Consensys Software Inc.
5049 Edwards Ranch Rd
Fort Worth, TX 76109, United States

April 12, 2024

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Re: File No. SR-CboeBZX-2023-095; Comments in Support of Proposed Rule Change to List and Trade Shares of the Fidelity Ethereum Fund under BZX Rule 14.11(e)(4), Commodity-Based Trust Shares

Dear Ms. Countryman:

Consensys Software Inc. ("**Consensys**") writes in response to the Securities and Exchange Commission's request for comments on whether to approve the proposed rule change filed by Cboe BZX Exchange Inc. ("**BZX**") to list and trade shares of the Fidelity Ethereum Fund under BZX Rule 14.11(e)(4).[1]

Specifically, in connection with providing notice of the grounds for disapproval under consideration, the Commission requested comment on the following question:

> 2. The Exchange raises substantially similar arguments to support the listing and trading of the Shares as those made in proposals to list and trade spot bitcoin exchange-traded products ("**Bitcoin ETPs**"). . . . **Are there particular features related to ether and its ecosystem, including its proof of stake consensus mechanism and concentration of control or influence by a few individuals or entities, that raise unique concerns about ether's susceptibility to fraud and manipulation?**[2]

Our response to the Commission's question addresses Ethereum's architecture at both the protocol and community levels, examining its proof-of-stake consensus mechanism, the decentralized nature of its development community, and the protocol's inherent transparency. We also provide a comparative analysis with Bitcoin's features. The following analysis demonstrates that Ethereum's design and operational features do not make ether more vulnerable to fraud and manipulation within

[1] *See* Self-Regulatory Organizations; Cboe BZX Exchange Inc.; Order Instituting Proceedings To Determine Whether To Approve or Disapprove a Proposed Rule Change To List and Trade Shares of the Fidelity Ethereum Fund Under BZX Rule 14.11(e)(4), Commodity-Based Trust Shares, 89 FR 16804 (Mar. 8, 2024).

[2] *Id.* (emphasis added).

the meaning of 15 U.S.C. § 78f(b)(5), and moreover, they serve to reduce these risks in comparison to Bitcoin.

In short, there is no substantive basis for rejecting ether-based products on the grounds of Ethereum's consensus approach or the inaccurate notion that a concentrated group has the ability to alter the price of ether through fraud or manipulation.

Ethereum's Proof of Stake Implementation

Basics of Ethereum Proof of Stake

As relevant here, a consensus mechanism is the technical means through which a blockchain network such as Bitcoin or Ethereum achieves a unified, authoritative ledger of transactions and accounts for that network's native token. The consensus mechanism assures the public that the resulting ledger is accurate and accepted by the majority of participating nodes. For ETPs that are based on native token prices, the reliability of the underlying consensus mechanism is relevant to whether the price of the underlying asset is susceptible to fraud or manipulation within the meaning of 15 U.S.C. § 78f(b)(5).

In September 2022, the Ethereum network upgraded from a proof of work ("**PoW**") consensus model, similar to that of Bitcoin, to a unique proof of stake ("**PoS**") implementation that affords enhanced security, operates on lower energy, and facilitates scaling that can lead to lower costs and increased transaction capacity.[3]

Under the former PoW model, "miners" competed against each other for the right to mine a block by solving a cryptographic challenge, and therefore needed to invest in computer hardware and consume significant electricity to maintain the blockchain. In Ethereum's PoS implementation, "validators," which are Ethereum nodes run by individuals or entities, each put up a stake of 32 ether to run the network and are randomly chosen to participate in block validation. These validators are responsible for confirming the validity of new blocks and periodically generating and broadcasting new ones, for which they receive protocol-based rewards similar to Bitcoin's compensation of miners. Should a validator fail to perform their duties or attempt to compromise the network, their rewards are forfeited and their staked ether is at risk of being destroyed through a mechanism called

[3] *See Proof-of-stake (PoS)*, Ethereum.org, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (last modified Jan. 25, 2024); Everett Muzzy, *What Is Ethereum 2.0?*, Consensys, https://consensys.io/blog/what-is-ethereum-2 (May 12, 2020).

"slashing."[4] This economic security model achieves not only consensus, but security, efficiency, and resilience as well.

Relevant to the Commission's request for comments, Ethereum's PoS implementation has several built-in protections providing additional security against fraud and manipulation.

