DeFi Education Fund

April 18, 2025

Via E-Mail: crypto@sec.gov

Crypto Task Force
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-0213

Re: Token Safe Harbor Guiding Principles

SEC Crypto Task Force:

The DeFi Education Fund commends the U.S. Securities and Exchange Commission (the "**SEC**" or "**Commission**") for launching its Crypto Task Force, dedicated to creating a comprehensive and clear regulatory framework for crypto assets. We appreciate the leadership of Acting Chairman Mark Uyeda and Commissioner Hester Peirce in this area, and we agree wholeheartedly with Commissioner Peirce's stated enthusiasm for developing a "regulatory environment that protects investors, facilitates capital formation, fosters market integrity, and supports innovation."[1] We look forward to working with Chairman Paul Atkins on these topics in the near future.

The DeFi Education Fund is a nonpartisan, nonprofit research and advocacy organization. Its mission is to advocate for sound policy for decentralized finance ("**DeFi**"), educate lawmakers and regulators about the technical workings and benefits of DeFi, and represent the interests of users and developers in the DeFi space.

Commissioner Peirce previously proposed that the Commission consider putting in place a non-exclusive safe harbor that would provide a time-limited exemption from the registration requirements under the Securities Act of 1933 for offers and sales of tokens during the development of a decentralized network (a "**Safe Harbor**").[2] We support this concept. A thoughtfully calibrated Safe Harbor—appropriately tailored to the realities, risks, and opportunities of digital assets and blockchain technologies—will provide important information to investors, eliminate information asymmetries, and protect investors, token holders, builders, and projects operating in this space while the long-term legislative and regulatory policymaking processes play out. To that end, while we wholeheartedly support the goals of this Safe Harbor, we strongly recommend that the Commission defer broader market structure and jurisdictional issues to Congress. It is

---

1 U.S. Securities and Exchange Commission, *SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of new Crypto Task Force* (Jan. 21, 2025), https://www.sec.gov/newsroom/press-releases/2025-30.

2 Commissioner Hester M. Peirce, *Token Safe Harbor Proposal 2.0* (Apr. 13, 2021), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-token-safe-harbor-proposal-20.

our view that for token holders, developers and users in the DeFi space to thrive, they need durable clarity: long-term legal regulatory certainty that only legislation can provide. While creating this Safe Harbor in the interim and requiring participants to conduct information disclosures will advance the Commission's goals and the public interest, we would also ask the Commission to encourage Congress to pass a comprehensive regulatory framework for digital assets.

We submit five guiding principles for your consideration, which we believe would help shape the development of Commissioner Peirce's proposal while also protecting the future of the DeFi industry. As described in further detail below, these principles are: (1) technology-agnostic rules and policies, (2) broad and inclusive eligibility criteria for the Safe Harbor, (3) appropriately calibrated disclosure and compliance considerations, (4) clear and well-defined exit criteria, and (5) appropriate treatment of secondary market activity.

Five Core Principles for Establishing an Effective Safe Harbor

1. Principle #1. Technology-Agnostic Approach

As a foundational principle, the Commission's rules and policies should be agnostic as to the underlying technology of the assets to which they apply while still being adaptable, focusing on substance over form and on the associated risks of activities rather than the specific technologies employed. In other words, fit-for-purpose regulations should be tailored to the realities of blockchain technology and acknowledge its value proposition, and should protect innovation and the unaffiliated network of participants who develop or operate the technology. This also means ensuring policies avoid entrenching particular technological models or favoring particular solutions, and instead allow for the technology to continue to evolve.

Given the vital role that the SEC plays in the U.S. economy and the fact that securities markets are constantly evolving due to ongoing innovation, the Commission must be wary of mandating specific, prescriptive requirements or formats that are unsuitable for new or emerging technologies. Instead, the Commission must establish principles-based regulatory standards focused on the core underlying risks—standards that could be met even where new or evolving technologies are involved. This is especially relevant with respect to digital assets and DeFi, so that the Commission can fulfill its mission without stifling innovation in this burgeoning asset class and industry. As the Commission has already seen with respect to digital assets, shoehorning fundamentally different types of activities into prescriptive traditional stock market regulatory frameworks will not only stymie innovation, but also leave regulatory gaps. Additionally, it does not work to impose regulatory obligations on the technology itself (as opposed to humans who actually bear the compliance burden). Software cannot comply with regulation.

