

June 3, 2025

**BY ELECTRONIC SUBMISSION**

Commissioner Hester M. Peirce  
Crypto Task Force  
U.S. Securities and Exchange Commission  
100 F Street, NE  
Washington, D.C. 20549-0213

**Subject: Comments on the SEC Crypto Task Force's Questions Concerning Safe Harbor from Registration**

Dear Commissioner Peirce:

Hedera Hashgraph, LLC ("Hedera Council"), as the governing body for the Hedera network, is deeply invested in the development of clear and effective regulatory frameworks for digital assets. We are committed to fostering responsible innovation and believe that thoughtful regulation is essential for the maturation and adoption of distributed ledger technology, particularly within enterprise contexts where clarity and compliance are paramount.

We commend Commissioner Peirce and the SEC Crypto Task Force for proactively engaging with the industry and seeking public comment on the proposed token safe harbor framework. We share the objective of establishing a pathway that allows novel decentralized projects to develop and achieve network maturity while ensuring adequate transparency and protection for market participants. Such a framework is vital for continued technological advancement within the United States.

In that spirit, this letter provides the Hedera Council's perspective on several key questions raised in the request for information, specifically Questions 10 through 14. We offer these comments based on our experience operating a decentralized network governed by leading global organizations, hoping they contribute constructively to the refinement of the Safe Harbor Proposal.

**Question 10: Should the Commission consider a version of Rule 195, my proposed token safe harbor? Is the iteration on my proposed safe harbor known as "Safe Harbor X," or some other iteration, a better approach?**

Yes, the Commission should consider some form of a token safe harbor. A safe harbor is important to provide a pathway for new entrants to come to market without regulatory uncertainty, to provide certainty to existing companies within the industry, to bring transparency to the industry, and accordingly to provide reasonable protections to the market.

We suggest clarifying the language of proposed Rule 195<sup>1</sup> to provide greater clarity around both the decentralization and functionality avenues of the safe harbor. In making these suggestions, we have also considered the proposals and ideas of Andreesen Horowitz,<sup>2</sup> Gabriel Shapiro,<sup>3</sup> and the Decentralization Research Center,<sup>4</sup> among others.

As an initial matter, we believe all current proposals suffer from an unfortunate omission: they do not adequately contemplate decentralized governance activity that is coordinated through a legal structure of some kind. As the experience of DAOs in recent court cases has illustrated,<sup>5</sup> collective activity for economic benefit (however loosely tied to those of other participants) without a legal wrapper of any kind risks courts concluding that the activity is done pursuant to a general partnership.

Thus current proposals that include language such as “when the network is . . . [n]ot economically or operationally controlled and is not reasonably likely to be economically or operationally controlled or unilaterally changed by any **single person, entity**, or group of persons or entities under common control”<sup>6</sup> (emphasis added) may have the unintended consequence of prohibiting legal entity wrappers that can protect participants in otherwise decentralized activity. That is so because a court may conclude, based on language of this type, that even though the *wrapper* entity cannot by itself take any action, if decentralized activity is coordinated and finalized *through* the wrapping entity’s actions, a “single person [or entity]” has control. It would be unfortunate for courts to reach this conclusion, particularly as veteran attorneys in the space have for years now been recommending that decentralized activity be wrapped in a legal entity of *some* kind.<sup>7</sup>

We believe this oversight can be remedied by modifying the definition of *Network Maturity* in the SafeHarbor2.0 proposal as follows (changes shown in blue):

(k) Definitions.

---

<sup>1</sup> Hester Peirce, [SafeHarbor2.0](#) (Apr. 13, 2021).

<sup>2</sup> Miles Jennings et al., [Comments on the SEC Crypto Task Force’s Questions Concerning the Security Status of Crypto Assets](#) (Mar. 13, 2025).

<sup>3</sup> Gabriel J. Shapiro, [Token Safe Harbor Proposal 3.0](#) (Mar. 14, 2025).

<sup>4</sup> Decentralization Research Center, [Designing Policy for a Flourishing Blockchain Industry](#) (Feb. 2025).

