allocation, and, where appropriate, loss mitigation mechanisms.

Both interest rate caps and fee limitations are complementary. One regulates what can be promised, the other regulates how much can be taken. Without both, centralized intermediaries will continue to dominate staking economics through opaque pricing and extractive reward structures, undermining retail participation and decentralization incentives. Furthermore, these risks exist in a fragmented regulatory environment. The IRS has already recognized staking rewards as taxable income (*Jarrett v. U.S.*), but no comparable protections exist against excessive intermediary extraction.[40] If staking is taxable, it must also be safeguarded under consumer protection principles.

This is particularly urgent as legacy financial institutions expand into staking services: Fidelity, Robinhood, Charles Schwab are launching staking-as-a-service offerings, and other U.S. banks are lobbying for the inclusion of staking in ETF products. Absent regulation, this expansion risks

[38] *How Does Coinbase's Staking Work?*, https://help.coinbase.com .
[39] *Slashing Conditions*, Ethereum https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/slashing/; *Policing Proof-of-Stake Networks: Regulatory Challenges Presented by Staking-as-a-Service Providers and the Need for a Tailored Regime*, https://www.researchgate.net/publication/359582425
[40] *Jarrett v. United States*, No. 22-6023 (6th Cir. 2023)

replicating historical abuses from the asset management industry: high fees, low transparency, and retail disadvantage.

We therefore urge the Commission to adopt the following regulatory actions regarding staking yield and service fee regulation:

1. Staking Yield Cap: Establish a cap on advertised staking yields, directly tied to the protocol-native base reward rate, to prevent deceptive marketing and protect retail users.
2. Fee Limitation: Impose a maximum fee cap of 5% on staking rewards retained by intermediaries, unless higher costs are disclosed and justified through auditable infrastructure operations.
3. Mandatory Disclosure Standards: Require all staking providers to publish standardized, auditable information including:
    a. Gross network yield vs. actual user payout;
    b. Percentage-based fee breakdown.
4. Personal Staking Exemption: Rulemaking should exclude direct staking by individuals from enforcement but ensure full compliance from intermediated services.

Disclosure

In the fast-paced and often volatile environment of blockchain networks, real-time public disclosure plays a critical role in protecting investors and maintaining trust. Unlike traditional financial markets, blockchain protocols can undergo rapid changes in governance, liquidity, and security—often driven by social sentiment, technical upgrades, or emergent vulnerabilities. A well-designed disclosure system should provide timely, accessible, and actionable information not only for investors, but also for developers. In the context of staking, this means offering up-to-date insights into validator performance, staking yields, rewards distribution, network health, and protocol changes. Such data should be presented in an interactive and user-friendly format (integrated into wallets, dashboards, or blockchain explorers) with visual elements like graphs, alerts, or performance widgets that encourage active engagement rather than passive observation. Disclosures should be readable, relevant, and brief, but also dynamic—designed not just for filing, but for informing ongoing decision-making.

Beyond static updates, an ideal system would also support collaborative and decentralized disclosure frameworks. Drawing inspiration from platforms like GitHub, developers could propose updates, flag concerns, or provide transparency tools directly into the network's disclosure layer, while community members, including investors, could verify, comment, and upvote relevant changes. This participatory model could be further gamified to encourage

meaningful engagement and improve the discoverability of high-value updates. Importantly, tailored tools for developers (e.g. smart contract auditing interfaces or real-time visualizations of validator activity) could elevate not only developer transparency but also investor confidence. In cases involving slashing risk or security incidents, real-time updates about coverage mechanisms or remediation efforts could reduce uncertainty and help manage systemic risk. By building disclosure into the blockchain's user interface and governance structure, projects could foster a more informed, empowered, and resilient ecosystem that is aligned with the decentralized principles they aim to uphold.[41]

We therefore urge the Commission and relevant stakeholders to adopt the following measures to improve disclosure and transparency in staking ecosystems:

1. Require Real-Time, In-Interface Disclosures: Mandate live updates on validator performance, staking yields, and protocol changes directly within wallets, explorers, and dashboards.

2. Enable Participatory, Open Disclosure Platforms: Support collaborative systems where developers and users can propose, verify, and upvote disclosures, similar to GitHub.

3. Support Developer Tools and Incident Reporting: Encourage smart contract audit interfaces, validator analytics, and real-time disclosures for slashing and security events.

Company controls

As staking grows in importance within blockchain ecosystems, the degree of decentralization across infrastructure layers becomes a key regulatory concern. While a network may appear decentralized at the level of consensus, its communication infrastructure may rely heavily on centralized actors such as relayers (e.g., Flashbots), cloud services (e.g., AWS), or node access providers (e.g., Alchemy). This creates a brittle architecture in which validator coordination and transaction propagation are vulnerable to centralized points of failure. Different Layer 1 networks exhibit vastly different decentralization profiles: Ethereum, with thousands of globally distributed nodes, offers strong censorship resistance and fault tolerance, whereas networks like Solana or Ripple maintain smaller validator sets and higher infrastructure centralization, raising the risk of collusion, downtime, or censorship. These issues are further magnified in Layer 2 rollups, where most rely on a single sequencer and are governed by multisig wallets controlled by core teams—introducing additional trust assumptions and reducing transparency for users and investors.