Block Finality

Block finality refers to the point at which a block of transactions on the public ledger is considered permanent and immutable, and it has important implications for the useability and security of blockchain technology. PoW consensus models, like Ethereum's earlier model and Bitcoin's current model, achieve probabilistic finality.[5] This means their transaction blocks never achieve absolute finality—instead, they become increasingly final as subsequent blocks are added to the blockchain.[6] As time passes, the risk that a given block will be excluded from the consensus ledger (also known as "reorganized") approaches zero, and thus the block is effectively final. In the case of Bitcoin, finality typically occurs about one hour after the block's initial confirmation.[7]

With its transition to PoS, Ethereum now relies on a model of provable transaction finality, meaning blocks are finalized—effectively set in stone and beyond reversal—within a much shorter time frame.[8] Ethereum currently achieves finality about 15 minutes after a block is validated, with proposals underway to further shorten that time.[9] Ethereum's finality model provides notable benefits, such as increased reliability and integrity, since finalized blocks cannot be reversed. This model provides faster guarantees that the current state of the ledger is accurate and not subject to alteration.[10]

---

[4] *See* Everett Muzzy, *What Is Proof of Stake?*, Consensys, https://consensys.io/blog/what-is-proof-of-stake (May 15, 2020).

[5] *See What Is Block Finality in Crypto?*, CoinDesk, https://www.coindesk.com/learn/what-is-block-finality-in-crypto/ (Mar. 8, 2024).

[6] *See What is Time to Finality (TTF)?*, Chainspect, https://chainspect.app/blog/time-to-finality-ttf (Jan. 25, 2024).

[7] *See id.*

[8] *See id.*; *see also* Benjamin Samuels, *The Engineer's Guide to Blockchain Finality*, Trail of Bits Blog, https://blog.trailofbits.com/2023/08/23/the-engineers-guide-to-blockchain-finality/ (Aug. 23, 2023).

[9] *See Single slot finality*, Ethereum.org, https://ethereum.org/en/roadmap/single-slot-finality/ (last modified Feb. 23, 2024).

[10] *See* Tim Copeland, *What is Block Finality and Why Does it Matter?*, THE BLOCK, https://www.theblock.co/learn/245700/what-is-block-finality-and-why-does-it-matter (Sept. 5, 2023) ("[Block finality] is a critical aspect of blockchain security and reliability, as it ensures that once a transaction is confirmed, it most likely cannot be tampered with.").

Distributed and Randomized Validation Process Prevents Large Stakeholder Control

Ethereum PoS relies on segregation of duties between two groups of block validators: proposers[11] and attesters.[12] This division of labor serves as a check and balance against error and manipulation.

Proposers are responsible for proposing new blocks of pending transactions, and attesters vote to confirm the validity of the proposed block. Assignment of these responsibilities relies on randomness, a committee approach for both efficiency and maximum security, and the re-shuffling of those committees at regular intervals.[13] During each 6.4-minute epoch,[14] every active validator is assigned to be a member of exactly one committee. Committees are assigned validation responsibilities randomly to reduce the risk of manipulation.[15] At the start of the next epoch, all the existing committees are disbanded, and the active validator population is reshuffled into a fresh set of committees.[16]

This model prevents bad actors from predicting who the proposer and attesters for a new block will be. For example, with about 1,000,000 active validators, each validator has a one in a million chance of being chosen as the proposer of a given block.[17] Moreover, even if a given proposer also controlled one-third of all active validators, their probability of controlling enough of the attesting committees randomly assigned to validate their block is still astronomically low. And even if such an improbable scenario occurred, the potential resulting damage is limited only to those few blocks that have not

---

[11] *See Block Proposal*, Ethereum.org, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/block-proposal/ (last modified Jan. 17, 2024).

[12] *See Attestations*, Ethereum.org https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/attestations/ (last modified Feb. 10, 2024).

[13] *See* Ben Edgington, Upgrading Ethereum, Part 2.9 "The Building Blocks," https://eth2book.info/capella/part2/building_blocks/ (Sept. 29, 2023).

[14] In Ethereum, validation occurs on a regular schedule and is split into epochs, which are about 6.4 minutes each. Each epoch is divided into 32 slots of 12 seconds each, and one block may be proposed during each slot. Committees are reshuffled and reassigned each epoch. *See generally Epoch in Ethereum*, Etherscan Information Center, https://info.etherscan.com/epoch-in-ethereum/ (May 2, 2023).

