

March 13, 2025

VIA EMAIL

Crypto Task Force Chairman and Commissioner Hester M. Peirce
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549-0213

**Re: Recommendations Regarding a Safe Harbor for Certain Airdrops and
Incentive-Based Rewards of Network Tokens**

Dear Crypto Task Force Chairman and Commissioner Peirce:

Andreessen Horowitz (“a16z” or “we”) appreciates the opportunity to provide recommendations regarding the circumstances under which certain public distributions of crypto assets¹—airdrops and incentive-based rewards of network tokens (as defined below)—should be excluded from federal securities laws. We welcome opportunities to meet with Securities and Exchange Commission (“SEC” or “Commission”) staff, answer any questions that the Commission may have, and discuss our comments below in more detail.

We recognize that federal securities laws do not extend to crypto assets that do not constitute securities under the Securities Act of 1933 or transactions of crypto assets that are not otherwise subject to federal securities laws. As a result, federal securities laws already do not apply to many airdrops and incentive-based rewards of crypto assets. However, such determination is subjective and difficult for entrepreneurs, slowing the pace of innovation without providing investor protections. The purpose of this submission is to create clear rules by providing clear criteria for circumstances under which airdrops and incentive-based reward distributions should be excluded from securities laws because they do not give rise to the risks federal securities laws are intended to address. In such cases, Section 5 registration is unwarranted and inappropriate.

This approach is therefore intended to establish limits with respect to the application of federal securities laws to airdrops and incentive-based rewards programs to safeguard them from becoming subject to retroactive application of federal securities laws by regulators. Not all airdrops and distributions of incentive-based rewards will be able to avail themselves of this safe harbor. On the contrary, *only* those airdrops and incentive-based reward programs which *do not* engender the risks that Section 5 was designed to address should be eligible. If effectively crafted, this approach would help fulfill the Commission’s mandate of protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation, while also promoting responsible innovation in blockchain technology.

A16z is a venture capital firm that invests in seed, venture, and late-stage technology companies, focused on bio and healthcare, consumer, crypto, enterprise, fintech, and games. A16z currently has more

¹ For the purposes of this discussion, by crypto assets, we mean a digital form of property that is recorded on, and can be possessed and transferred person-to-person, through the use of a blockchain network or other similar technology.

March 13, 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

Re: Comments on the SEC Crypto Task Force’s Questions Concerning the Security Status of
Crypto Assets

Dear Commissioner Peirce:

Andreessen Horowitz (“a16z”) appreciates the opportunity to provide comments on the questions that the Securities and Exchange Commission’s Crypto Task Force provided to the public on February 21, 2025.¹ The Task Force’s thoughtful approach, seeking detailed and comprehensive information about a wide range of crypto issues, is commendable. While we recognize that the questions are not a roadmap to actions the Commission will take, we nonetheless applaud the Commission for its commitment to soliciting information from the public through a transparent process and its willingness to engage.

At a16z, we believe blockchain technology has incredible potential to promote innovation, entrepreneurship, and economic growth. Like the Crypto Task Force, we are deeply committed to the development of a legal and regulatory framework for crypto assets, which we believe is critical to fostering innovation while protecting market participants. Our numerous publications on developing regulatory approaches, as well as our ongoing engagement with regulators reflect this commitment and belief.² To that end, we hope that our observations, drawn from our deep experience, can be of assistance to the Commission. We believe that time is of the essence in these endeavors, and have separated our responses to the Task Force’s questions into different topic letters, which we intend to submit to the Commission as quickly as possible.

In this first letter, we address **Questions #1** through **#6**, presenting a single unifying regulatory framework that resolves many of the uncertainties surrounding the application of federal securities laws to blockchain systems. At the core of our approach is **control-based decentralization**—a straightforward yet powerful principle:

When control is eliminated, the application of securities laws should be limited;
When control is present, traditional (but modernized) approaches should be used.

¹ Statement, Securities and Exchange Commission, Hester M. Peirce, There Must Be Some Way Out of Here (Feb. 21, 2025), <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125>.

² For a list of our publications relating to crypto policy, see: <https://a16zcrypto.com/posts/focus-areas/policy>.

Control-based decentralization is not merely about dispersing ownership—it requires the elimination of *operational*, *economic*, and *voting* control, ensuring that blockchain systems function autonomously and without reliance on any central party. By applying this framework across our responses, we demonstrate how it can resolve the most significant areas of regulatory uncertainty, including with respect to the *Howey* test, *Reves* test, profits interests, transferable shares, stablecoins, wrapped tokens, staking-as-a-service offerings and liquid staking tokens, decentralized finance, and the broker, dealer, and registration regimes. By establishing a consistent, objective, and repeatable regulatory approach that is both merit- and technology-neutral, the Commission can provide the legal clarity necessary for entrepreneurs to build, market participants to engage and invest with confidence, and regulators to effectively protect markets—without stifling innovation.

I. About a16z	3
II. Responses to Crypto Task Force Questions #1 - #6	3
Question 1: Regulatory Taxonomy	3
1. Separate Crypto Asset Classification from Transaction Analysis.....	3
2. Identify Issues Arising from the Application of the Howey Test.....	5
3. Establish a Control-Based Decentralization Framework to Limit Federal Securities Laws.....	7
4. Create a Crypto Asset Taxonomy Based on Function and Risk.....	11
5. Establish Compliant Pathways for Network Tokens.....	15
6. Provide Regulatory Clarity for Certain Other Crypto Assets.....	21
7. Ensure Consistent Treatment of Comparable Economic Arrangements.....	22
Question 2: Other Financial Instruments	24
1. Profits Interests & Transferable Shares.....	24
2. Notes.....	25
Question 3: Security Status of Technology Functions	28
1. Background on the Exempt Technologies.....	29
2. Case Law & Analysis.....	31
3. Control-Based Decentralization Framework For Certain Exempt Technologies.....	38
Question 4: Security Status of Liquid Staking Tokens	41
1. Decentralized Smart Contract Protocol LSTs.....	41
2. Centralized Issuer LSTs.....	43
Question 5: Security Status of Certain Categories of Crypto Assets	45
1. Asset-Backed Tokens.....	45
2. Collectible Tokens.....	45
3. Company-Backed Tokens.....	46
Question 6: Merit- and Technology-Neutral Taxonomy	48
III. Conclusion	49

I. About a16z

A16z is a venture capital firm that invests in seed, venture, and late-stage technology companies, focused on bio and healthcare, consumer, crypto, enterprise, fintech, and games. A16z currently has more than \$74 billion in assets under management across multiple funds, with more than \$7.6 billion in committed capital for crypto funds. In crypto, we primarily invest in companies using blockchain technology to develop protocols that people will be able to build upon to launch Internet businesses. Our funds typically have a 10-year time horizon, as we take a long-term view of our investments, and we do not speculate in short-term crypto-asset price fluctuations.

II. Responses to Crypto Task Force Questions #1 - #6

Question 1: What type of regulatory taxonomy would provide a predictable, legally precise, and economically rational approach to determining the security status of crypto assets and transactions in such assets without undermining settled approaches for evaluating the security status of non-crypto assets and transactions?

Comprehensive legislation for the blockchain technology industry is necessary to both foster innovation and protect market participants. The Commission does not currently have the authority to provide this regulatory clarity beyond the application of the federal securities laws. Given that many crypto assets are outside the reach of current securities and commodities laws, effective regulation will therefore require legislation. Nevertheless, the Commission can address many of the harms that stem from present regulatory uncertainty. Among other things, it could articulate a fit-for-purpose regulatory taxonomy that clarifies the boundaries of securities laws. These efforts would also likely aid Congress as it attempts to craft a framework that extends to transactions in crypto assets that are not securities.

A regulatory taxonomy that balances predictability, legal precision, economic rationality, and workability—without disrupting established securities law—would incorporate the following:

1. Separate Crypto Asset Classification from Transaction Analysis
2. Identify Issues Arising from the Application of the *Howey* Test
3. Establish a **Control-Based Decentralization Framework** to Limit Federal Securities Laws
4. Create a Crypto Asset Taxonomy Based on Function and Risk
5. Establish Compliant Pathways for Network Tokens
6. Provide Regulatory Clarity for Certain Other Crypto Assets
7. Ensure Consistent Treatment of Comparable Economic Arrangements

Each of these steps is discussed in further detail below.

1. Separate Crypto Asset Classification from Transaction Analysis

The taxonomy should first distinguish between (i) the underlying crypto asset (which may or may not be a security), and (ii) specific transactions involving the asset, which could, under certain conditions, constitute securities transactions.

Due in large part to previous Commission actions, considerable confusion exists regarding the circumstances under which crypto assets may themselves constitute securities. For example, in *SEC v. Coinbase*,³ the Commission alleged that 13 crypto assets available for trading on the platform were “crypto asset securities” because they were the subjects of investment contracts. This appeared at odds with Supreme Court precedent, which as far back as *SEC v. W.J. Howey Co.*, made clear that the subject of an investment contract—in that case an orange grove—is not necessarily a security in and of itself.⁴ Rather, in elucidating the test for an investment contract, the Supreme Court highlighted that “[f]orm [is] disregarded for substance and the emphasis [is] placed upon economic reality”; what is primarily at issue in determining whether the transaction in a particular crypto asset involves the sale of a security is not the asset itself, but how it is being sold, the economic and non-economic attributes of the arrangement, and the reasonable expectation of purchasers.⁵ Recently, the Commission has walked back its previous assertions that crypto assets are themselves securities,⁶ returning to the *Howey* interpretation,⁷ but it remains difficult for today’s market participants to determine whether transactions in a particular crypto asset involve the sale (and resale) of a security.

An effective taxonomy must therefore separate crypto asset classification from transaction analysis. In particular, the taxonomy should distinguish:

- **Nature of the asset** – Much like commodities or currencies, a crypto asset might not have the embedded characteristics of a security—it may not be a security in isolation.
- **Nature of the transaction** – Certain sales, distributions, schemes, or other arrangements involving the asset might meet the criteria of an investment contract under *Howey* or other securities law tests, but even so, the investment contract may be distinguishable from the crypto asset involved in the transaction.⁸

By maintaining this separation, a regulatory taxonomy can align with traditional securities principles, ensuring market participants are protected without unnecessarily or unintentionally restricting non-securities use cases that appropriately fall outside the Commission’s jurisdiction. In establishing this

³ Complaint, *SEC v. Coinbase, Inc.*, No. 1:23-cv-04738 (S.D.N.Y. June 6, 2023), ECF No. 1.

⁴ 328 U.S. 293 (1946).

⁵ *Id.*, at 298.

⁶ In an amended complaint against Binance, the SEC clarified that “[...] with its use of the term ‘crypto asset securities,’ the SEC is not referring to the crypto asset itself as the security” and that it “[...] regrets any confusion it may have invited in this regard.”

Amended Complaint, *SEC v. Binance Holdings Ltd.*, No. 1:23-cv-01599 (D.D.C. Sept. 12, 2024), ECF No. 273.

⁷ In a recent staff statement on meme coins, the SEC clearly distinguished between the underlying crypto asset and specific transactions involving the asset, writing that “[g]iven that a meme coin is not itself a security, we conduct our analysis of whether a meme coin may be offered and sold as part of an investment contract under the “investment contract” test set forth in *SEC v. W.J. Howey Co.* [...] The *Howey* test analyzes whether certain arrangements or instruments are investment contracts based on their “economic realities.””

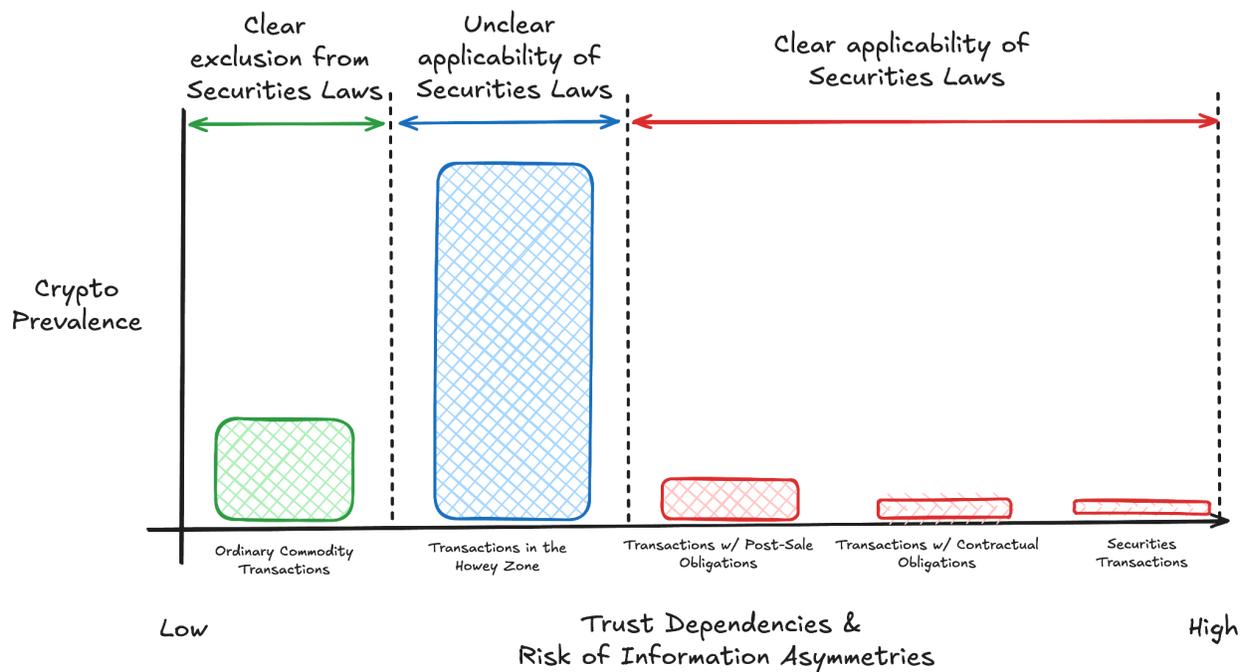
SEC Division of Corporation Finance, *Staff Statement on Meme Coins* (Feb. 27, 2025), <https://www.sec.gov/newsroom/speeches-statements/staff-statement-meme-coins>.