<sup>5</sup> [Samuels v. Lido DAO](#), No. 23-cv-06492-VC, at \*8–14 (N.D. Cal. Nov. 18, 2024) (concluding plaintiff adequately alleged Lido DAO operated as a general partnership and that certain institutional investors were adequately alleged to be general partners); [Sarcuni v. bZx DAO](#), No. 22-cv-618-LAB-DEB, at \*12–17 (S.D. Cal. Mar. 27, 2023) (concluding plaintiffs adequately alleged founders and token holders of a DAO were general partners and potentially subject to liability); [CFTC v. Ooki DAO](#), No. 3:22-cv-05416-WHO, at \*10–11, 12–13 (N.D. Cal. Dec. 20, 2022) (concluding CFTC sufficiently alleged the defendant DAO was an unincorporated association capable of receiving service of process).

<sup>6</sup> SafeHarbor 2.0 at (k)(2)(i).

<sup>7</sup> See, e.g., Miles Jennings & David Kerr, *A Legal Framework for Decentralized Autonomous Organizations*, [a16zcrypto.com](#) (Oct. 26, 2021); Miles Jennings & David Kerr, *A Legal Framework for Decentralized Autonomous Organizations Part II: Entity Selection Framework*, [a16zcrypto.com](#) (June 2, 2022).

(2) *Network Maturity*. Network Maturity is the status of a decentralized or functional network that is achieved when the network is either:

(i) Not economically or operationally controlled and is not reasonably likely to be economically or operationally controlled or unilaterally changed by any single person, entity, or group of persons or entities under common control or a single ultimate beneficial owner, except that networks for which the Initial Development Team owns more than 20% of Tokens or owns more than 20% of the means of determining network consensus cannot satisfy this condition[.] For the purposes of this section, otherwise independent persons or entities participating in a decentralized governance system through a Decentralized Wrapper shall not be deemed to collectively constitute a single person, entity, or group of persons or entities under common control or a single ultimate beneficial owner, nor shall the Decentralized Wrapper constitute a single person, entity, or group of persons or entities under common control. All Tokens held by each member of the Initial Development Team shall be added together for purposes of determining whether the 20% threshold of this section has been exceeded.

...

(5) *Decentralized Wrapper*. A Decentralized Wrapper is a legal entity constituted for the sole purpose of coordinating decentralized governance activity among network participants, whereby:

(i) No person, either alone or as the ultimate beneficial owner, owns more than 20% of the ownership interests in such legal entity;

(ii) No person, either alone or as the ultimate beneficial owner, owns or has the right, including through proxies, to exercise more than 20% of the voting interests in such legal entity;

(iii) Such entity cannot act unilaterally to change the functioning, code, access to, or consensus mechanism of the underlying Network or Protocol, and all such changes must be made consistent with the pre-established Source Code published pursuant to (b)(1) through the entity's members, owners, or network participants.

(iv) The members or owners of such entities have no right to distributions from or the profits of such entities.

We believe this language protects an important mechanism for encouraging decentralized activity: giving participants the confidence that they will not have general liability for participating in that activity. As an enterprise-focused project, the Council has seen first hand that liability protection for participating in decentralized governance is essential for established businesses that should not be subjected to the unlimited liability of a de facto general partnership.

The language also proposes the concept of a “Decentralized Wrapper” entity, which must meet certain criteria to qualify: namely, that it exists only to coordinate decentralized governance, and that participation through a wrapper does not change the limits on control of the underlying network or its native token that the safe harbor imposes. A version of this idea was recently included in H.R. 3633, the Digital Asset Market Clarity Act of 2025.<sup>8</sup> We strongly support the adoption of a similar characterization to promote consistency and reinforce that decentralized governance systems include legal entities used to implement them. The proposed language also prohibits the entity itself from taking action other than through the persons or entities participating through it to change the underlying network or protocol, which must be done in ways that are consistent with previously published and open source code.<sup>9</sup>

Finally, such entities must not permit distributions or dividends to the entity’s “owners” or “members.” The reason for this restriction is that it ensures that participation in the entity is done without profit motive and is for the purpose of making autonomous networks and protocols freely available to the public. Any native token treasury, membership fees, or contributions to the entity itself would then be used for coordinating governance activity or put towards work on the underlying network or protocol. This model of coordinating development has seen considerable success in the open source software community (e.g., the Linux Foundation) and in the development of the Internet itself (e.g., Internet Engineering Task Force, World Wide Web Consortium, Internet Corporation for Assigned Names and Numbers), either through explicitly non-profit legal entities or ones that are effectively so. These models work for public goods technology development, and importing these open governance concepts to crypto provides a known and accessible framework through which to develop open, public digital resources like blockchains and protocols built on top of them.