[15] *See* Ben Edgington, Upgrading Ethereum, Part 2.9.4 "Committees," https://eth2book.info/capella/part2/building_blocks/committees/ (Sept. 29, 2023) ("We assign validators to committees randomly in order to defend against a minority attacker being able to capture any single committee. If committee assignments were not random, or were calculable long in advance, then it might be possible for an attacker with a minority of validators to organise them so that they became a supermajority in some committees.").

[16] *Id.*

[17] *See* Open Source Ethereum Blockchain Explorer, https://beaconcha.in/ (last visited Mar. 28, 2024) (displaying 979,107 active Ethereum validators).

yet been finalized, given the block finality model discussed above. This check-and-balance system—whereby proposers initiate block proposals and attesters confirm their validity—ensures a distributed and secure validation system.[18]

Total Cost to Attack

In blockchain security, there is a concept known as "Byzantine fault tolerance" ("BFT"), a metric indicating the minimum proportion of network validators required to function honestly for the system's integrity. For certain network attacks, the BFT threshold is 33% for Ethereum and 50% for Bitcoin.[19] In other words, if an attacker group controls 34% of Ethereum nodes or 51% of Bitcoin nodes, then they can break BFT and compromise the network. Although at first glance Ethereum's lower threshold makes attempting an attack appear easier, researchers have found that the *cost* of obtaining even 34% control of active Ethereum validators is greater than obtaining 51% control of Bitcoin nodes. For example, the total cost to attack on Ethereum would be nearly $34.39 billion (at December 2023 ether prices), and it would take nearly six months.[20] The total cost to attack on Bitcoin, consisting mostly of the cost of computer hardware and electricity, would range from just under $5 billion to a little over $20 billion and could be waged more or less immediately.[21] This makes Ethereum significantly more costly to attack than Bitcoin for the particular scenario addressed by the researchers. Moreover, in other attack scenarios, Ethereum's BFT is even higher.

Slashing Penalties

There is another layer of security inherent in Ethereum's requirement that validators post stakes of 32 ether. Ethereum penalizes validators who violate protocol rules by docking their stakes, a process known as "slashing."[22] Slashing serves as both a punitive measure and a deterrent. Unlike PoW, which primarily relies on the high costs of equipment and electricity to discourage attacks, PoS integrates

---

[18] By contrast, Bitcoin's PoW system entrusts the entirety of block confirmation to the miner who successfully solves the cryptographic challenge. This system lacks Ethereum's additional measures, which include random selection of block proposers and an independent review by attesters. Consequently, Ethereum's approach to block validation distributes control and enhances security beyond what is inherent in Bitcoin's PoW validation process.

[19] *See* Lucas Nuzzi, Kyle Waters, & Matias Andrade, *Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum* at 3-4 (Feb. 15, 2024), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4727999.

[20] *Id.* at 26.

[21] *Id.* at 20-21.

[22] *See generally* Matthieu Saint Olive & Simran Jagdev, *Understanding Slashing in Ethereum Staking: Its Importance & Consequences*, Consensys, https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences (Feb. 7, 2024).

this upfront staking cost with the ongoing risk of financial penalty. Validators reduced below the 32 ether threshold by slashing are automatically removed from their validator role, reinforcing the network's integrity. PoW attackers retain their equipment and may repeatedly attempt to re-attack.

Increased Security Alongside Environmental Benefits

As explained above, there are several ways that Ethereum's PoS implementation results in increased security. This model comes with a further benefit which, although not directly relevant to the Commission's charge, deserves mention given its importance to society: Ethereum's PoS is vastly more energy efficient than Bitcoin's PoW. As of March 27, 2024, the annualized estimated energy consumption of the Bitcoin network is 170.04 *Tera*watt hours (TWh), while that of the Ethereum network is 5.53 *Giga*watt hours (GWh).[23] That is, Bitcoin's estimated annual energy consumption based on current rates is greater than Ethereum's by a factor of 30,000.

Ethereum's Decentralized Community

Number of Developers

Ethereum's resilience against attacks is significantly enhanced by its active and sizable developer community, which surpasses any other blockchain protocol in scale. In 2023, Ethereum was supported by 7,864 monthly active developers, significantly more than Bitcoin's 1,071.[24] This broad community serves as a first line of defense against software vulnerabilities, including bugs, that could otherwise compromise Ethereum's integrity.