⁸ That a crypto asset has a nexus to a particular transaction does not necessarily mean that the crypto asset itself takes on the status of being a security under the federal securities laws. *Howey* centered on a business deal concerning what was, in substance, an investment in an orange business; that did not turn the oranges grown in the relevant groves into securities or into physical representations of the economic terms of the investment contract the parties entered into.

separation, it would be useful to articulate what specific actions or characteristics turn transactions involving non-securities crypto assets into securities transactions. In primary transactions, the application of *Howey* is straightforward given that the issuer’s sales efforts typically create reasonable expectations for the buyers that the efforts of the promoters will generate a return for those buyers. In secondary transactions or transactions in which there is no issuer, the application of *Howey* is challenging given that the buyer may have no relationship with the issuer, the issuer’s efforts may have diminished or disappeared and there may be no embedded obligations in the crypto asset itself. Guidance with respect to secondary transactions would therefore be most helpful. Overall, this approach would provide regulatory clarity and reduce the risk of enforcement-driven policymaking.

2. Identify Issues Arising from the Application of the *Howey* Test

Compounding the problem created by the lack of a clear approach by the Commission regarding asset classification and transaction analysis, prior Commission enforcement efforts using the *Howey* test have created significant uncertainty about when secondary transactions in many crypto assets that are not themselves securities are nevertheless subject to securities laws. This zone of uncertainty (the “**Howey Zone**”) applies to the vast majority of crypto asset transactions:⁹



The *Howey* test is an essential tool under federal securities law because it is a flexible, substance-over-form framework that captures investment schemes not explicitly enumerated in the definition of “security.” Its emphasis on “economic reality,” rather than rigid formal categories, prevents regulatory arbitrage based on efforts to raise form over substance. Historically, federal securities laws

⁹ Transactions involving crypto assets that are not securities (e.g., no grant of any rights, title, or interest in the issuer), do not involve any formal contractual obligations, and do not involve any post-sale obligations (e.g., no obligation on the part of the issuer or third party to undertake any efforts).

have also adapted to new financial instruments and structures, and *Howey* has played a central role in ensuring that securities regulation is not circumvented through superficial structural changes.

However, as discussed above, while the application of the *Howey* test, predicated on determining whether an “investment contract” exists, to primary transactions is relatively straightforward, its application to secondary transactions is difficult—this is particularly the case in the usual circumstance where the crypto asset issuer has no contractual privity with secondary market purchasers of its crypto assets and the crypto asset itself has no embedded obligations. Further, many crypto assets are autonomously issued by software and there is no issuer. Yet any application of *Howey* to secondary market transactions of crypto assets conceptually demands that an issuer exists and that the crypto asset itself essentially “embodies” obligations of that issuer such that the crypto asset is conceived of as the digital representation of certain rights and obligations that make up what are commonly called under *Howey* the “economic realities.” Conventional securities, such as stocks or bonds, do not create similar confusion as there is always an issuer and secondary-market purchasers have enforceable rights against that issuer. Thus, for crypto assets, this “embodiment” approach is at odds with the separation of asset classification from transaction analysis discussed above, and is therefore not useful. While courts and the Commission are beginning to appreciate this issue, more clarification is needed.¹⁰

These concepts have confused market participants and created uncertainty as to whether federal securities laws apply to a given crypto asset transaction. Compounding this confusion, the Commission’s application of the *Howey* test has exposed several issues that must be addressed to provide predictability and legal precision, including:

- **Lack of Predictability** – The subjective nature of the *Howey* test leads to high regulatory uncertainty, forcing crypto market participants to rely on *ex post* enforcement actions rather than clear *ex ante* rules in trying to discern whether federal securities laws apply. This is at odds with the need for a predictable regulatory environment.
- **Difficult to Enforce** – The subjective nature of the *Howey* test also means the Commission needs to expend considerable resources to determine whether the criteria of the test are satisfied and the Commission has jurisdiction. Bad actors have taken advantage of this slow and lack of uniform enforcement to harm market participants.
- **Impractical to Apply** – Many crypto assets may satisfy the criteria of the *Howey* test one day only to fail it another depending on a subjective assessment of “ongoing efforts” by third parties—something neither regulators nor crypto asset market participants can effectively assess; *Howey* provides no clear framework for recognizing when a transaction in a crypto asset transitions is out of the reach of federal securities laws when the relevant facts and circumstances change over time.

¹⁰ See, e.g., *SEC v. Ripple Labs, Inc.*, 2023 WL 4507900, at *23 (S.D.N.Y. July 13, 2023) (declining to address the question of whether indirect secondary sales constitute securities transactions, but stating that “whether a secondary market sale constitutes an offer or sale of an investment contract would depend on the totality of circumstances and the economic reality of that specific contract, transaction, or scheme.”); Transcript of Motions Hearing, *SEC v. LBRY*, No. 1:21-cv-260 (D.N.H. Jan. 30, 2023) (declining to extend holding to include secondary sales), ECF No. 105 at 34:14-16.

- **Boundless Reach** – Without clear limiting principles, the *Howey* test can be contorted and weaponized to target transactions a regulator does not like, potentially capturing everyday assets such as Nike shoes (the value of which may depend on Nike maintaining the status of its brand), Tesla cars (the value of which may increase depending on the success of new “full-self driving” software updates), or digital art (the value of which may increase as an artist grows in prominence)—all of which may involve investments of money, expectations of profits, and efforts of others. If *Howey* is read as expansively as some have read it, goods and services that never would have been considered securities could be treated as securities, dramatically expanding the reach of the federal securities laws beyond what they were enacted to accomplish.

Abandoning *Howey*, or attempting to limit it through formalistic requirements, would likely open up the potential for significant circumvention of federal securities laws.¹¹ Nor should special treatment be given to transactions in investment contracts where the nature and structure of those transactions (and the assets to which they relate) do not mitigate the risks characteristic of ordinary securities transactions that federal securities laws are intended to address.¹² However, the Commission’s recent unbounded application of the *Howey* test to crypto assets has been counterproductive to its stated mission: this approach has failed to protect market participants, has not facilitated fair and efficient markets, and has hindered capital formation.

A better approach is possible. The Commission can preserve *Howey* while addressing its limitations when applied to secondary transactions in a merit- and technology-neutral way. In particular, through the issuance of guidance, granting of no-action relief, and creation of safe harbors, the Commission could establish a **control-based decentralization framework** (as discussed below) that constrains the reach of federal securities laws while substantially mitigating the risks they are intended to address. The principles of such a framework could then be applied to *Howey* to mitigate the risks associated with transactions in digital assets. Doing so could help ensure that investment schemes that give rise to information asymmetries and other such risks remain subject to securities laws, regardless of whether they involve traditional instruments or blockchain-based innovations, while continuing to protect market participants and foster innovation. We outline a path for doing so in the remainder of the steps for our proposed taxonomy.

3. Establish a Control-Based Decentralization Framework to Limit Federal Securities Laws

The confusion arising at the intersection of federal securities laws and blockchain technology is not isolated to the *Howey* test. As detailed in our responses to **Questions #2** through **#5**, regulatory uncertainty that goes well beyond *Howey* exists with respect to a number of crypto asset transactions,

¹¹ For example, stipulating that the *Howey* test will only be satisfied when a formal contract exists between the issuer and the purchaser of a crypto asset would not only carve out nearly all crypto assets from the Commission’s authority, even where they present similar risks to investors as securities, it would also enable disguised securitizations—issuers would sell assets to investors and promise to deliver profits from their business to asset holders, but would negotiate such arrangements without a formal contract simply because entering into such contract would make the transaction a securities transaction, thereby encumbering it with the requirements of securities laws.

¹² For example, if crypto assets that have similar risk profiles to securities can trade on secondary markets simply by complying with a significantly reduced disclosure regime when compared to traditional securities, issuers would likely restructure traditional securities offerings to take advantage of the lower burden.

participants, and technologies. Tackling each of these uncertainties as isolated and unique problems would no doubt remove significant regulatory uncertainty, but it risks creating inconsistencies, confusion, and potential gaps in regulatory coverage that may be exploited by bad actors. Instead, a far better approach would be to use a straightforward, yet powerful unifying principle across these challenges:

**When control is eliminated, the application of securities laws should be limited;
When control is present, traditional (but modernized) approaches should be used.**

Using this principle, the Commission can establish a clear, readily measurable, and objective **control-based decentralization framework** that limits the reach of federal securities law when control has been eliminated from a system, including with respect to transactions of crypto assets currently in the *Howey* Zone. Importantly, this does not mean that the application of federal securities laws is always warranted where systems are controlled—it means that in such circumstances the Commission should follow traditional (but modernized) approaches in assessing the applicability of federal securities laws. Collectively, this provides a comprehensive and consistent approach to providing regulatory certainty while fostering innovation and protecting crypto asset market participants.

The focus on control in this framework stems from the nature of blockchains and smart contract protocols (“blockchain networks”). Blockchain networks do not function as agents. Rather, they empower users with agency. By executing transactions according to predefined rules in an automatic, transparent, and deterministic manner, they remove trust dependencies from arrangements, including arrangements that might otherwise implicate federal securities laws. For example, crypto assets providing holders with rights in decentralized blockchain networks do not have the same trust dependencies as shares of stock of centralized companies; smart contract protocols autonomously issuing crypto assets to users in exchange for collateral do not have the same trust dependencies as money market funds managed by brokers; and smart contract protocols enabling peer-to-peer transfers of securities do not have the same trust dependencies as securities brokers and exchanges.

This amelioration of trust dependencies with respect to a blockchain network and its crypto asset (together, a “blockchain system”) is made possible by the fact that such systems are capable of decentralization—operation absent human intervention and control.¹³ **Whoever controls a system (a company, a blockchain system, etc.) controls the risks associated with that system and can unilaterally affect or structure its risk.**¹⁴ For example, the officers and directors of Apple control the company’s direction and can unilaterally change the risks associated with holding a share of Apple stock; Vanguard controls their clients funds, which exposes those clients to the risk of loss of funds; and Meta controls the application Facebook and can unilaterally change the risks associated with using the Facebook platform, including by deplatforming users. Where blockchain systems are controlled, they are subject to many of the trust dependencies of ordinary intermediary-based arrangements such as these examples—control negates their purpose and undermines the justification for their exclusion from federal securities laws where such laws are implicated.

¹³ Miles Jennings, *Defining decentralization: It comes down to control*, a16z crypto (Feb. 13, 2025), <https://a16zcrypto.com/posts/article/defining-decentralization-control/>.

¹⁴ Dennis S. Corgill, *Securities as Investments at Risk*, 67 Tul. L. Rev. 861 (1992), <https://www.tulanelawreview.org/pub/volume67/issue4/securities-as-investments-at-risk>.

But where blockchain systems can eliminate mechanisms of control—including *operational*, *economic*, and *voting* control—they are not subject to the trust dependencies that intermediary-based arrangements give rise to and, therefore, should be excluded from the direct application of the federal securities laws.

The Commission should use a control-based decentralization framework to appropriately limit the applicability of the federal securities laws to blockchain systems where reduced trust dependencies mitigate the risks securities laws are intended to address. Such a framework would not only be helpful in evaluating the applicability of federal securities laws to transactions in many different types of crypto assets (see Part 5 of this response to **Question #1** and our response to **Questions #2, #4 and #5**), it could also form the basis for excluding participants and technologies from registration requirements for brokers, dealers, and exchanges (see our response to **Question #3**).