We also believe this approach encourages progressive decentralization, an important tool for allowing new entrants to come to market under the safe harbor without requiring the level of decentralization currently achieved by the largest networks. Decentralization is a good way of addressing concerns about control, but sometimes too much decentralization too fast can lead to security risks and unintended consequences that could harm the investors the SEC is charged with protecting. For example, proof of work networks like Bitcoin can be manipulated when malicious actors control a majority (greater than 50%) of the computing power. Similarly,

---

<sup>8</sup> See French Hill, *Chairman Hill Unveils Bipartisan Digital Asset Market Structure Legislation*, [House.gov](https://www.house.gov/legislation/record/frchill) (May 29, 2025); H.R. 3633, the Digital Asset Market Clarity Act of 2025 at §§ 101 (adding a new definition to the Securities Act of 1933 for Decentralized Governance System that notes that “[t]he term ‘decentralized governance system’ shall include a legal entity used to implement the rules-based system described in subparagraph (A) . . .”), 205 (adding a new section 42 to the Securities Exchange Act of 1934 criteria for Mature Blockchain Systems that clarifies that “[f]or purposes of this section, a decentralized governance system is not a ‘person’ or a ‘group of persons under common control’.”), available at [https://financialservices.house.gov/uploadedfiles/052925\\_clarity\\_act.pdf](https://financialservices.house.gov/uploadedfiles/052925_clarity_act.pdf) (PDF pages 6, 102).

<sup>9</sup> We note that many crypto industry participants mistakenly state that code is “open source” merely because it is publicly available online. However, *open source* is a term of art meaning that the code is not just publicly available but available to be freely used by others, usually through an Apache 2.0 or MIT license. For more information, see *The Open Source Definition*, [Open Source Initiative](https://opensource.org/licenses/OSD) (Feb. 16, 2024). We encourage the commission to require open source code for safe harbor applicability.

proof of stake networks can be vulnerable to attacks when a significant portion of the network's stake is controlled by malicious actors, though the specific threshold varies depending on the consensus mechanism. On small networks that are just at the beginning of their lifecycle, requiring control to be distributed too widely too early risks undermining a fundamental security mechanism of blockchain networks. Thus, having reasonable, but not insurmountable requirements in place to qualify for the safe harbor makes sense — but we agree such requirements should encourage continuing efforts toward meaningful decentralization by permitting “lighter-touch disclosure obligations, fewer selling restrictions, and greater access to secondary markets where projects broadly disseminate ownership and control.”<sup>10</sup>

Specifically setting forth requirements of a Decentralized Wrapper that encourages dissemination of ownership and control not only encourages progressive decentralization, but also empowers blockchains and protocols to integrate in easily understandable ways for other parts of the economy, empowering decentralized initiatives with a clear path to hiring consultants, employees, attorneys, and opening bank accounts. This is a win-win solution that encourages the benefits of decentralization while bringing crypto projects responsibly into the broader economy.

**Question 11: Should the safe harbor be available retroactively for projects that comply with the disclosure requirements?**

Yes. We believe that making the safe harbor available retroactively, contingent upon full compliance with its stipulated disclosure requirements, offers significant benefits for market transparency and investor protection within the digital asset space. Indeed, such an approach would properly incentivize robust disclosure practices while reducing information asymmetry by requiring standardized information for public use.

**Encouraging Disclosure.** The digital asset industry is rapidly evolving, and establishing norms for comprehensive and reliable disclosure is paramount for building market integrity and trust. Offering retroactive availability of the safe harbor provides a powerful incentive for the many projects that have already launched. This retroactive incentive can significantly accelerate the transition towards greater transparency across the existing market, rather than only applying standards to future projects.