With this context in mind, it is paramount that the SEC not pick winners and losers: that the Safe Harbor and its eligibility criteria remain agnostic with respect to the merits of the underlying technology relevant to digital assets, and that any regulations be sufficiently flexible to avoid technology- or function-specific standards or conditions. The Safe Harbor should not create incentives for the development of certain technologies or privilege certain solutions over others (*e.g.*, in the context of consensus mechanisms, the Commission should not create regulations that privilege proof of stake or proof of work). The SEC's primary focus should remain on information disclosure and addressing information asymmetries, while remaining agnostic as to whether the asset is blockchain-native or not, thereby preserving its merit and neutrality. If the SEC were to do otherwise, the Commission could cut off important innovations or improvements to investors and the markets, such as blockchain scaling solutions and decentralized protocols. A technology-agnostic approach should be at the foundation of any Safe Harbor.

2. Principle #2. Eligibility and Entrance

While the eligibility criteria for the Safe Harbor should be broad enough to accommodate a wide range of technologies and projects, it should also be limited to those projects (1) intending to decentralize and (2) capable of meeting the Exit Test described below. Since this Safe Harbor is meant to incentivize projects on the path to decentralization, those applying or registering to enter the Safe Harbor should submit good faith plans to decentralize and evidence that they are designing a project that is capable of fully decentralizing in the future. This means projects would have to provide sufficient information for the Commission to evaluate the project's compliance with the requirements imposed by the Safe Harbor.

The Safe Harbor should also focus on the facts and circumstances of a token as it exists at the time of entry to the Safe Harbor and not at genesis, which means there should be pathways for previously distributed tokens to become eligible for the Safe Harbor. Transition assistance is especially vital to existing projects that were launched in the past. These projects should have an opportunity to enter the Safe Harbor, assuming they meet the eligibility criteria, and should not be penalized by virtue of being launched before the Commission developed a sensible regulatory approach in this area.

When making an initial determination of whether a project may enter the Safe Harbor, the Commission should ensure the framework is not so narrow that it applies only to a small or select group of tokens, which may stifle the very innovation that the Safe Harbor aims to advance. If the Commission determines a project is capable of meeting the Exit Test described below, the project should be given the chance to develop while making information disclosures along the way.

3. Principle #3. Disclosures and Other Compliance Considerations

Any information disclosure requirements associated with the Safe Harbor should be carefully calibrated: they should provide the specific type of information that is material to prospective or existing token holders' evaluation of the token and underlying technology, while being commercially feasible for initial development teams to provide. In this vein, relevant disclosures could potentially include, as proposed in Commissioner Peirce's Token Safe Harbor Proposal 2.0: source code and bytecode transparency, transaction history, token economics, plan of development, history of code audits, secondary trading platforms solicited by the initial development team, initial development team members, sales of tokens by the initial development team, and related-party transactions.[3]

Additional disclosure obligations may be warranted when a person or entity retains control over a network or its associated assets, or where a limited group is responsible for development and maintenance. The categories of information outlined below would help token holders adequately assess such risks.

- Team and Control Disclosures: Identities and roles of the project's executives, directors, key contributors, and third-party affiliates responsible for ongoing development.

- Plan of Development: Project roadmap, decentralization plan, current status, anticipated timeline to network maturity, funding needs, use of assets, token distribution strategy, how tokens are minted and whether minting contract is upgradable or privileged minting functions exist within the contract, known risks, and post-launch activities.

- Conflicts of Interest: Known conflicts of interest, related party transactions and key agreements supporting token or network development.

- Token Allocations: Allocations held by the issuer, team,[4] insiders, and related persons relevant to ongoing development.

- Code and Cybersecurity: Source code and bytecode, permission structures, history of security incidents, and results of third-party audits.

- Governance: Network and smart contract governance mechanisms and control permissions.

---

[3] *See generally* Commissioner Hester M. Peirce, *Token Safe Harbor Proposal 2.0* (Apr. 13, 2021), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-token-safe-harbor-proposal-20.

[4] The Commission should consider allowing disclosures on team allocation to be categorical rather than on an individual basis so as to ensure the privacy and security of individual employees.

- Tokenomics: Token supply, pricing, lockups, distribution methods, treasury/foundation holdings, prior sales, unlock schedules, issuance model (fixed/variable, inflationary/deflationary), consensus mechanism, burn functions, economic design, and data enabling independent verification of token transaction history.

The frequency of disclosure obligations should also be appropriately calibrated, and the Commission should make best efforts to simplify disclosure filing such as providing opportunities for Application Programming Interface connectivity. For example, it would be logical to condition the Safe Harbor on ongoing periodic disclosures until the end of the Safe Harbor period. Ongoing disclosure requirements could include updates on the state and timeline for the development of the network to show how and when the initial development team intends to satisfy the Exit Test criteria. To the extent it is possible to automate disclosures via the relevant blockchain, such automated disclosures could continue beyond the Safe Harbor period.