In practice, the following criteria are what distinguish centralized, controlled systems from decentralized systems, thereby mitigating control-related risks. Importantly, these criteria are not just about the distribution of ownership; rather, they focus on mechanisms of *operational*, *economic*, and *voting* control.¹⁵ In addition they are intended to be objective and easily verifiable—market participants and regulators should be able to verify any objective dimension of control in a system’s source code, significantly increasing transparency.¹⁶

- **Open source** – The system’s source code is open source, freely and publicly available to all.
- **Autonomous** – The system operates, executes, and enforces transactions and other activities without human intervention, functioning solely through transparent, predetermined rules embedded in source code, and no person or group under common control has unilateral authority or the ability to alter the functionality, operation, or rules of the system.
- **Permissionless** – No person or group under common control has unilateral authority or the ability to restrict or prohibit access to or operation of the system for any use.
- **Credibly neutral** – The system’s source code does not empower anyone with private permissions, hard-coded privileges, or similar rights over others that would enable them to discriminate against particular users or use-cases.
- **Non-custodial** – The system’s source code enables participants to maintain total independent control of crypto assets owned by them, with access and management governed solely by their private keys.

¹⁵ Namely, a system has effectively eliminated operational control if it is autonomous, permissionless, credibly neutral, and non-custodial. Likewise, it has alleviated economic control if it has achieved economic independence, credible neutrality, and is open source. Finally, it has eliminated voting control if it is distributed.

¹⁶ The suggested criteria are intended to be a starting point for the Commission’s evaluation. They need further legal precision and input from industry participants. For instance, some powers should be capable of being reserved through decentralized governance mechanisms, such as pause controls to ensure security. And specific applications of the criteria to blockchain technologies need to be explored and tested, such as layer-1 blockchains versus layer-2 blockchains. For a more in-depth discussion of these criteria, see: Decentralization Research Center, *Designing Policy for a Flourishing Blockchain Industry* (Feb. 2025), <https://thedrcenter.org/wp-content/uploads/2025/02/DRC-Designing-Policy-Final.pdf>.

- **Economically independent** – The economic mechanisms of the system that are designed to drive the value of any crypto asset of the system are functional and not dependent on any development company or issuer.
- **Distributed** – To the extent that the foregoing features of a system can be amended, changed, or modified, no person or group under common control has control of voting power necessary to make such amendment, change, or modification.

The above characteristics are the foundational requirements that enable blockchains to realize their full potential; they are what enable them to operate absent any and all human intervention and control, thereby mitigating control-related risks. A control-based decentralization framework established on these principles would help to foster innovation and protect market participants for several reasons:

- *Eliminates Control:* The framework abrogates control, ensuring that blockchain networks are not dependent on intermediaries (including entrenched players like big banks and big tech), thereby providing substantial protections to market participants, and guarding against regulatory capture and value extraction. It also provides the foundation for a democratized, user-controlled internet that promotes competition, safeguards freedom, and rewards stakeholders.¹⁷
- *Incentivizes Decentralization:* The framework provides powerful incentives in favor of decentralization. Without such incentives, the costs of decentralization push strongly towards shortcuts and centralization, subjecting market participants to risk.¹⁸ Decentralization requires eliminating mechanisms of control to protect market participants. It requires entrepreneurs and developers to proceed by broad consensus, rather than by singular command-and-control. It necessitates the distribution of ownership to other network participants and invites third-parties to compete, thereby diluting any one person’s economic interest, standing, and singular vision. All of these steps are costly, but necessary to ensure blockchain systems protect market participants by functioning more like public infrastructure than proprietary, closed systems.
- *Increases Transparency:* The framework provides clear, objective, and easily verifiable criteria to help ensure that market participants are able to adequately assess when the risks associated with a blockchain system have been successfully mitigated, while enabling entrepreneurs to understand exactly what criteria they need to focus on. Transparency further limits the ability of crypto asset market participants to attempt to use “decentralization theater” as a means of circumventing federal securities laws.

Once a control-based decentralization framework is promulgated, the Commission can foster innovation, protect market participants, and establish the U.S. as the center of the blockchain industry by providing further guidance, no-action relief, and carrying out enforcement efforts in line with the framework, including with respect to specific types of crypto asset transactions and participants. In certain of these contexts, all of the criteria will be necessary to establish a lack of control, and in others only certain criteria will need to be achieved in order to sufficiently address the risks federal securities laws are

¹⁷ Miles Jennings, *Decentralization Is Why We Fight for Crypto*, CoinDesk (Dec. 17, 2024), <https://www.coindesk.com/opinion/2024/12/17/decentralization-is-why-we-fight-for-crypto> (last updated Dec. 20, 2024).

¹⁸ Miles Jennings, *Why decentralization matters, and needs incentives*, a16z crypto (Feb. 3, 2025), <https://a16zcrypto.com/posts/article/why-decentralization-matters-incentivizing-decentralization-incentives/>.

intended to mitigate. But the Commission’s application of the framework could nevertheless be uniform—for example, in each instance the test could begin with a question of whether or not the system is controlled, with the Commission then creating (i) a list of objective criteria that, if met, would create a presumption that the system is not controlled (i.e., a safe harbor) and (ii) a list of objective criteria that, if met, would create a rebuttable presumption that the system is controlled.

In the remainder of this response, we detail how this approach be applied across several different types of crypto asset transactions (our response to Part 5 of **Question #1**, and **Questions #2, #4 and #5**) and transaction participants (our response to **Question #3**).

4. Create a Crypto Asset Taxonomy Based on Function and Risk

The adoption of a control-based decentralization framework enables the creation of a coherent, merit- and technology-neutral crypto asset taxonomy based on function and risk.

Because they are embedded in software, crypto assets can be programmed to represent anything, including any digital form or record of property. This means that crypto assets can be designed as digital stores of value like Bitcoin, productive and consumptive assets like Ether, collectibles like digital trading cards and game items, payment stablecoins like USDC, and even shares of stock. Some crypto assets provide holders with various rights (such as voting power or economic rights) while others simply enable the use of a product. Some crypto assets are transferable among users, and others are not. And some crypto assets are fungible in the sense that all units are equivalent, whereas others are non-fungible, in that they represent unique individual assets. These design choices dictate the function and risk associated with a given crypto asset and inform whether federal securities laws are applicable to a specific crypto asset or transactions therewith.

While crypto asset categorizations continue to evolve, the seven categories we primarily see entrepreneurs building with today are: **Network Tokens**, **Security Tokens**, **Company-Backed Tokens**, **Collectible Tokens**, **Arcade Tokens**, **Asset-Backed Tokens**, and **Memecoins**.

- **Network Token:** A network token is a crypto asset that is intrinsically linked to, and primarily derives or is expected to primarily derive its value from, the programmatic functioning of a blockchain network. Network tokens often have embedded utility; they may be used for network operations, to form consensus, to coordinate protocol upgrades, or to incentivize network actions. Critically, the value of network tokens are driven by the adoption and functioning of their underlying networks—often containing programmatic economic mechanisms that render network tokens productive and *economically independent* from any person. These mechanisms include programmatic and autonomous buybacks, distributions, and other changes to the total crypto asset supply via crypto asset creation (faucets) or burning (sinks) to introduce inflationary and deflationary pressures in service of the network.¹⁹

¹⁹ See Tim Roughgarden, *Transaction Fee Mechanism Design* (Oct. 2019), <https://timroughgarden.org/papers/eip1559exchanges.pdf>; See also Mason Hall, Porter Smith, Miles Jennings and Ross Shuel, *A New Financial Model for App Tokens: How to Generate Cash Flows*, a16z Crypto (Aug. 8, 2024), <https://a16zcrypto.com/posts/article/application-tokens-economic-model-cash-flows/>.

Network tokens are essential to the deployment of blockchain technology and are best used to bootstrap the creation of a new network—to self-fund and incentivize its own continuous and secure operation, and to drive network effects by incentivizing network growth.²⁰ Examples include BTC, ETH, SOL, and UNI. In the context of smart contract protocols, network tokens are also sometimes called “Protocol tokens” or “App tokens.”

The trust dependencies of network tokens are distinct from securities. Network tokens can have trust dependencies that arise from both control of the underlying network and the ongoing efforts of centralized actors.²¹ But because they relate to blockchain networks that are capable of decentralized operation, they can eliminate trust dependencies relating to control, thereby justifying the exclusion of transactions of network tokens from federal securities laws. Distribution of network tokens can facilitate decentralization by enabling the system to function autonomously (eliminating *operational control*) as well as by eliminating *voting control* and reducing *economic control* of the system. We discuss the treatment of network tokens under federal securities laws further in our response to Part 5 of **Question #1** and **Question #2**.

- **Security Token:** A security token is a crypto asset that represents the digital form of a security on a blockchain.²² The security might be in a traditional form, like a share in a company or a corporate bond, or might take on specialized characteristics, such as providing a profits interest in an LLC,²³ a share in an athlete’s future earnings,²⁴ or even securitized rights to future payments of litigation settlements.²⁵ Securities typically grant the holder a defined right, title, or interest, and their issuers usually have unilateral power to affect or structure the risk of the asset, including by exerting control over how the underlying enterprise is managed or operated.²⁶ Security tokens will likely become increasingly prevalent, bringing efficiencies and liquidity to securities markets.
- **Company-Backed Token:** A company-backed token is a crypto asset that is intrinsically linked to, and primarily derives or is expected to primarily derive its value from, an offchain application, product, or service operated by a company (or other centralized organization). Like network tokens, company-backed tokens may make use of blockchains and smart contracts (e.g., to facilitate payments). But because they primarily relate to offchain operations, rather than ownership of a blockchain network, a company may unilaterally control their issuance, utility, and value. Like arcade tokens (described below), company-backed tokens often have their own embedded utility, but unlike arcade tokens, company-backed tokens are speculative rather than being held or used for consumptive purposes.

²⁰ See Chris Dixon, *The Web3 Playbook: Using Token Incentives to Bootstrap New Networks*, a16z crypto (Dec. 9, 2021), <https://a16zcrypto.com/posts/article/the-web3-playbook-using-token-incentives-to-bootstrap-new-networks/>

²¹ See Miles Jennings, Defining decentralization: It comes down to control (Feb. 13, 2025), <https://a16zcrypto.com/posts/article/defining-decentralization-control/>.

²² Cornell Law School, *Security*, Legal Information Institute, <https://www.law.cornell.edu/wex/security>.

²³ Kristoffer Warren, *Profits Interest*, Carta (Aug. 30, 2022), <https://carta.com/learn/startups/compensation/equity-incentive-plans/profits-interest/>.

²⁴ Wikipedia, *Fantex*, <https://en.wikipedia.org/wiki/Fantex> (last edited Feb. 16, 2025).

²⁵ Wikipedia, *Tobacco Bond*, https://en.wikipedia.org/wiki/Tobacco_bond (last edited Sept. 13, 2024).

²⁶ Corgill, *supra* note 14.

Company-backed tokens are most often used to stimulate investment in applications, products, or services controlled by a company, potentially acting as a proxy for an equity interest or profits interest in that company. Examples of company-backed tokens include FTT, which was the economic equivalent of a profits interest in FTX.

Even though company-backed tokens do not grant the holder a defined right, title, or interest like a traditional security, they have trust dependencies that are similar to securities—both control-related and ongoing efforts-related. That means their value is inherently dependent upon and is controlled by their issuer. But unlike in the case of network tokens, the control-related risks are not capable of being mitigated through decentralization because the value is associated with an offchain application, product, or service not capable of operation without human intervention and control. We discuss the treatment of company-backed tokens under federal securities laws further in our response to **Question #5**.

- ***Arcade Token***: An arcade token is a crypto asset that provides utility within a system and is not intended for investment purposes.²⁷ Arcade tokens often function as currencies within an issuer-controlled digital economy: digital gold in a game, loyalty points within a membership program, or redeemable credits for digital products and services. Importantly, they are distinguishable from security tokens, network tokens, and company-backed tokens because they are specifically designed to dissuade speculation. For instance, they may have uncapped supplies (meaning an unlimited number can be minted) or limited transferability; they may expire or lose value if unused; or they may only have monetary value and utility within the system in which they are issued. Most importantly, they do not offer or promise financial returns outside of the system or specific digital economy.

Arcade tokens are best used as currencies within an issuer-controlled digital economies, where the issuer derives economic benefit from controlling the monetary policy (i.e., acting as the central bank) of that digital economy and engaging in efforts to dampen price volatility, as opposed to benefiting from the appreciation of token price. Examples include Pocketful of Quarters, an in-game asset that received no-action relief from the Commission in 2019. Arcade tokens are also sometimes called “Utility tokens,” “Loyalty tokens,” or “Points.”²⁸

Arcade tokens have both control-related and ongoing efforts-related trust dependencies. However, because they are non-speculative in nature, they are excluded from federal securities laws.

- ***Collectible Token***: A collectible token is a crypto asset whose value, utility, or significance is primarily derived from being a record of ownership of a tangible or intangible good. For instance, a collectible token may be a digital analog or representation of a work of art, a musical composition, or a literary work; a collectible or merchandise, like a ticket stub from a concert; membership in a club or community; or an asset in a game or metaverse, like a digital sword or

²⁷ *United Housing Foundation, Inc. v. Forman*, 421 U.S. 837 (1975) (holding that an instrument must have investment characteristics in order to qualify as a security).

²⁸ Pocketful of Quarters, Inc., SEC No-Action Letter (July 25, 2019), <https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1>.

plot of metaverse land.²⁹ These crypto assets are typically non-fungible and often have utility entirely aside from any investment motivation. For example, a collectible token may function as a license or ticket to an event, could be used in a video game (like that sword), or could provide ownership rights with respect to a song.