**Fostering Standardized Information.** Equally important is ensuring the quality and consistency of that disclosure. A key challenge for anyone in the digital asset market is the difficulty in comparing different projects due to disparate, incomplete, or non-standardized information. A standardized disclosure requirement could rectify this problem for huge swaths of the market very quickly by allowing potential token purchasers and market participants to make meaningful, "apples-to-apples" comparisons regarding tokenomics, governance, technology, risks, and team background across different projects.

---

<sup>10</sup> See Miles Jennings, *Why decentralization matters, and needs incentives*, [a16zcrypto.com](https://a16zcrypto.com) (Feb. 3, 2025) (“Decentralization isn’t a light switch that can be flipped on or off; it is a process, which takes place in steps.”).

**Question 12: If a safe harbor of some form is the right approach, what disclosure requirements would be feasible for early-stage projects to provide to token purchasers the material information regarding the blockchain project, crypto assets, and development team? What information should be required to be updated on an ongoing basis, and how should that information be provided?**

We believe that the disclosures currently listed in Rule 195 provide a good framework of disclosure requirements for initial development teams and also establish certain minimum functional requirements for the project (like requiring a live block explorer). We also applaud that the Rule permits disclosure through a public website, rather than requiring forms or submissions, which ensures the public has access to the latest information in a comprehensively updated format.

Although Rule 195 currently requires only semiannual reporting, given the pace of change in the crypto industry, we believe such information should be updated on at least a quarterly basis initially, perhaps moving to a monthly basis as the project matures or is prepared to file its exit report.

We would also offer the following suggestions to provide additional relevant detail to the market:

- (b)(1)(i): *Source Code*: For projects relying on decentralization to reach Network Maturity, require that the code be subject to an open source license agreement approved by the [Open Source Initiative](#), and disclose which license the project has chosen, with a live link demonstrating the applicable license has been applied to the relevant code.
- (b)(1)(ii): *Transaction History*: Require the link to the block explorer (or equivalent) and sufficient information for a third party to create their own tool for exploring transaction history in this section, and remove it from the *Token Economics* section.
- (b)(1)(iii): *Token Economics*: Because dynamics of tokenomics can change based on what's happening in the market, we suggest requiring updated disclosures about tokenomics on a regular basis (e.g., monthly) while the project is subject to the safe harbor. This ensures the public has the latest information about the project's current treasury, how it is allocated, and how its planned allocation or release schedule has changed. This can be particularly pertinent to projects that are pursuing progressive decentralization and turning over decisionmaking and control beyond the founding team, who may ultimately steer the project in directions that were not foreseeable to the founding team.
- (b)(1)(iv): *Plan of Development*: We suggest permitting greater flexibility in this provision to clarify that development plans are not binding on the project,

provided that material changes to the plans are timely disclosed. We recommend this approach because it is difficult to predict the rate of development for nascent technology projects, and while many founders are well-intentioned and aggressive in their projections, the real timeline proves slower than anticipated. Subjecting these projects and founders to potential fraud claims would be unfortunate.

- (b)(1)(vi): *Initial Development Team and Certain Token Holders*: Given the relatively high turnover of employees in startups, we suggest, consistent with Gabriel Shapiro,<sup>11</sup> that the public disclosure of the initial development team be limited to those individuals “who directly or indirectly beneficially owns or has the right to receive or control 1% or more of the total maximum possible supply” of the project’s tokens, or who has 1% or more of the voting interests necessary to make changes to the network or protocol.
- (b)(1)(viii): *Sales of Tokens by Initial Development Team*: We suggest including a time requirement for disclosure of insider sales of 2 business days after the sales occur to ensure the market has reasonable access to this information and to provide consistency with existing requirements imposed by Sarbanes-Oxley.
  - We also suggest an exception to any filing or updated disclosure requirement if the Initial Development Team discloses their crypto wallet addresses holding the relevant Tokens, provided that activity in those wallet addresses is publicly visible through a readily accessible block explorer, and that a presumption applies that transfers to known crypto exchanges would be assumed to be sales on that day. This exception could reduce the compliance burden on founding teams while still ensuring the same information is publicly accessible.