Any other compliance requirements, conditions, or restrictions associated with the use of the Safe Harbor, such as lock up periods or disclosure requirements for project insiders, should likewise be tailored to reflect the realities of digital assets. The purpose of imposing some form of a lock up period or disclosure requirement would be to add additional incentives for projects to continue along the path to decentralization while protecting the retail public. Once the token satisfies the Exit Test criteria and the project developers have given up control, there will be no information asymmetries between project insiders and the retail public, obviating the need for insider lock ups or continuing disclosure requirements.

4. Principle #4. Safe Harbor Exit Test

The Safe Harbor should clearly define the criteria that a project must meet in order to fully transition out of the Commission's jurisdiction and no longer be considered a "security"—*i.e.*, an "Exit Test." Critically, since this Safe Harbor should be designed for projects intending to decentralize control,[5] the Exit Test should include the principles outlined below. However, and as described in further detail below, the Commission should allow projects in which developers maintain control to stay in the Safe Harbor for an extended period of time, so long as they continue to demonstrate verifiable efforts to decentralize and reliably make information disclosures.

[5] It may be appropriate for the Commission to consider other amendments or new rules to address digital assets that are subject to ongoing control, such as tokenized offchain securities or crypto-native digital securities. However, the Commission should focus the Safe Harbor solely on assets that are intended to be decentralized, and address any other necessary regulatory changes through separate efforts.

Exit Test Criteria

- Maximum Transparency: The deployed instance of the code is publicly available and auditable, the network's functionality is clearly described and publicly disclosed, any existing permissions—such as the ability to run, modify, or redistribute the source code, upgrade the protocol, or delegate powers to others—are clearly described and publicly disclosed, and any known insiders who retain significant ownership stakes in the network are identified.

- Permissionless: No person or group of persons under common control[6] has the ability to unilaterally exclude, block, or approve persons or entities from (i) using or modifying the network, (ii) participating in consensus mechanisms, (iii) building software that provides access to the network, or (iv) otherwise interacting with the network, its underlying technology, or the associated digital asset.

- Non-Custodial: Users of the network retain custody, possession, and control over their digital assets. No person or group of persons under common control maintains custody over third-party assets without consent. Put differently, no person or group of persons has the unilateral legal authority or technical ability to initiate transactions involving digital assets without the approval, consent, or direction of the asset holder or an authorized third party.

- No Centralized Network Control: No person or group of persons under common control should be able to unilaterally modify the network unless that authority has been delegated by an unaffiliated, dispersed group of token holders or validators within the consensus mechanism, which shall retain the ultimate authority to revoke such delegation.[7] If an initial development team, or any person, entity or

---

[6] We included the term "group of persons under common control" throughout this list to describe the type of centralization that should bar a token from exiting the Safe Harbor. The principle underlying this term is that the risks traditionally addressed by the securities laws are only mitigated when token holders no longer depend on privileged parties with greater powers or superior access to information. Including only "person" would continue to expose token holders to those risks, since a group of persons coordinating privately may have privileges comparable to those of a single person. However, "common control" may also inadequately describe the type of centralized group that may create such risks, since two persons with no mutual beneficial owners may still have unequal rights or powers compared to token holders. Another term often used is "group of persons acting in concert," but that term may have the opposite issue, capturing broadly dispersed, unaffiliated groups that have no capability to take advantage of token holders. The Commission should be careful to select language, or provide guidance, that achieves the intended end result: no centralized group of people or entities should be able to unilaterally and autonomously effect the kinds of decisions or changes described in this list.

[7] DEF intends to submit an additional letter to the Commission discussing the proper treatment of Decentralized Autonomous Organizations in the near future.

group of related persons under common control, has unilateral authority to restrict or prohibit others from using, earning, or transmitting the token, deploying software that uses or integrates with the technology, or participating in governance of the technology, then they would be deemed to have control, and the Exit Test would not be satisfied.[8] The Commission should ensure that "network control" is defined in a way that permits restrictions that are non-discriminatory, transparent, and do not impose unreasonable barriers to participation, so long as they do not conflict with the other principles included here.

- Fully Automated Transactions: The network operates continuously without human intervention and functions according to transparent, pre-established rules encoded in its source code. Transactions are executed, validated, and enforced automatically without human intervention.

- No Retained Economic Authority: The economics of the network may be modified but are not dependent on any person or group of persons under common control. No changes to economic drivers are possible unless such authority and ability has been delegated by an unaffiliated and dispersed group of token holders or validators within the consensus mechanism.