Collectible tokens are best used to convey ownership of tangible or intangible goods. Many, although not all, “NFT” products fall into this category.³⁰ Examples include NFTs that convey ownership of digital art or other media; profile pictures (“pfp”) like CryptoPunks and Bored Apes, as well as other virtual fashion and branded goods;³¹ and game items. Some collectible tokens are directly associated with physical products, such as to provide a digital extension of the physical product experience, like with Pudgy Penguins toys.

Collectible tokens should generally be excluded from federal securities laws. We discuss their treatment further in our response to **Question #5**.

- **Asset-Backed Token:** An asset-backed token is a crypto asset that primarily derives its value from a claim on, or economic exposure to, one or more underlying assets. These underlying assets may include physical-world assets (e.g., commodities, fiat currency, or securities) or crypto assets (e.g., cryptocurrencies or liquidity pool interests). Asset-backed tokens may be fully or partially collateralized and can serve different purposes: acting as stores of value, hedging instruments, or onchain financial primitives. Unlike collectible tokens, which derive value from ownership of a unique good (like digital art, in-game items, or event tickets), asset-backed tokens function more like financial instruments, deriving value from their collateral, price-pegging mechanisms, or rights to redemption.

There are many use cases for asset-backed tokens, including: **derivative tokens**, which provide synthetic exposure to underlying assets or financial positions; **deposit receipt tokens**, which represent deposited or escrowed assets; **liquidity provider tokens** (“LP tokens”), which represent claims on pooled assets in decentralized finance (“DeFi”) protocols; **liquid staking tokens**, which represent staked assets; and **stablecoins**, which are pegged to a currency or asset. Examples include OPYN’s Squeeth, Compound’s C-tokens, Uniswap LP tokens, Lido’s stETH, and Circle’s USDC.

Certain asset-backed tokens, like derivative tokens and fiat-backed stablecoins, will be subject to regulatory regimes beyond federal securities laws. But where they are not covered by such regimes, they may implicate federal securities laws. The trust dependencies of asset-backed tokens are a function of the trust dependencies of the underlying asset as well as the manner in which they are structured and issued. Asset-backed tokens issued by centralized issuers may take on risks associated with both control and the ongoing efforts of the issuer. Conversely,

²⁹ Scott Duke Kominers, *Metaverse Real Estate: Digital Land & Value to Users*, a16z crypto, (June 2, 2022), <https://a16zcrypto.com/posts/article/metaverse-real-estate-digital-land-value-to-users/>.

³⁰ Steve Kaczynski & Scott Duke Kominers, *The Everything Token: How NFTs and Web3 Will Transform the Way We Buy, Sell, and Create* (Penguin Publishing Group, 2024).

³¹ Scott Duke Kominers & Steve Kaczynski, *The NFT Staircase: How digital ownership benefits brands and consumers*, a16z crypto, (Feb. 21, 2024), <https://a16zcrypto.com/posts/article/the-nft-staircase/>.

asset-backed tokens issued by decentralized blockchain networks may eliminate all trust dependencies. We discuss the treatment of asset-backed tokens further in our responses to **Questions #2, #4, and #5**.

- **Memecoin:** A memecoin is a crypto asset without intrinsic utility or value, often tied to an internet meme or community-driven movement, and not fundamentally tied to a network, company, or application. As recognized by a recent SEC Division of Corporation Finance Staff Statement, memecoins’ prices are driven purely by speculation and associated market forces (which unfortunately makes them highly susceptible to manipulation).³² Their central features are their lack of intrinsic purpose (if they had an intrinsic purpose, they would no longer be memecoins), lack of utility, and their resulting zero-sum nature and volatility. Given this, memecoins have no trust dependencies and are properly excluded from federal securities laws. Examples include PEPE, SHIB, and TRUMP.

Every crypto asset may not fit neatly within one of these categories—entrepreneurs are regularly iterating and experimenting. But these categories are broadly applicable, with the defining characteristic that delineates them being the expected source of value accrual, which implicates control.³³ In other words, the taxonomy focuses on the *economic function* and *risk* profile of a given asset rather than the underlying technology itself using a control-based decentralization framework.

5. Establish Compliant Pathways for Network Tokens

Using the control-based decentralization framework and token taxonomy outlined in Parts 3 and 4 above, the Commission should provide additional compliant pathways for projects seeking to utilize network tokens. Through the issuance of guidance, granting of no-action relief, creation of safe harbors, and tailoring of registration pathways, the Commission should: (a) provide a clear pathway for certain transactions of network tokens to be exempt from federal securities laws; and (b) create a fit-for-purpose registration pathway for primary offerings of network tokens.

a. *Exempt pathway for network tokens*

The availability of any new exemptions for transactions of network tokens from federal securities laws should hinge on (i) the trust dependencies inherent to network tokens and (ii) the presence of potential information asymmetries.

The Commission’s 2019 Framework for “Investment Contract” Analysis of Digital Assets (the “2019 Framework”)³⁴ similarly sought to address trust dependencies and information asymmetries

³² U.S. Securities and Exchange Commission, Staff Statement on Meme Coins (Feb. 27, 2025), <https://www.sec.gov/newsroom/speeches-statements/staff-statement-meme-coins>.

³³ Miles Jennings, Scott Duke Kominers & Eddy Lazzarin, *Defining Tokens*, a16z crypto (Mar. 5, 2025), <https://a16zcrypto.com/posts/article/defining-tokens/>.

³⁴ U.S. Securities and Exchange Commission, Framework for “Investment Contract” Analysis of Digital Assets (2019), <https://www.sec.gov/about/divisions-offices/division-corporation-finance/framework-investment-contract-analysis-digital-assets>.

through its “sufficient decentralization” construct. In particular, the framework concluded that where control-related and ongoing efforts-related trust dependencies of a network token are eliminated via the achievement of “sufficient decentralization,” the risk of information asymmetries arising with respect to the network token are low, and transactions of such network token should not be subject to federal securities laws. While reasonable, the single-pronged approach of using decentralization to resolve the information asymmetries arising with respect to network tokens has not been effective. As discussed in Part 2 above, the Commission’s application of the *Howey* test to secondary transactions created several problems. Further, use of the 2019 Framework has had several unintended consequences, ultimately failing to foster innovation or protect market participants.

The Commission can establish a more effective framework for network tokens using a two-pronged approach—utilizing objective control-related decentralization criteria to mitigate the risks arising from control-related trust dependencies and applying supplemental disclosure requirements to mitigate the risks of information asymmetries arising from ongoing efforts-related trust dependencies. As set out below, this can be done by (i) replacing the 2019 Framework with a control-based decentralization framework and (ii) taking additional steps to bolster the control-focused approach.

First, there are many reasons why the control-based decentralization framework outlined in Part 3 above is superior for mitigating the trust dependencies and risks of information asymmetries associated with transactions of network tokens:

- Even though the presence of both control-related and ongoing efforts-related trust dependencies can give rise to information asymmetries regarding a network token, the risks arising from control are much more significant. As mentioned above, whoever controls a system can unilaterally affect or structure the risk associated with that system.³⁵ In such cases, risks of information asymmetries are likely to be high. While a dependence on the ongoing efforts of a small number of actors to maintain and develop the system can give rise to information asymmetries, such risk is greatly reduced when the centralized control of the system is eliminated.³⁶
- A focus on control enables more objectivity than the 2019 Framework, whose expansive and subjective approaches to defining decentralization for network tokens produced outcomes antithetical to the Crypto Task Force’s dual-mandate. In the words of Crypto Task Force Chairman and Commissioner Peirce, it went about “[...] splashing lots of factors on the canvas without any clear message.”³⁷ The 2019 Framework’s expansiveness and subjectivity were largely

³⁵ Corgill, *supra* note 14.

³⁶ It is worth observing that third parties independently engaging in efforts with respect to a commodity can manifest information asymmetries with respect to that commodity without triggering the need to regulate that commodity as a security. In addition, similar to ordinary commodities, network tokens (by definition) do not entitle the holder of the token to any right, title, or interest in the issuer or any ongoing efforts by any third parties. As a result, outside of the context of primary transactions, where investors are buying from an issuer, the holders of network tokens have no right to benefit from the ongoing efforts by third parties, who are acting on their own behalf. Further, by nature of the system not being controlled, no party can implement changes to the system without broader consensus, thereby mitigating the risk that anyone can unfairly capitalize from the creation of asymmetric information.

³⁷ Hester M. Peirce, SEC Comm’r, Speech at the Securities Enforcement Forum: How We *Howey* (May 9, 2019), <https://www.sec.gov/newsroom/speeches-statements/peirce-how-we-howey-050919>.

due to its use of criteria focusing on tokenholder reliance on ongoing efforts, which has created confusion for market participants and enabled capricious enforcement. Further, it was not merit-neutral, inherently requiring regulators to assess whether the efforts of a development team with respect to a given blockchain system were valuable. The subjective questions posed by the 2019 Framework have not been constructively advanced or resolved since it was introduced, and leaves unanswered the essential question of how to determine objectively when a platform is “sufficiently decentralized.”

- The 2019 Framework’s emphasis on ongoing efforts discouraged builders from improving upon networks post-token launch, introducing new operational and execution risks and hampering innovation. Elaborating on how to ascertain whether the third prong of the *Howey* test (reasonable expectation of profits derived from efforts of others) is met, the 2019 Framework asserts that it is more likely that this prong is satisfied if an active participant is “[...] responsible for the development, improvement (or enhancement) [...] of the network.”³⁸ Many reasonably interpreted this statement to mean that if a developer makes an effort to enhance a network post-launch—irrespective of whether or not the developer controls the network and thus poses risks to market participants—this action could satisfy *Howey*’s third prong.³⁹ The result is that, today, developers are disincentivized from upgrading existing networks. This perverse incentive is the opposite of what is necessary to foster innovation and protect market participants.⁴⁰

In sum, a control-based decentralization framework like the one discussed in Part 3 enables a clear, objective definition of decentralization focused on control-related trust dependencies that would enable market participants and regulators to determine when control-related risks have been effectively eliminated. This would resolve many of the issues introduced by the 2019 Framework’s subjective and expansive approach.

Second, the Commission should bolster this approach by improving the pathways by which entrepreneurs are able to pursue decentralization. Here again, analyzing the challenges that resulted from the 2019 Framework is informative:

- The 2019 Framework necessitated that networks achieve “sufficient decentralization” in order to exempt public transactions in network tokens from the federal securities laws, but it did not

³⁸ The 2019 Framework, *supra* note 34.

³⁹ William Hinman, Dir., SEC Div. of Corp. Fin., Remarks at the Yahoo Finance All Markets Summit: Digital Asset Transactions: When *Howey* Met Gary (Plastic) (June 14, 2018), <https://www.sec.gov/newsroom/speeches-statements/speech-hinman-061418> (suggesting that the Commission should consider whether a “person or group retained a stake or other interest in the digital asset such that it would be motivated to expend efforts to cause an increase in value in the digital asset,” and whether “purchasers [would] reasonably believe such efforts will be undertaken and may result in a return on their investment in the digital asset.”).

⁴⁰ Miles Jennings, *Defining decentralization: It comes down to control*, a16z crypto (Feb. 13, 2025), <https://a16zcrypto.com/posts/article/defining-decentralization-control/> (“The incorporation of ‘ongoing efforts’ into the definition of decentralization created a paradox: It incentivized builders to forestall or obfuscate ongoing development efforts post-token launch, thereby introducing greater operational and execution risks to token holders rather than reducing such risks.”).

provide sufficient flexibility for projects to achieve sufficient decentralization over time. This construct created a catch-22 for entrepreneurs, leading many to conclude that the only way to distribute tokens without triggering the requirements of federal securities laws was to launch a decentralized network and yet, achieving decentralization paradoxically *requires* tokens to be broadly and equitably distributed. As a result, the 2019 Framework created a “chicken-or-the-egg” paradox for networks that need to make use of a network token in order to achieve decentralization.⁴¹ This interpretation and application of the federal securities laws has, unfortunately, discouraged technological innovation by stifling progress toward decentralization.

- As discussed above, the 2019 Framework used decentralization as the sole tool to address potential information asymmetries arising from network tokens resulting from both control and ongoing efforts, and this expansive definition of decentralization resulted in negative unintended consequences, like incentivizing builders to forgo development of their project post-token launch in order to avoid regulatory scrutiny. But, if a control-based decentralization framework is used, market participants could potentially be exposed to information asymmetries that may develop as a result of ongoing efforts of entrepreneurs.
- The 2019 Framework definition of “sufficient decentralization” meant that a network could meet the applicable decentralization threshold one day but fail it another. While decentralization is a spectrum and projects can move both ways across it, this “morphing” concept has been difficult to enforce in practice. A project’s decentralization status (and the regulatory classification of its network token) can change without secondary market participants ever being able to assess the difference, which exposes tokenholders to risk. As discussed above, a control-based decentralization framework that utilizes objective criteria could mitigate this risk,⁴² but it would nevertheless remain present without further measures (which we propose below).