**Question 13: At the expiration of the safe harbor as envisioned, if the network were sufficiently decentralized or functional, registration of the tokens would not be required. If decentralization is used as an indicator of network maturity, should the Commission define objective quantitative thresholds (such as percentage thresholds for ownership and control) to provide greater clarity for issuers, developers, or minters of tokens regarding whether their networks and protocols are sufficiently decentralized and to allow third parties to verify decentralization?**

Yes, objective thresholds should be established. We propose those thresholds be consistent with the criteria set forth in our proposal for a Decentralized Wrapper set forth in response to Question 10 above, namely that no single person or entity (either alone or as the ultimate beneficial owner) owns or controls greater than 20% of any aspect of the network or protocol, whether that be of tokens, nodes, validators, voting rights, or ability to change the code running on the network or protocol.

---

<sup>11</sup> Gabriel J. Shapiro, [Token Safe Harbor Proposal 3.0](#), at \*6 (Mar. 14, 2025).

**A. Is dispersion of control a better framework than decentralization? If so, how should ownership of governance tokens and voting rights be considered in assessing dispersion of control? How should the delegation of voting rights be taken into account?**

Control is a more intuitive way to understand the risk decentralization is designed to address, however, we do not see these as mutually exclusive subjects. Whether something is “decentralized” or not is really the same question as whether control has been dispersed among some threshold number of genuinely independent actors. We therefore believe thinking about the concepts of control and decentralization together is the best method.

Control should be addressed at both the technical and legal levels to propel “sufficient decentralization” that actually addresses the risk of single point failures: from where nodes/validators are hosted, to who owns particular entities, tokens, and voting rights. On the technical level, control should be considered not just from an ownership level (e.g., ABC Corp owns node 1, DEF Corp owns node 2, etc.) but also on if there is a single technical method of control that would allow a small minority of entities to exert coercive power over a network or protocol. For example, if ownership of nodes is dispersed across 100 entities, but all 100 nodes are hosted in AWS, a single entity still has a way to shut down the blockchain network or protocol or otherwise exert undue influence. Requiring dispersion of technical control to achieve network maturity will incentivize meaningful decentralization that will better protect individuals buying digital assets. We encourage the Commission to carefully consider requiring multiple layers of dispersion of control that address the distinctions between practical, legal, and technical control over blockchain networks and protocols.

Regarding tokens and/or voting rights (to the extent they are separate), we believe the Rule’s language must focus on the ultimate beneficial owners to provide meaningful dispersion of control, and therefore decentralization of power. By doing so, the Rule will prevent gamesmanship in which a holding company could create many subsidiaries that it controls, but could appear to be independent entities to an unwitting public. Invalidating eligibility for the Safe Harbor by focusing on ultimate beneficial owners would prevent this sort of gamesmanship or “decentralization theater.”

**B. If an exit marker is achieved, who should be responsible for notifying the Commission?**

Because the Initial Development Team is composed of a set of individuals who may or may not continue to work on the project by the time an exit marker is achieved or it is time to file an exit report, we believe greater flexibility for filing an Exit Report is necessary than the proposed Rule currently provides. We suggest permitting any of the following:

- Initial Development Team;
- The legal entity through which the project was originally developed or the applicable Token was issued; or

- Any entity willing to certify under penalty of perjury and assume the consequences for violating the securities laws. This approach would be consistent with the one taken in the European Union under the Markets in Crypto Assets Regulation.

**Question 14: How should the decentralization of a deployed protocol best be evaluated? How should permissioned aspects of crypto-adjacent software or participant roles, such as validators, relayers, and sequencers, be considered? Are there tech-neutral thresholds that can be agreed upon for determining thresholds for decentralization?**

The Hedera Council is broadly supportive of the decentralization criteria set forth in the Digital Market Asset Clarity Act of 2025. We believe that additional nuance is appropriate regarding the distinction between permissioned and permissionless nodes on a layer-1 blockchain network and how the ability to participate in the infrastructure of a network should affect the evaluation of a network's decentralization.<sup>12</sup>

Permissionless nodes are frequently seen as a key indicator of decentralization, based on the idea that allowing anyone to operate a node removes the risk of centralized control. However, as mentioned above, this assessment often fails to fully examine the entire technology stack, such as whether the infrastructure (e.g. hardware and network resources) that validators rely on might be geographically concentrated or rely heavily on individual service providers, or whether such an approach permits well-funded but malicious actors an attack vector that is difficult to defend against by nascent projects.