Ultimately, the Exit Test should be principles based and flexible so as to account for new technologies and unique structures, and should not inadvertently discourage continued benefits to investors and ecosystems. A successful safe harbor regime would allow for a fair, orderly, and efficient decentralization process to occur. Ongoing efforts to maintain or develop a system—when made without centralized control—do not create information asymmetries and trust dependencies that would normally implicate the need for securities regulation, and should not serve as a basis for failing the Exit Test. Further, it is in the token holders' interest for these efforts to continue, and the initial development team should not be penalized for contributing to projects on which they are knowledgeable and valuable members of the broader community.

It will be important for the Commission to craft a reasonable timeframe within which projects can meet the exit criteria. The Exit Test should be applied only after a period that reflects the practical development timelines and challenges of decentralized systems, ensuring projects acting in good faith have a fair opportunity to achieve compliance. From informal polling of the DeFi ecosystem, we believe that a reasonable timeframe would be three to four years.

Clarity regarding the status of the token once it satisfies the Exit Test will be a necessary part of any guidance. For example, it seems prudent for a project to make a final required disclosure when the token exits the Safe Harbor, so that holders understand

[8] Note, however, that technical restrictions and prohibitions exist in many decentralized system designs (*e.g.*, for security and stability of the network), and the presence of certain restrictions should not pose a barrier to passing the exit test.

that the token itself should not be considered a security and will not be subject to ongoing disclosure or other regulatory requirements that apply to securities transactions or to securities market participants. Furthermore, after a successful exit, there should be clarity regarding who has and does not have any further obligations or responsibilities under the SEC's rules (*e.g.*, initial development team no longer potentially viewed as an issuer or control person). Clearly defining this release from obligations and liability will ensure regulatory certainty and provide a strong incentive for decentralization.

In order to gather the necessary information to assess whether a token satisfies the Exit Test, the Commission should require submission of an exit report at or prior to the conclusion of the Safe Harbor period. The Commission should allow for different options for who can submit the report. For example, in the case of a project that has met the Exit Test, an unaffiliated party could submit the exit report or the report could be voted on and paid for through governance action, empowering individuals or a group to generate and submit the proper documentation without having to be recognized as an official spokesperson of the project. The Commission should work with the industry to identify the criteria that would need to be addressed or certified, such as examples of decentralized governance and development, quantitative measurements of decentralization, and confirmation that the initial development team has no material non-public information about the network.

The Commission should consider a phased approach that allows flexibility based on demonstrable progress, along with defined extension opportunities tied to good faith efforts, pre-established milestones, and additional disclosures. As described below, the Commission should allow projects who have not yet met the Exit Test to extend the Safe Harbor period, subject to certain conditions.

Extended Safe Harbor

Given the reality that some projects may need or want additional time to satisfy the Exit Test, the Commission should consider allowing projects to apply for an Extended Safe Harbor. This would allow developers planning to give up control and making demonstrable efforts to do so more time to meet the Exit Test criteria safely and reliably, while also protecting the public from a scenario in which projects hasten to exit before they are ready. For as long as the project remains within the Safe Harbor framework, the project would be required to provide evidence of continued efforts to decentralize and make periodic information disclosures. The Commission could consider extending lock-ups, disclosure requirements, and other compliance obligations that applied during the original Safe Harbor period.

Finally, for tokens that do not satisfy the exit criteria by the end of the Safe Harbor period, or even the Extended Safe Harbor, the Commission should ensure there is a clear and reasonable pathway and timeframe for compliance with securities laws or wind down of the project, as well as an opportunity to apply for exemptive relief.

5. Principle #5. Secondary Markets

While a token remains in the Safe Harbor, protections should extend to secondary market transactions. Exemptions should apply to market infrastructure providers and intermediaries that support activity involving tokens covered by the Safe Harbor. Digital asset trading platforms, market makers, and other intermediaries should not be required to register as broker-dealers or securities exchanges if all tokens they support are covered by the Safe Harbor or otherwise deemed non-securities.

The Safe Harbor should explicitly exclude market infrastructure providers and intermediaries that support secondary transactions from entity registration statuses that apply in the context of the sale of stocks, bonds, and other traditional securities, including registration requirements applicable to securities brokers, dealers, exchanges, transfer agents, investment advisers, and clearing agencies. Past SEC enforcement actions demonstrate the risk that decentralized protocols and those that facilitate or participate in economic activity associated with decentralized protocols may face without regulatory clarity.

* * *

Again, we commend the Commission for forming the Crypto Task Force. We hope that the views expressed in this letter will help advance the Crypto Task Force's work. We will publish this letter on our website and solicit feedback on its content from the community, and would be happy to provide the Commission with additional feedback we receive. We intend to remain active participants in the ongoing policy discussions over the coming weeks and months, and we would be pleased to answer any questions that you may have.

Respectfully submitted,

Amanda Tuminelli
Executive Director & Chief Legal Officer
DeFi Education Fund