In sum, in order to resolve the issues of the 2019 Framework, an exempt pathway for network tokens needs to: (i) provide a pathway for progressive decentralization; (ii) pair the application of a control-based decentralization framework with other mechanisms to reduce information asymmetries; and (iii) provide greater certainty to market participants regarding the impact of individuals exercising control over a previously decentralized project. Importantly, none of these steps would mandate that projects eliminate control. Rather, they provide regulatory certainty for projects that pursue decentralization, while leaving the Commission to pursue traditional approaches or develop modernized approaches for assessing the applicability of federal securities laws to centralized systems.

⁴¹ Jad Esber & Scott Duke Kominers, *Progressive decentralization: a high-level framework*, a16z crypto, (Jan. 12, 2023), <https://a16zcrypto.com/posts/article/progressive-decentralization-a-high-level-framework/>.

⁴² With a control-based decentralization framework, it is unlikely that Network Tokens would drift in and out of their exempt status. This is one of the strong benefits of objective criteria. Once the criteria are met, it would be difficult for a party to regain operational control or to position itself as being able undertake efforts that third parties could reasonably expect to create a return. Nevertheless, if a party in connection with the sale of a Network Token conveyed to the marketplace a plan that reasonably gave rise to such expectations, the Commission could assert the principles of *Howey* to characterize that sale by such person as a securities transaction subject to protections under the federal securities laws. Such an approach, would restrict controlling persons, while enabling other market participants to continue unabated.

Given the foregoing, the Commission could take the following steps:

- i. ***Airdrop Safe Harbor*** – The Commission should facilitate progressive decentralization by establishing a safe harbor under its exemptive authority for distributions of crypto assets via “airdrops” and other incentive-based rewards that meet certain conditions, including that: (i) the crypto assets be network tokens; (ii) the underlying blockchain network be functional (e.g., exhibits basic operational capacity and is capable of fulfilling its essential purposes absent intervention of individual actors, but not yet autonomous); (iii) the distribution be broad and equitable; (iv) the distribution be for limited consideration; and (v) that insiders be subject to robust transfer restrictions. Network tokens issued via airdrop or incentive-based rewards program in compliance with the safe harbor would then be free to be traded in secondary transactions exempt from federal securities laws.

With airdrops and incentive-based rewards of network tokens permissible prior to the elimination of control, projects can launch and pursue decentralization without risk of running afoul of federal securities laws. Meanwhile, this approach would help to protect market participants from predatory behaviors, end the detrimental and self-inflicted exclusion of U.S. persons from such distributions, and facilitate decentralization, engendering the many benefits decentralization provides along with market participant protections.

We have separately prepared and submitted a detailed safe harbor proposal for airdrops and incentive-based rewards in-line with the foregoing.⁴³

- ii. ***Control-Based Decentralization Framework Guidance for Network Tokens*** – The Commission should adopt a control-based decentralization framework for network tokens by issuing tailored guidance regarding (I) a control-based decentralization framework for network tokens and (II) the use of Rule 144 by individuals receiving network tokens in private transactions subject to existing exemptions from federal securities laws, such as officers, directors, employees, shareholders, investors, advisors and consultants (“insiders”):

- A. The Commission’s application of a control-based decentralization framework to network tokens should require that projects eliminate *operational*, *economic*, and *voting* control. Of the control-based decentralization criteria discussed in Part 3 above, the Commission should emphasize that the most critical elements are *autonomy* (which eliminates single points of control and failure) and *economic independence* (which squarely anchors profit expectations to the functioning of the network, as opposed to a company).⁴⁴ The Commission should issue interpretive guidance that secondary transactions of network tokens of a given blockchain system will not implicate federal securities laws where

⁴³ Miles Jennings, Jai Ramaswamy, Scott Walker, Michele Korver, David Sverdllov, & Aiden Slavin, *SEC RFI: Safe harbor for certain airdrops & incentive-based rewards of network tokens*, a16z crypto, (March 13, 2025), <https://a16zcrypto.com/posts/papers-journals-whitepapers/sec-rfi-safe-harbor-airdrops-network-tokens>.

⁴⁴ For a more in-depth discussion of these criteria, see: Decentralization Research Center, *Designing Policy for a Flourishing Blockchain Industry* (Feb. 2025), <https://thedrcenter.org/wp-content/uploads/2025/02/DRC-Designing-Policy-Final.pdf>.

blockchain systems are open source, autonomous, permissionless, credibly neutral, economically independent, and distributed. In the case of sales by insiders, additional conditions, discussed in paragraph II directly below, should also be met.

- B. The Commission’s guidance should provide a conditioned path to liquidity for sales by insiders. This guidance could be based on a Rule 144 approach, making clear that sales meeting the conditions are not securities transactions. In particular, such guidance should require that projects satisfy certain current information requirements similar to those found in Rule 144, but reflecting a fit-for-purpose disclosure framework applicable to blockchain systems. In addition, such guidance could identify what activities and influence over a network amount to control, thereby potentially triggering “affiliate” status, again building on the principles found in Rule 144. Doing so could help to restrict persons that exert control over a network token from participating in secondary markets of such a token and limit their ability to act on potential information asymmetries.

Having established such guidance and best practices, the Commission could then focus enforcement efforts on bad actors engaged in manipulative and deceptive practices in violation of the foregoing. In particular, the Enforcement Division could release a formal policy statement outlining a risk-based enforcement strategy, prioritizing cases where:

- Developers retain centralized control while misrepresenting decentralization;
- Tokens are marketed with false profit expectations rather than profit expectations anchored in the programmatic functioning of the network;
- Insiders participate in secondary markets when holding period, control-based decentralization, and current information requirements are not met; and
- Deceptive market practices (wash trading, price manipulation) are present.

Collectively, these measures would create powerful incentives for decentralization, thereby yielding substantial protections for market participants while fostering innovation. In addition, this approach comports with the control-based decentralization framework outlined in Part 3 above: when control is eliminated, the application of securities laws should be limited; but when control is present, their application should conform to traditional (but modernized) approaches. Further, this approach is directionally consistent with the proposed approach in the most recent market structure legislation proposed in Congress.⁴⁵ It is therefore likely to be helpful to ongoing Congressional efforts.

b. *Fit-For-Purpose Registration Pathway*

In tandem with establishing a more clear and effective exempt pathway for network tokens, the Commission should establish a fit-for-purpose registration pathway for primary offerings of network tokens. As discussed above, the application of *Howey* to primary offerings of network tokens is straightforward. Yet people who have conducted or attempted to conduct registered or qualified offerings of network tokens have expressed frustration about the cost and feasibility of registration. Network tokens

⁴⁵ Financial Innovation and Technology for the 21st Century Act, H.R. 4763, 118th Congress (introduced July 20, 2023), <https://www.congress.gov/bill/118th-congress/house-bill/4763>.

and their issuers can differ significantly in some aspects from traditional securities and their issuers. Allowing network token issuers to use appropriately tailored registration regimes may protect investors better than insisting that they use registration forms and mechanisms that are designed for other types of securities offerings. We expect to respond to the Crypto Task Force questions on the creation of such pathway, including **Question #7** in a separate submission.

While Rule 195, the Token Safe Harbor Proposal 2.0, is also worth consideration as a mechanism for accomplishing the Crypto Task Force’s goals with respect to network tokens, we respectfully recommend that the Task Force focus its efforts and priorities on other areas, including the exempt and registration pathways identified above.

The Token Safe Harbor Proposal could provide clarity and facilitate more efficient crypto asset markets. But, it may be more useful to defer the adoption of a safe harbor until a comprehensive modernization of the laws, rules, and regulation that will govern crypto assets occurs. Pending such revisions, token issuers may be reluctant to use a safe harbor given the uncertainty on how federal securities laws may apply to crypto assets, particularly the secondary trading of such assets and the reporting obligations that may ultimately apply to tokens placed under the safe harbor. Further, any such efforts undertaken by the Crypto Task Force to develop and implement the safe harbor could conflict with Congress’s current intention to pass market structure legislation, which we believe is necessary to provide the long-lasting regulatory certainty that entrepreneurs need to invest in building businesses, that investors need to fund such efforts, and that regulators need to effectively oversee those efforts.

We nevertheless expect to respond to the Crypto Task Force questions regarding the token safe harbor proposal, including **Questions #10** through **#14** in a separate submission.

6. Provide Regulatory Clarity for Certain Other Crypto Assets

To further foster innovation while ensuring protection of market participants, the Commission should use guidance and no-action relief to address regulatory uncertainty as it relates to the application of federal securities laws to certain other crypto asset transactions, including transactions of:

- **Asset-Backed Tokens** – Many asset-backed crypto assets may be at risk of being misinterpreted to represent financial instruments other than investment contracts and face additional uncertainty under *Howey*. This regulatory uncertainty can be addressed using a control-based decentralization framework. See our response to **Questions #2, #4** and **#5** for more information.
- **Collectible Tokens** – Like network tokens, collectible tokens face uncertainty under *Howey* that could be resolved by the Commission. See our response to **Question #5** for more information.
- **Company-Backed Tokens** – The use of a control-based decentralization framework makes distinguishing between network tokens and company-backed tokens more objective and principled. The Commission should seek to clarify the respective treatment of such assets under federal securities laws. See our response to **Question #5** for more information.

7. Ensure Consistent Treatment of Comparable Economic Arrangements

A merit- and technology-neutral regulatory framework would treat crypto assets similarly to economically equivalent non-crypto instruments. For regulatory parity, the taxonomy must apply consistent legal treatment across asset classes that share key characteristics. This prevents arbitrary distinctions that advantage legacy financial instruments and commercial transactions while placing an undue burden on blockchain-based alternatives and curtailing technological innovation. We believe the Commission can accomplish this by tailoring guidance, no-action relief, and enforcement efforts to ensure consistent treatment of comparable economic arrangements. Set forth below are several examples.

- **Loyalty Points/Software Licenses/Prepaid Goods vs. Crypto Assets** – Software licenses and prepaid goods or services (such as loyalty points, software subscriptions, gift cards, etc.) are not ordinarily regulated as securities. Many crypto assets provide the same or substantially similar utility, but their regulatory treatment is uncertain. Currently, the Pocket Full of Quarters No-Action Letter, issued in April 2019, is the best guidance the crypto industry has regarding the circumstances under which these types of utility-focused assets are not subject to federal securities laws.⁴⁶ While helpful, the facts on which this letter is based are restrictive. It does not permit interoperability and fails to address legitimate efforts by developers to dampen price volatility. To the extent these narrow facts are viewed as dispositive, developers are dissuaded from giving consumers actual property rights over these types of assets, which they otherwise would have with a gift card in the physical-world. While intended to guard investors, these restrictions are harmful to market participants. Going forward, guidance and no-action relief should provide that crypto assets with bona fide utility characteristics are not subject to securities laws simply because they are transferable or built on blockchain.
- **In-Game Items & Currencies vs. Collectible & Arcade Tokens** – Historically, in-game items and currencies (e.g., CS:GO skins, Fortnite V-Bucks, etc.) have not been regulated as securities because they are primarily designed for consumption rather than investment. However, active and liquid secondary markets for in-game items and currencies have long been available, opening up possibilities for speculation. Further, traditional video game developers now regularly market and sell items and currencies long before they have been developed and released to the public (e.g., “pre-release skins,” “founder packs,” etc.). These transactions are not securities transactions, and developers consummating similar transactions on a blockchain should not face threat of regulatory enforcement. Subjecting blockchain developers to such measures creates regulatory capture for traditional game developers at the expense of consumers. Regulatory frameworks should not impede developers using blockchains and crypto assets to give consumers actual digital property rights over in-game assets and currencies. In that vein, guidance and no-action relief should confirm that in-game items and currencies receive the same treatment as their non-crypto counterparts.
- **Art Sales vs. Collectible Token/NFT Sales** – A person who buys a painting—whether from a gallery, at auction, or directly from an artist—does not enter into a securities transaction,

⁴⁶ See *supra* note 28.

notwithstanding that they may buy, at least in part, hoping that the price of the painting will increase and they can earn a financial gain. Even if the artist endeavors to become prolific, causing the artwork to appreciate in value and enabling the buyer to resell the art for a profit, federal securities laws do not apply to sales of the artist's art. Collectible tokens that represent digital art, music, memorabilia, or collectibles function just like physical art—they are unique assets whose value is driven by cultural trends, subjective demand, and resale markets and the value is driven primarily by supply and demand rather than anything akin to the efforts of a centralized team running a business. If a buyer purchases an NFT artwork from an artist, the transaction is economically identical to purchasing a physical painting. Secondary transactions of such art are even further removed from the applicability of securities laws. Nevertheless, the Commission's enforcement efforts have introduced significant and unwarranted uncertainty regarding the applicability of securities laws to digital art and digital art marketplaces.⁴⁷ Guidance and no-action relief should confirm that such transactions receive the same treatment.