For example, as things stand today, financial institutions run the risk of being in breach of the law when using permissionless blockchains, as some nodes might be geographically concentrated in sanctioned jurisdictions. Too many nodes being operated out of one single jurisdiction also raises important cybersecurity, geopolitical and financial stability considerations, as critical public infrastructure is vulnerable to a specific jurisdiction's laws, providers and infrastructure. Similarly, from an operational resilience standpoint, a large percentage of nodes relying on one single cloud service provider represent a single point of failure, as all it takes is one company (e.g. Amazon Web Services) to take the network down or severely slow down its operations.

For the above reasons, the Basel Committee on Banking Standards (BCBS) recently [articulated](#) the importance of simultaneously upholding the principles of 'node diversity' and 'node trustworthiness.' A legal wrapper coordinating the activities of public institutions with a reputation to uphold, which are geographically distributed and trustworthy, helps uphold both principles. It provides greater transparency in relation to any potential concentration of risks.

Accordingly, we recommend that the Commission not establish a default assumption that a network with permissioned nodes equates to a lack of decentralization. Rather, the

---

<sup>12</sup> Our comments are directed only to the infrastructure of layer-1 blockchain networks.

Commission should establish criteria to evaluate a network or protocol's nodes holistically, whether they be permissioned or permissionless. Namely, we believe the Commission should consider:

- (a) How new nodes are added to the network. Permissionless may indicate decentralization or a lack of control, but if the network is of a small size, this may indicate a substantial risk of takeover by coordinated, malicious actors. Conversely, permissioned nodes may suggest control, but if permission is granted not by a single entity but through a decentralized governance system (in the words of H.R. 3633, the Digital Market Asset Clarity Act of 2025), that should be indicative of decentralization.
- (b) How dispersed is node ownership/control. We encourage the Commission to set criteria that evaluates networks and protocols based on how dispersed node ownership and control is among network participants. For example, a permissionless network might have a substantial majority of nodes controlled by a single actor or small group, while a permissioned network might require each new node be owned and controlled by independent entities. Because of the central role nodes play in networks, looking beyond permissionless/permissioned distinctions to see how concentrated ownership (and therefore control) of nodes is will give meaningful insight into the extent to which a network or protocol has achieved functional decentralization.
- (c) How nodes are dispersed geographically. Nodes heavily concentrated in a single or very small geographic area could indicate risks of political control or natural disasters that could severely impact network or protocol operations. Nodes widely dispersed would indicate operational resilience and decentralization.
- (d) Where nodes are operated. A network or protocol with nodes heavily concentrated on a single cloud provider could indicate a latent risk of control by a single actor, whereas nodes that are spread across cloud providers or bare metal infrastructure providers would indicate resilience against latent single actor control.

Evaluation of these practical criteria as it relates to network or protocol nodes would reveal the true extent to which nodes contribute to decentralization, rather than reliance on the shorthand of "permissioned" versus "permissionless," which may obfuscate, rather than clarify, the extent to which control is concentrated in single actors or small groups.

## Conclusion

In conclusion, the Hedera Council appreciates the opportunity to provide commentary on the proposed token safe harbor framework. We strongly support the establishment of a safe harbor that accommodates the use of legal entities through which decentralized governance can be performed. We believe that objective, quantitative thresholds are crucial for determining network maturity and that a nuanced evaluation of decentralization, considering dispersion of control at technical, legal, and practical levels – including a holistic assessment of both permissioned and permissionless node operations – will best serve the goals of innovation and investor protection. The Hedera Council remains committed to collaborating with the Commission to develop a regulatory environment that supports the responsible growth of distributed ledger technology in the United States.

Sincerely,



Nilmini Rubin, Chief Policy Officer  
Hedera Hashgraph, LLC



Gregory Schneider, General Counsel  
Hedera Hashgraph, LLC