Software Client Diversity

To participate in Ethereum's network, validators must run software that complies with the protocol specification. Validators have a choice of over ten independently developed open source software clients, with more in development.[25] The redundancy afforded by these independent clients—an important concept in network security—means that the network's integrity is maintained even if one software client fails due to a bug or malicious exploit.[26] For example, in May 2023, the Prysm software

---

[23] *See* Cambridge Blockchain Network Sustainability Index, Cambridge Center for Alternative Finance, https://ccaf.io/cbnsi/ (last visited Mar. 27, 2024).

[24] *See 2023 Crypto Developer Report*, Electric Capital, https://www.developerreport.com/developer-report (Jan. 17, 2024) at slides 73 & 83.

[25] *See Client Resources*, Clientdiversity.org, https://clientdiversity.org/ (last visited Mar. 28, 2024) (listing Ethereum clients).

[26] *See generally Client Diversity*, Ethereum.org, https://ethereum.org/en/developers/docs/nodes-and-clients/client-diversity/ (last modified Jan. 25, 2024).

client encountered a bug that caused finality issues on two consecutive days. Despite this, validators using other software clients carried on with processing and validating transactions, and the broader Ethereum network remained stable and operational.[27]

By contrast, Bitcoin node operators rely chiefly on a single client implementation, Bitcoin Core.[28] As researchers have shown, Bitcoin Core, like any other software, is not immune to bugs and has featured critical vulnerabilities that were fortunately patched before any material exploits.[29] Bitcoin's dependence on a single software client is a point of vulnerability; despite the fact that critical bugs in Bitcoin Core have been identified and rectified in time, the potential for unpatched vulnerabilities remains a risk. Such a single point of failure could be catastrophic if exploited, potentially compromising the network's integrity. This contrasts sharply with Ethereum's multi-client environment, which inherently distributes and minimizes such risks.

Ethereum's Transparency

Finally, Ethereum's inherent transparency forms a significant barrier to fraud and manipulation at the protocol level. All protocol development takes place in public on GitHub, and weekly development discussions are livestreamed on YouTube.[30] This commitment to openness facilitates not just preventative measures but also the swift detection of any irregularities, providing robust protection against fraud and manipulation. There are numerous readily-available blockchain analytic tools that, coupled with the blockchain's immutability, enable comprehensive monitoring of network activities. Through these tools, any anomalous activity that would undermine the blockchain ledger's validity can be rapidly identified and addressed, equipping the community to promptly counteract and contain potential threats.

* * *

---

[27] *See* Nishant Das et al., *Post-Mortem Report: Ethereum Mainnet Finality (05/11/2023)*, https://medium.com/offchainlabs/post-mortem-report-ethereum-mainnet-finality-05-11-2023-95e271dfd8b2 (May 17, 2023) (describing finalization failures due to Prysm bug and finding that "Client diversity helped the chain recover with some clients still being able to propose blocks and create attestations").

[28] For example, on March 28, 2024, of approximately 18,000 reachable Bitcoin nodes, 93% ran a version of Bitcoin Core client software (denoted in the User Agents dashboard by "Satoshi" and a version number), while only 7% ran different software (denoted by "Other"). *See Dashboard – User Agents*, Bitnodes, https://bitnodes.io/dashboard/ (last visited Mar. 28, 2024).

[29] *See, e.g.*, Braydon Fuller and Javed Khan, *Bitcoin Inventory Out-of-Memory Denial-of-Service Attack*, https://invdos.net/ (last visited Mar. 28, 2024).

[30] *See* Ethereum, Github Repository, (last visited Mar. 28, 2024); @ethereumprotocol, YouTube Channel, https://www.youtube.com/@EthereumProtocol (last visited Mar. 28, 2024).

In conclusion, Ethereum's PoS consensus mechanism, decentralized development community, and inherent network transparency establish a robust security framework that significantly reduces the risk of fraud and manipulation as compared with Bitcoin, a relevant benchmark given the Commission's approval of Bitcoin ETPs. There is no justifiable reason to deny the listing and trading of the Fidelity Ethereum Fund based on concerns over ether's susceptibility to fraud and manipulation. We urge the Commission to recognize the advanced safeguards inherent in Ethereum's design, which not only meet but exceed the exemplary security and resilience safeguards underlying Bitcoin-based ETPs that have previously been approved by the Commission. Ethereum's PoS implementation is not just a technological advancement over its prior PoW model, but also a testament to Ethereum's commitment to maintaining a secure, fair, and environmentally considerate blockchain ecosystem.

Sincerely,

Laura Brookover
Matt Corva
William C. Hughes

Consensys Software Inc.