The foregoing regulatory taxonomy provides a way out of the quagmire created by the collision of blockchain technology and federal securities laws. It not only provides a predictable, legally precise, and economically rational approach to determining the security status of many different types of crypto assets under *Howey*, but its core principle—**control-based decentralization**—can be consistently applied to resolve the regulatory uncertainty that persists in a number of other areas, as we discuss in our responses to **Questions #2** through **#5**. Applying a uniform approach has many benefits, including guarding against risks of inconsistencies, confusion, and potential gaps in regulatory coverage that may otherwise be exploited by bad actors. Further, as outlined in our response to **Question #6**, it can achieve all of this while remaining both merit- and technology-neutral.

⁴⁷ Practical Law Finance and Baker Hostetler LLP, *Updated: SEC Push to Regulate NFTs Continues with OpenSea Wells Notice* (Sept. 25, 2024), [https://uk.practicallaw.thomsonreuters.com/w-044-3330?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/w-044-3330?transitionType=Default&contextData=(sc.Default)&firstPage=true).

Question 2: Should the Commission address when crypto assets fall within any category of financial instruments, other than investment contracts, that are specifically listed in the definition of “security” in the federal securities laws?

The Commission should clarify the application of federal securities laws to certain crypto assets that may be at risk of being misinterpreted as representing financial instruments other than investment contracts. The federal definition of “security” includes other categories, such as “profits interests,” “transferable shares,” and “notes,” which, absent guidance, could potentially be misused to classify crypto assets as securities, just as courts and the Commission have previously done with the *Howey* investment contract analysis. Addressing these alternative classifications would provide greater legal certainty and ensure consistency with longstanding interpretations of securities law. This certainty would enable entrepreneurs to invest in building businesses, investors to fund such efforts, and regulators to effectively oversee those efforts, thereby fostering innovation and protecting market participants.

1. Profits Interests & Transferable Shares

Network tokens are crypto assets that are intrinsically linked to, and primarily derive or are expected to primarily derive their value from, the programmatic functioning of a blockchain or smart contract protocol (each, a “blockchain network”). They often confer network rights (e.g., use, profit sharing, governance rights, residual claims on assets) to network tokenholders. For example, following Ethereum Improvement Proposal 1559 (EIP-1559), the Ethereum Network implemented a base fee to be burned for all Ethereum transactions, causing Ethereum’s total ETH issuance rate to be deflationary when transaction volume is high and providing a financial benefit to all ETH holders.⁴⁸ Many blockchains and smart contract protocols also delegate certain authorities to tokenholders via token-based governance.⁴⁹

In various actions and public statements, the Commission has referenced network token economic and governance models as justification for why certain secondary transactions of network tokens satisfy the *Howey* test.⁵⁰ Further, the enforcement efforts have raised concerns that ambiguities in securities laws could potentially be exploited by the Commission to contort network tokens with these features into other categories of securities, namely profits interests and transferable shares. A profits interest generally gives the holder a claim on the earnings or equity appreciation of a business entity, such as a company or partnership. Similarly, a transferable share generally gives the holder an equity-like interest that confers ownership rights in a business entity. Neither of these categories is appropriate for extending the reach of the federal securities laws to encompass network tokens.

As a threshold issue, neither blockchains nor smart contract protocols are business entities. Blockchains are decentralized computers composed of networks of individual computers maintaining shared ledgers—effectively, a “computer in the sky.”⁵¹ Smart contract protocols are self-executing

⁴⁸ See Ethereum Improvement Proposals, *EIP-1559: Fee Market Change for ETH 1.0 Chain* (July 2021), <https://eips.ethereum.org/EIPS/eip-1559>.

⁴⁹ Andrew Hall, *6 Decentralized Governance Trends for 2025*, a16z crypto (Jan. 3, 2025), <https://a16zcrypto.com/posts/article/6-decentralized-governance-trends-for-2025/>.

⁵⁰ See *supra* note 4.

⁵¹ Tim Roughgarden, *Ideal Functionality: A Computer in the Sky*, YouTube (Mar. 7, 2024), https://www.youtube.com/watch?v=l8uRkvrnc_c.

programs stored on blockchains that programmatically function pursuant to their code and a pre-established set of rules. As a result, blockchain networks do not meet any objective interpretation of the definition of a profits interest or transferable share.

But for argument's sake, even if those definitions were interpreted to apply to blockchain networks, the Commission should approach their application consistently with the control-based decentralization framework outlined in Part 3 of our response to **Question #1**. In other words, because blockchain networks can eliminate trust dependencies present with business entities and can operate absent human intervention and control, application of federal securities laws to network tokens should be limited.

A limited approach is particularly suitable under these securities designations, as the granting of network rights to network tokenholders facilitates decentralization (the elimination of control) and provides beneficial protections to market participants. For instance, the granting of voting rights helps to eliminate *voting control* by any single party. In addition, the use of programmatic economic mechanisms to drive monetary value to network tokens via the functioning of a blockchain network increases the *economic independence* of the network token. In other words, it increases reliance on systems that are operated without human control (the network) and reduces *economic control* on systems that are operated with human control (centralized companies). As a result, even in cases where a network token provides economic and governance rights in blockchain or smart contract protocol, and are transferable, such network tokens are not comparable to profits interests or transferable shares.

Nevertheless, the Commission's previous enforcement efforts have created confusion in regard to these categories, which has had the effect of disincentivizing projects from granting such rights to network tokenholders to the detriment of the tokenholders themselves. This in turn has fueled the rise of unproductive assets and assets without intrinsic value, like memecoins, thereby hindering innovation, harming investors, leading to inefficient capital markets, and stifling productive economic activity.⁵² This is the opposite of the approach the Commission should be taking.

For the foregoing reasons, the Commission should issue guidance and no-action relief to clarify that network tokens are not profits interests or transferable shares, and that the provision of network ownership rights to network tokenholders does not increase the likelihood that transactions in a network token will be subject to securities laws.

2. Notes

Asset-backed tokens are crypto assets that primarily derive their value from a claim on, or economic exposure to, one or more underlying assets. They are often autonomously issued by smart contract protocols in response to user-initiated activity. For example, many decentralized finance ("DeFi") protocols, such as DeFi lending protocols and decentralized exchange ("DEX") protocols, autonomously issue crypto assets that function similarly to deposit receipts when a user contributes assets to the protocol (often called "deposit receipt tokens" or "LP tokens"). Similarly, decentralized stablecoin protocols

⁵² Chris Dixon, a16z Crypto, *How bad policy favors memes over matter*, a16z crypto (Apr. 20, 2024), <https://a16zcrypto.com/posts/article/memecoins-tokens-regulation-policy/>.

autonomously issue decentralized stablecoins upon contribution of collateral in a smart contract. In public statements⁵³ and enforcement efforts,⁵⁴ the Commission has indicated that many of these asset-backed tokens have the characteristics of debt instruments and therefore may be “notes” (an enumerated security) and implicate federal securities laws.

Under *Reves v. Ernst & Young*, the court recognized that notes are not securities *per se*, but that they are presumed to be securities unless they bear a strong resemblance to one of the recognized exemptions (e.g., consumer financing, short-term loans, or commercial paper).⁵⁵ In assessing that resemblance, the court outlined four factors: (1) the motivations of the buyer and seller (is the note sold for investment or commercial or consumer purposes); (2) the plan of distributions (how widely is it offered); (3) what are the reasonable expectations of the investing public; and (4) the existence of another regulatory scheme that may already protect investors.

Reves is not suitable for most asset-backed tokens autonomously issued by a smart contract protocol, as the decision was based on an investment relationship that is absent: (a) users interact directly with a smart contract protocol, not with an identifiable issuer or counterparty; and (b) the smart contract protocols are not raising capital for ongoing business operations—they execute transactions according to pre-programmed rules.⁵⁶ As a result, no investment relationship is established, and the contribution of collateral to the smart contract protocol by the user more closely resembles a commercial or consumer purpose. Further, with no person acting as a counterparty, it would be very difficult to argue that a reasonable person would expect their deploying of collateral into a smart contract to be an investment in another person. Given this, the risks inherent in autonomously issued-asset backed tokens are not the same as ordinary notes and federal securities laws should not apply.

However, consistent with the approach we outlined for “network tokens” in Part 5 of our response to **Question #1**, the Commission’s approach in applying *Reves* must be dictated by the function and risk of the deposit receipt tokens or LP tokens issued by the smart contract protocol, focusing on the trust dependencies and the presence of information asymmetries. In particular, where a smart contract protocol is being used to pool investor funds before taking control of them and manually deploying them for investment purposes to generate a return for investors, the risks discussed in *Reves* and intended to be mitigated by federal securities laws may well be present—the person deploying collateral into the smart contract is forming an investment relationship with the person that controls the protocol, even though that relationship is indirect and facilitated via a smart contract.

⁵³ *Oversight of the U.S. Securities and Exchange Commission Before the S. Comm. on Banking, Housing, and Urban Affairs, 116th Cong.* (Sept. 14, 2021) (testimony of SEC Chair Gary Gensler), <https://www.banking.senate.gov/hearings/09/10/2021/oversight-of-the-us-securities-and-exchange-commission>; Caroline A. Crenshaw, SEC Comm’r, *Digital Asset Securities – Common Goals and a Bridge to Better Outcomes* (Oct. 12, 2021), <https://www.sec.gov/news/speech/crenshaw-sec-speaks-20211012>; Gurbir Grewal, Director of SEC Division of Enforcement, *2021 SEC Regulation Outside the United States – Scott Friestad Memorial Keynote Address* (Nov. 8, 2021), <https://www.sec.gov/news/speech/grewal-regulation-outside-united-states-110821>.

⁵⁴ *In re Blockchain Credit Partners d/b/a DeFi Money Market*, Securities and Exchange Commission File No. 3-20453 (Aug. 6, 2021), <https://www.sec.gov/litigation/admin/2021/33-10961.pdf>.

⁵⁵ *Reves v. Ernst & Young*, 494 U.S. 56 (1990)

⁵⁶ Peter Davis, Benjamin Naftalis & Douglas Yatter, *The Limits of Applying Reves v. Ernst & Young to DeFi and the Perils of Regulating Web3 by Enforcement*, JD Supra (Jan. 26, 2022), <https://www.jdsupra.com/legalnews/the-limits-of-applying-reves-v-ernst-5896777/>.

On the other hand, a decentralized smart contract protocol that is not *operationally controlled*, i.e., one that is autonomous, permissionless, credibly neutral, and non-custodial, does not give rise to the same risks. Further, the elimination of operational control increases the likelihood that the asset-backed token is *economically independent*—the economic mechanisms that drive value to the crypto asset are derived from the underlying asset and protocol’s operation, not dependent on any development company or issuer. The satisfaction of such criteria ensures that the protocol is not only disintermediated, but also that relevant information (verifiable collateral, rewards, smart contract functioning, governance) is publicly available onchain.

Given the foregoing, the Commission should adopt a control-based decentralization framework (as described in Part 3 of our response to **Question #1**) for purposes of assessing the applicability of *Reves* to asset-backed tokens for the same reasons that should adopt such a framework for assessing the applicability of *Howey* to network tokens (as described in Part 5 of our response to **Question #1**)—when control is eliminated, the application of securities laws should be limited; and when control is present, their application should conform to traditional (but modernized approaches).

Using a control-based decentralization framework, the Commission should therefore direct guidance, no-action relief, and enforcement efforts to clarify that asset-backed tokens autonomously issued by smart contract protocols are not “notes” under *Reves* or otherwise subject to the federal securities laws. For a comprehensive discussion of what a control-based decentralization framework for asset-backed tokens may entail, see our response to **Question #4**.

Question 3: Certain crypto assets are used in a variety of functions inherent to the operation of a blockchain network, such as mining or staking as part of a consensus mechanism or securing the network, validating transactions or other related activities on the network, and paying transaction or other fees on the network. These technology functions may be conducted directly or indirectly, such as through third-party service providers. What types of technology functions are inherent to the operation of a blockchain network? Should the Commission address the status of technology functions under the federal securities laws and, if so, what issues should be addressed?

The Commission should address and provide guidance on the specific network participants and functional technologies that fall outside of the broker, dealer, and exchange registration regimes, which would help provide market participants with increased certainty when establishing businesses or operating in new areas of the blockchain ecosystem.

The categories of participants and technologies that should, in general, fall outside of the scope of the registration regimes under the federal securities laws (the “Exempt Technologies”) include various blockchain network participants, including those that engage in technological functions inherent to the operation of a blockchain network.⁵⁷ In addition, participants and technologies that are analogous to those blockchain network participants should be similarly and contemporaneously addressed by the Commission, including smart contract protocols, front-end interfaces, and self-hosted wallets. These include nearly every participant and technology that facilitates user transactions on a blockchain network, thereby providing a comprehensive foundation to assess the application of federal securities laws.

Importantly, the Exempt Technologies do not give rise to the risks that the broker, dealer, and exchange registration regimes of federal securities laws are intended to address. In particular, the Exempt Technologies typically never have the ability to exercise control over a transaction or user assets, enabling truly disintermediated peer-to-peer transactions. Because they eliminate control-related trust dependencies, proposed market structure legislation provides for the exemption of the Exempt Technologies where certain criteria are met.⁵⁸ Similarly, the application of federal securities laws to the Exempt Technologies should be limited, and we urge the Commission to provide comprehensive guidance confirming this.