In the absence of robust decentralization, a comprehensive regulatory framework for staking becomes critical to investor protection and network integrity. This includes minimum disclosure

[41] *A Developer Theory of Disclosure*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5137972

and licensing requirements for entities that control a meaningful share of validating power. Key disclosures should identify validator affiliations, stake concentration, and governance influence, including whether validators participate in coordinated voting or disproportionately shape protocol decisions. Investors should also have access to data on validator behavior—such as transaction inclusion practices (e.g., censorship, MEV extraction), compensation models, uptime records, slashing incidents, and jurisdictional exposure. These disclosures would complement on-chain enforcement mechanisms like slashing by enabling informed oversight and early identification of problematic patterns. Licensing dominant validators or staking providers at defined thresholds of influence would introduce enforceable standards and eligibility criteria, adding a layer of accountability to centralized actors within the network. To reinforce transparency, networks and providers should also adopt open-source validator software, with disclosed audit histories, governance mechanisms for code changes, and security patch protocols. Together, slashing, disclosure, and licensing create a multi-layered governance system that combines protocol-level enforcement, real-world accountability, and public oversight to ensure blockchain networks remain secure, transparent, and aligned with the interests of users and investors.

L1	Validator Count	Control Distribution	Downtime Risk	Censorship Resistance	Example Use
Ethereum	1,000s of nodes globally (incl. 1M+ validators)	Widely distributed across individuals, companies, and geographies	Very low	Very high	Public blockchain
Solana	Dozens to a few hundred validators; ~2,000+ nodes total, but high resource demands limit who can run a validator	Concentrated among high-perf infra providers (many in data centers)	Medium – several major outages in 2022–23	Medium – possible censorship by stake concentration	High-speed DeFi apps
Ripple (XRP Ledger)	~150 known validators, but most nodes follow Ripple's default UNL (Unique Node List)	Heavily influenced by Ripple Labs (they curate and publish the default validator list)	Medium – Ripple Labs' infrastructure is critical to network function	Low – validator set is permissioned and curated by a central entity	Enterprise and banking transfers (e.g., RippleNet/XRP)

We therefore urge the Commission and relevant stakeholders to adopt the following measures to address infrastructure centralization risks in staking systems:

1. Mandate Disclosures on Validator Influence and Behavior: Require entities controlling significant validating power to disclose affiliations, stake concentration, governance participation, censorship practices, uptime, and jurisdictional exposure.

2. Introduce Licensing for Dominant Validators and Staking Providers: Establish licensing requirements for validators or providers exceeding defined thresholds of influence to ensure enforceable standards and accountability.

3. Require Open-Source Validator Infrastructure: Mandate the use of open-source validator software with published audit histories, transparent governance for code changes, and documented security protocols.

Open Source Validator Infrastructure

To safeguard decentralization, auditability, and network resilience, it is critical that staking-related infrastructure, particularly validator clients and staking middleware, remain open source. In the context of governance, open-source validator infrastructure promotes transparency in network operations, distributes control over consensus-critical software, and reduces systemic risks associated with reliance on centralized or proprietary codebases.[42]

We recommend that the SEC require:

1. Open Source Infrastructure that critical staking infrastructure be open source under a recognized, permissive license such as MIT, Apache 2.0, or GPL.[43]

2. Disclosure: Public disclosures should also specify whether validator clients are open source, whether multiple independent validator clients are available and actively maintained, how protocol upgrades are implemented and who holds authority over software updates, and whether users and operators can independently audit, fork, or modify the validator software if necessary.[44]

This approach would ensure that no single party can unilaterally control staking operations or governance outcomes.[45] It would also create transparency for investors, who would be better able to assess operational risks and systemic dependencies in staking services. In decentralized networks, open-source infrastructure is not just a technical choice, it is a governance safeguard.

[42] *SoK: Communication Across Distributed Ledgers*, https://eprint.iacr.org/2019/1128.pdf.
[43] *Licenses & Standards*, https://opensource.org/licenses
[44] *Staff Accounting Bulletin No. 121*. SEC, 2022
[45] *Blockchain and the Law: The Rule of Code,* Primavera De Filippi

IV. Conclusion

Staking has emerged as a foundational component of decentralized finance, offering both innovation and complexity. While it presents a powerful alternative to traditional financial systems by aligning economic incentives with network security, the current regulatory framework fails to adequately address the growing diversity and opacity of staking models. Without tailored standards, investors face mounting risks from custodial staking services, undisclosed fees, and systemic vulnerabilities introduced by mechanisms such as liquid staking and restaking.

We urge the Commission to adopt a more nuanced regulatory approach: one that distinguishes between protocol-native and intermediary staking models, sets enforceable limits on fees and advertised yields, mandates robust disclosures, and promotes decentralization through open-source infrastructure. Doing so will not only protect investors but also reinforce the trustless, permissionless ethos that underpins blockchain networks. Through thoughtful oversight, the SEC can help staking evolve into a secure, transparent, and equitable financial primitive that supports innovation while safeguarding market integrity. We appreciate the opportunity to share our views and stand ready to provide further input as needed.

Sincerely,

Kiyan Mohebbizadeh

Gurnoor Narula

Joey Yu

Yi Qu

Jana Krahforst

Shreeyash Mittal

Varsha Jhavar

Giovana Grupenmacher

Yae Lin Lee

DISCLAIMER:

The views and opinions expressed in this letter are solely those of the authors and do not reflect the official positions, policies, or endorsements of any institutions or organizations with which we are affiliated.