To aid in this effort, in Part 1 of this response we provide background information on the Exempt Technologies. In Part 2, we explain how the Commission should harness the case law and legal arguments that have already addressed and rejected the application of the registration regimes to certain Exempt Technologies, demonstrating how these legal principles can apply to all of the Exempt Technologies. In Part 3, we propose that the Commission adopt a control-based decentralization framework (as introduced in our response to **Question #1**) to ensure that where control-related trust dependencies are relevant to the functioning of an Exempt Technology, the risks that federal securities laws are intended to address are eliminated via decentralization.

⁵⁷ For sake of clarity, in this section we refer to “blockchain networks” and “smart contract protocols” separately, whereas in the rest of our response we refer to both collectively as “blockchain networks.”

⁵⁸ Financial Innovation and Technology for the 21st Century Act, H.R. 4763, 118th Congress (introduced July 20, 2023), <https://www.congress.gov/bill/118th-congress/house-bill/4763>.

1. Background on the Exempt Technologies

The technological functions we believe are relevant to the Commission’s inquiry include:⁵⁹

- **Blockchain networks** – A blockchain is a decentralized computer composed of a network of individual computers maintaining shared ledgers, which record and verify data across the entire network. The ordered records, also referred to as blocks, are linked together using cryptography. In many instances, the process of ordering and validating blocks is divided into specialized roles performed by “**blockchain network participants**.” The first step is the collection of transactions and bundling them together, which “**searchers**” perform. Then the searchers submit the bundled transactions to “**builders**” who construct the blocks. Following construction of the blocks, “**validators**” verify the transactions and add them to the blockchain network. In some instances, “**mining pool operators**” or “**staking pool operators**” allow multiple participants to pool their tokens together to participate in the validation process. When “blockchain rollups,” i.e. “Layer-2 scaling solutions”⁶⁰ are implicated, “**sequencers**” act similarly to builders and are responsible for ordering and processing transactions on those networks.⁶¹
- **Relayers** – Relayers are network participants that help facilitate offchain order discovery and communication for onchain execution. In some decentralized finance (“DeFi”) protocols, particularly order book-based DEXs, or cross-chain bridges, relayers aggregate trade requests, match counterparties, and broadcast signed transactions to the blockchain for finalization by smart contracts. Relayers do not take custody of user funds or execute trades themselves—they merely facilitate transaction routing in a non-custodial manner.
- **Remote Procedure Call nodes** – Remote Procedure Call (“RPC”) nodes serve as the communication bridge between users and blockchain networks. They allow wallets, DApps, and front-end interfaces to query blockchain data, submit transactions, and interact with smart contracts. Although RPC nodes facilitate blockchain access, they do not control transactions or alter blockchain data, making them analogous to ISPs in traditional web infrastructure.
- **Smart contract protocols** – A smart contract is a self-executing program stored on a blockchain that programmatically functions pursuant to its code and a pre-established set of rules. Collections of smart contracts (often called “smart contracts protocols”) enable the creation of decentralized applications (or “DApps”) that greatly enhance the functionality of blockchains. The Commission has previously indicated that certain smart contract protocols and DApps may be implicated under

⁵⁹ For a more robust, technical description of the transaction execution flow and each technological function, see Rebecca Rettig, Michael Mosier & Katja Gilam, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance* (Jan. 29, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4607332

⁶⁰ *What are "Rollups" in crypto?*, Coinbase, <https://www.coinbase.com/learn/wallet/what-are-rollups-in-crypto>.

⁶¹ See Dan Robinson, Amy Aixi Zhang & Rodrigo Seira, *Base Layer Neutrality*, Paradigm (Feb. 8, 2022), <https://www.paradigm.xyz/2022/09/base-layer-neutrality>.

securities laws because they may facilitate transactions in crypto assets that are alleged to be securities.⁶² In particular:

- ***Decentralized exchange protocols*** – Decentralized exchange protocols (“DEXs”) are DApps that enable users to engage in peer-to-peer transactions in crypto assets without use of an intermediary. Buyers and sellers are not matched on a one-to-one basis before a trade occurs, and smart contracts automatically enforce the parties’ arrangement by self-executing transactions under set conditions and posting the completed transactions to the blockchain. Crypto assets are paired and locked in a DEX’s liquidity pool smart contract, and users can interact with the pool to swap tokens in an automatic and permissionless manner.⁶³ The pools are entirely transparent with respect to their available assets and prices at all times, and use a mathematical algorithm built into the pool’s smart contract, known as an automated market maker (“AMM”), to price the assets in the pool based on supply and demand. To incentivize users to contribute tokens to the pool, “**liquidity providers**” receive passive income when they place their crypto assets into these pools. Importantly, liquidity pools obviate the need for third-party middlemen that would normally serve as market makers in traditional markets, and therefore, they are essential to the functioning of a DEX.
- ***NFT marketplace protocols*** – Non-Fungible Token (“NFT”) marketplace protocols are DApps that enable users to buy, sell, and trade collectible tokens that are digital representations of a work of art, musical composition, literary work, etc. (often just called “NFTs”) directly with one another, without relying on an intermediary. Unlike traditional marketplaces that rely on centralized gatekeepers, smart contracts autonomously facilitate transactions, ensuring that buyers receive NFTs and sellers receive payment without requiring trust in a third party. When a user lists an NFT for sale, the NFT is typically held in escrow by the marketplace’s smart contract or remains in the seller’s wallet until a buyer meets the listed price. Once a purchase is initiated, the smart contract automatically executes the transaction, transferring the NFT to the buyer and the payment (in crypto assets) to the seller. Some NFT marketplace protocols also incorporate auction mechanisms, where users submit bids, and the highest bid at the end of a predetermined period triggers the smart contract to finalize the sale. Because NFT marketplace smart contracts remove the need for centralized platforms to facilitate transactions, enforce agreements, or mediate disputes, they enable direct peer-to-peer commerce in crypto assets while maintaining full transparency and security.
- **Front-end interfaces & applications** – Users of DApps typically access them via custom front-end interfaces (such as a website), or applications that passively provide information to users about the DApps and enable them to interact with the DApps smart contracts. In response to directions and inputs from a user, an application can autonomously generate a message for a

⁶² Uniswap Labs, *Wells Submission on Behalf of Uniswap Labs* (May 21, 2024), <https://blog.uniswap.org/wells-notice-response.pdf>.

⁶³ Uniswap Labs, *What is a liquidity pool?*, <https://support.uniswap.org/hc/en-us/articles/8829880740109-What-is-a-liquidity-pool>.

user’s self-hosted wallet to send to a DApp, which, as described above, results in smart contracts automatically enforcing the transaction and posting it on the blockchain. In many cases, self-hosted wallets have their own embedded front-end interfaces and applications for interacting with DApps, blurring the lines between what constitutes a front-end and wallet. Custom front-end interfaces and applications for DEXs sometimes utilize an offchain computational algorithm (referred to as a “**Solver**” or “**Router**”) to determine the best route for trades via the DEX’s smart contracts. Custom front-end interfaces and applications are not required for users to interact with decentralized protocols; users with technical expertise can circumvent applications and interact with protocols directly.

- **Self-hosted (non-custodial) wallets** – Self-hosted wallets are a type of software or hardware that enable users to store and access their crypto assets on their own computers or mobile devices by allowing them to sign and send cryptographic messages to blockchains. With a self-hosted wallet, users are able to hold their private keys and crypto assets, as well as send and receive crypto assets in a peer-to-peer manner. The software provider of a self-hosted wallet can neither access the user’s private keys or assert control over the user’s crypto assets. Individuals typically use self-hosted wallet software applications as a convenient way to interact with blockchain networks and DApps, similarly to how web users tend to use web browsers to access the internet. Self-hosted wallets sometimes also provide links to or incorporate functionality of DApps, enabling users to directly swap, bridge, and engage in other functions directly from their wallet without the presence of intermediaries.⁶⁴ (Note: hosted or custodial wallets, unlike self-hosted wallets, may allow third parties to exercise total independent control over a user’s assets, and therefore, are not addressed in this paragraph or otherwise in this response).

2. Case Law & Analysis

Courts have already rejected attempts to impose registration requirements on certain Exempt Technologies. While the courts have not had occasion to consider each of the categories, the reasoning behind the decisions applies more broadly across other blockchain technologies. In addition, industry participants have responded to many of the Commission’s previously proposed rules with comments that support this position, which we describe below.

a. *Broker & Dealer Registration Regimes*

The Securities Exchange Act of 1934 (“Exchange Act”) defines “brokers” to include, “any person engaged in the business of effecting transactions in securities for the account of *others*.”⁶⁵ The Exchange Act defines “dealers” to include “any person engaged in the business of buying and selling securities. . . for such person’s *own account* through a broker or otherwise.”⁶⁶ Whether an entity acts as a broker or dealer is facts-specific, and courts consider the numerous factors, e.g., soliciting investors, accepting, or routing

⁶⁴ These functionalities can be accomplished through direct API connectivity to a protocol, so that no transaction messaging is routed through the wallet provider. These functionalities allow users to access information transmitted through the protocol and to transmit such information on their own, rather than participating in the investment decision or order processing.

⁶⁵ 15 U.S. Code § 78c(a)(4) (emphasis added).

⁶⁶ 15 U.S.C. § 78c(a)(5)(A) (emphasis added).

orders, processing documents relating to the sale of securities, making valuations, and others, in making the assessment.⁶⁷

The following case law has addressed these regimes as applied to the Exempt Technologies:

- **SEC v. Coinbase** – Judge Failla considered and rejected the application of the broker regime to Coinbase’s self-hosted wallet.⁶⁸ She reasoned that the Commission not allege that Coinbase had engaged in many traditional broker activities—it did not negotiate terms for transactions, make investment recommendations, arrange financing, hold customer funds, process trade documentation, or conduct independent asset valuations;⁶⁹ she noted that Coinbase never had control over a user’s crypto assets or transactions; she disagreed with the Commission’s characterization that the wallet provided routing activities;⁷⁰ and she held that receiving a commission did not, on its own, turn Coinbase into a broker. While such finding departs from the Commission’s historical emphasis on transaction-based compensation, it was reasonable given that there was no accompanying solicitation or other broker-related activity that might give rise to conflicts of interest.⁷¹
- **Risley v. Universal Navigation** – Judge Failla also addressed questions about potential liability arising from the misuse of blockchain technology by bad actors and the potential liability of developers in a class action lawsuit against Uniswap Labs and others. In that case, she was not required to opine on whether the user front-end interface developed and operated by Uniswap Labs that provides access to the Uniswap DEX constituted a “broker” or an “exchange,” but her

⁶⁷ In the Commission’s enforcement action against Coinbase, Judge Failla noted that courts typically consider the following factors in determining whether an entity is acting as a broker, including whether it: (1) actively solicits investors; (2) receives transaction-based compensation; (3) handles securities or funds of others in connection with securities transactions; (4) processes documents related to the sale of securities; (5) participates in the order-taking or order-routing process; (6) sells, or previously sold, securities of other issuers; (7) is an employee of the issuer; (8) is involved in negotiations between the issuer and the investor; and/or (9) makes valuations as to the merits of the investment or gives advice. *SEC v. Coinbase Inc. et al.*, 726 F. Supp. 3d 260, 305 (S.D.N.Y. Mar. 27, 2024) (citing *SEC v. GEL Direct Tr.*, No. 22-cv-9803, 2023 WL 3166421, at *2 (S.D.N.Y. Apr. 28, 2023).

⁶⁸ *Id.*

⁶⁹ *Id.*, at 306.

⁷⁰ *Id.* (“As alleged, Coinbase’s participation in the order-routing process is minimal. While Wallet “provide[s] access to or link[s] to third-party services, such as DEXs” ... the SEC does not allege that Coinbase performs any key trading functions on behalf of its users in connection with those activities.”).

⁷¹ *Id.*, at 307. See also Miles Jennings & Brian Quintenz, *Case studies for “Grading recent actions: How the SEC, CFTC, and the courts measure up,”* a16z crypto (Oct. 26, 2023), <https://a16zcrypto.com/posts/article/case-studies-for-grading-recent-actions-how-the-sec-cftc-and-the-courts-measure-up/>. As we discussed prior to the issuance of Judge Failla’s opinion, transaction-based compensation is often referred to by the SEC as the hallmark of broker activity. However, the SEC’s own stated policy rationale for the broker registration requirements of the Exchange Act fails to justify applying that position broadly to self-hosted wallets, like Coinbase Wallet. In particular, the Commission’s policy rationale is often referred to the ‘salesmen’s stake’ conflict of interest, but that sort of conflict does not generally exist for self-hosted wallets. Although self-hosted wallets may receive fees, as Coinbase allegedly did, which would technically constitute ‘transaction-based compensation’, the salesmen’s stake conflict does not arise where there is no solicitation for investment or recommendation for purchases or sales. While self-hosted wallet providers, like Coinbase, do make more money if people engage in more transactions, the conflict of interest is no different than that of any counterparty or service provider in any sort of business arrangement.

reasoning, which heavily emphasized that the smart contract protocol constituted a general purpose tool rather than a controlled service offering from Uniswaps labs, suggests she would have rejected such allegations in any event.⁷² The plaintiffs had attempted to hold Uniswap Labs and others liable for losses that they sustained trading certain tokens on the Uniswap DEX. Judge Failla dismissed the claims, reasoning that the harm arose from third parties, rather than the underlying Uniswap platform. Notably, she compared the plaintiffs’ lawsuit to “an effort to hold a developer of self-driving cars liable for a third party’s use of the car to commit a traffic violation or to rob a bank . . . In those circumstances, one would not sue the car company for facilitating the wrongdoing; they would sue the individual who committed the wrong.”⁷³ The Second Circuit largely affirmed Judge Failla’s dismissal of the class action.⁷⁴

- **Crypto Freedom Alliance of Texas v. SEC** – Although the courts have not had occasion to directly opine on the application of the dealer registration regime to the Exempt Technologies, an industry case that challenged—and led to the overturning of—a rule that the Commission proposed to expand the definition of dealer provides guidance on the application (or lack thereof) of the dealer regime to participants in DEX liquidity pools.⁷⁵ The Commission had proposed an expansion of the definition of dealer, which would have captured anyone engaging in trading activities that had the effect of providing market liquidity as a dealer, potentially including decentralized software that facilitates market-making (like an AMM), traders, developers and other entities and activities that may not have been able to comply with registration and reporting, like the liquidity pool participants described above. Judge O’Connor overturned the proposed expansion, holding that the Commission’s rule was arbitrary and capricious and would have rendered the Exchange Act’s longstanding distinction between “dealer” and “trader” (i.e., someone who buys and sells securities for their own account *not* as a regular business) void. Based on the judge’s explicit rejection of the Commission’s attempt to broaden the scope of the dealer registration regime, the judge implicitly rejected the inclusion of participants in liquidity pools within its original scope. The Commission recently moved to dismiss its appeal of the case.⁷⁶

Despite these rulings, given the Commission’s enforcement efforts with respect to DeFi and front-end interfaces and its attempts to expand the dealer registration regime, there remains significant uncertainty about the Commission’s intentions to apply broker and/or dealer registration requirements to the Exempt Technologies. As a result, the Commission should use the reasoning in these cases to provide interpretive guidance, no-action relief, and exemptive relief to resolve lingering regulatory uncertainty, clearly excluding the Exempted Technologies from the registration requirements for brokers and dealers (subject to certain decentralization requirements discussed below).

⁷² *Risley v. Universal Navigation Inc. et al*, 690 F. Supp. 3d 195 (S.D.N.Y. 2023) (“...“it defies logic that a drafter of computer code underlying a particular software platform could be liable under Section 29(b) for a third-party’s misuse of that platform.”).

⁷³ *Id.*, at 217.

⁷⁴ *Risley v. Universal Navigation Inc. et al*, No. 23-cv-1340 (2d Cir. Feb. 26, 2025) (Summary Order).

⁷⁵ *Crypto Freedom Alliance of Texas v. SEC*, 2024 WL 4858590 (N.D. Tex. Nov. 21, 2024).

⁷⁶ Order, *Crypto Freedom Alliance of Texas v. SEC*, No. 4:24-cv-00361 (N.D. Tex. Feb. 20, 2025), ECF No. 57.

Although Judge Failla’s decisions only directly speak to the application of the broker regime to self-hosted wallets (and, in particular, Coinbase’s self-hosted wallet and the front-end interface it provided users for purposes of engaging in swaps), her principled analysis—which draws a sharp distinction between systems that can operate absent human intervention and control, and those that depend on intermediaries—is consistent with the core principle that when control is absent, the application of federal securities laws should be limited. Judge O’Connor did the same insofar as he restrained the Commission’s rulemaking authority to actual traditional financial intermediaries, rather than participants in autonomous software protocols. This reasoning can and should be read more broadly to apply across the Exempted Technologies:

- ***Applicability to Blockchain Network Participants*** – The above case law is most naturally read to exclude blockchain network participants from the broker and dealer registration regimes. As described above, blockchain network participants take part in the public recording of the order of data blocks at the blockchain network. Because their activities resemble participants in existing communications infrastructure, they are the furthest removed from the trading activities of individual users, and almost certainly fall outside of all of the factors that courts consider when assessing broker status. Searchers, builders, validators, and sequencers do not solicit investors, and likely do not have any contact or personal knowledge of the users transacting on blockchain networks; they are *non-custodial* and do not control user funds; they do not process documents, make valuations, or engage in almost any other conduct that would suggest broker or dealer activities. Not even the transaction-based compensation factor, which Judge Failla acknowledged provided some support to the Commission’s allegation that Coinbase acted as a broker through its self-hosted wallet, applies to blockchain network participants, given that they receive compensation which is pre-determined according to the source code of the network, is distributed by the network itself, and is not transaction based.⁷⁷ As a result, the most plausible reading of the case law is that the broker and dealer regimes do not extend to blockchain network participants.⁷⁸
- ***Applicability to Relayers and RPC Nodes*** – Similarly to blockchain network participants, relayers and RPC nodes do not take custody of user funds and merely facilitate user interactions with a blockchain. As a result, relayers and RPC nodes both function more like traditional web infrastructure and do not implicate the broker and dealer regimes.

⁷⁷ *Proof-of-stake rewards and penalties*, Ethereum, <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/> (last edited Nov. 23, 2024).

⁷⁸ International regulators have also recognized the importance of regulatory neutrality in regard to blockchain network participants. For example, the European Securities and Markets Authority recently shared its view that miners, validators, searchers, and builders not be considered “persons professionally arranging or executing transactions” in cryptoassets under the Markets in Crypto-Assets Regulation for the purposes of the prevention and detection of market abuse. *See* European Securities and Markets Authority, Final Report: Draft technical Standards specifying certain requirements in relation to the detection and prevention of market abuse under the Markets in Crypto Assets Regulation (MiCA) (Dec. 17, 2024), https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75-453128700-1278_Final_Report_STOR_MiCA_Article_92_2_pdf.

- ***Applicability to Smart Contract Protocols*** – A natural reading of Judge Failla’s and Judge O’Connor’s opinions should also extend to smart contract protocols, like DEXs and NFT marketplaces. Smart contract protocols replace traditional intermediaries with autonomous, self-executing algorithms, eliminating both the risks posed by intermediaries and the justification for applying broker-dealer regulation. In addition, smart contract protocols, like blockchain network participants, do not come close to meeting the facts and circumstances that are typical of brokers and dealers, exhibiting few, if any, of those characteristics. The basic reasoning that underlies the registration regimes also weighs in favor of not applying the registration regimes to smart contract protocols—these regimes reflect Congress’s goal of regulating the conduct of actual financial intermediaries, a goal that cannot be attained by extending the broker and dealer regulations to cover decentralized systems that can operate absent human intervention and control.
- ***Applicability to Front-End Interfaces & Wallets*** – Front-end interfaces are the most analogous of the Exempt Technologies to the particular functionalities specifically addressed in the case law. Specifically, front-end interfaces are a broad category of software tools that includes self-hosted wallet application front-ends where they facilitate user activity on DeFi, like Coinbase Wallet. As explained above, Judge Failla determined that providing free software in the form of Coinbase Wallet did not subject Coinbase to broker registration requirements as a matter of law, and although her analysis was necessarily fact specific, much of it can be used to inform the parameters of Commission’s guidance on this issue. As Judge Failla recognized, Coinbase Wallet simply provides a user interface and technical connection to third-party platforms. Importantly, the centralized development teams at Coinbase that control the wallet interface are tasked with maintaining the UX/UI features of the interface and other typical programming functions—not any of the key functions that brokers typically tend to perform on behalf of their customers. Other front-end interface providers in the blockchain ecosystem generally operate in the same manner, except rather than providing access to a user’s crypto assets, as is the case with Coinbase Wallet, those front-end interfaces provide users with an array of other functionalities. Further, self-hosted wallets that do not have embedded DeFi functionality within them (e.g., ability for a user to submit order instructions to a DEX), similarly do not take custody of user funds or implicate the broker and dealer regimes because they merely act as a way for a user to maintain their assets, and do not perform any of the activities that are indicative of brokerage activity.

However, it is important to qualify the foregoing by noting that not every instance of an Exempted Technology will have identical function and risk—blockchain technology only ameliorates trust dependencies inherent with intermediaries when they are decentralized. As a result, any guidance clarifying under what conditions the Exempted Technologies may be exempt should apply a control-based decentralization framework, as discussed below in Part 3.

Further, it is important to acknowledge that front-end interfaces are inherently centralized—centralized businesses operate and control them. Nevertheless, even where such front-ends and applications remain non-custodial, it is plausible that certain front-ends could engage in activities and provide services that implicate the risks the broker and dealer registration regimes were intended to

address, including actively soliciting investors and specific investments, while collecting transaction based compensation. For example, where they introduce intermediary-based risks that are ordinarily addressed by the broker or dealer registration regime (such as those arising from conflicts of interest), some form of targeted regulation may be appropriate. On the other hand, where they are merely passive information services that facilitate peer-to-peer transactions, they are unlikely to introduce intermediary-based risks even where they collect transaction-based compensation.

Given the significant number of factors relevant to the foregoing analysis and the novel functioning of blockchain technology, it is critically important for the Commission to provide interpretive guidance, no-action relief, and exemptive relief to clarify what type of front-end interfaces may be subject to broker and/or dealer registration requirements. Such guidance should be consistent with existing case law and historical precedent,⁷⁹ but give significant weight to the fact that the disintermediated infrastructure such front-end interfaces provide access to eliminate trust-dependencies far better than any regulatory regime applicable to intermediaries could ever hope to achieve.

b. *Exchange Registration Regime*

The Commission adopted Regulation ATS in 1998 to develop an alternative regulatory scheme so that new electronic communication networks and alternative trading systems could operate through enhanced broker-dealer registration and Commission oversight without incurring the costs associated with registering as national securities exchanges.⁸⁰ Exchange Act Rule 3b-16, adopted at the same time as Regulation ATS, defines an “exchange” as any organization, association, or group of persons that “brings together the orders for securities of multiple buyers and sellers” and “uses established, non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of the trade.”

The federal courts have not had an opportunity to consider the application of the registration regime for exchanges to the Exempt Technologies. However, in 2022, the Commission proposed amendments to Exchange Act Rule 3b-16 to expand the definition of “exchange” in a manner that may implicate the Exempt Technologies. Under the proposed rule, an “exchange” would have included any organization, association or group of persons that “brings together buyers and sellers of securities using trading interest” and “*makes available* established, non-discretionary methods (whether by providing a

⁷⁹ The Commission has previously issued “No Action Letters” finding activities that are similar to the functionalities that self-hosted wallets provide to be outside the bounds of broker regulations when certain conditions are satisfied. For example, the SEC Staff has issued guidance agreeing that “Finders,” “Internet Portals,” and “Online Bulletin Boards” platforms fall outside of the broker regime even though they facilitated offers and sales of securities. One of the key conditions to these no-action positions is the presence of transaction-based compensation, the presence of which generally gives rise to potential conflicts of interest because the platforms are all operated and controlled by their creators. However, because transaction-based compensation on trades initiated through self-hosted wallets do not give rise to conflicts of interest, passive information front-end interfaces and self-hosted wallet functionalities should not be considered broker activity.

⁸⁰ The Exchange Act defines the term “exchange” to include “any organization, association, or group of persons, whether incorporated or unincorporated, which constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange as that term is generally understood...” 15 U.S. Code § 78c(a)(1).

trading facility or *communication protocols*, or by setting rules) under which buyers and sellers can interact and agree to the terms of a trade.”⁸¹ The proposed rule included a new term—“Communication Protocol Systems”—to describe the entities that offer communication protocols and the use of non-firm trading interest to bring together buyers and sellers of securities. When the proposed rule was first published, it did not explicitly mention crypto assets and there was no analysis of the economic impact that it might have on the blockchain ecosystem, but the Commission re-opened the rule for comment in 2023 and solicited comments specific to blockchain technology.⁸²

Numerous concerns were raised in response to the Commission’s proposal, many of which are similar to the points discussed above regarding the inapplicability of the broker-dealer regime to the Exempt Technologies.⁸³ In response to those submissions, the Commission should withdraw the rule as it applies to Exempt Technologies and should not consider any of the Exempt Technologies to fall within the scope of the exchange registration regime under federal securities laws. Further, the Commission should use interpretive guidance, no-action relief,⁸⁴ and exemptive relief to clarify that the Exempt Technologies are not subject to exchange registration requirements (subject to certain decentralization requirements discussed below)—the fact that the Commission felt the need to broaden the definition of exchange appears like an implicit admission that it recognized its lack of authority over the Exempt Technologies.⁸⁵

- ***Applicability to Blockchain Network Participants, Relayers & RPC Nodes*** – Many of the Exempt Technologies, including blockchain network participants, liquidity participants, relayers, and RPC nodes, do not engage in any activities that bear a resemblance to traditional exchange-like functions, and therefore, clearly do not meet the exchange definition on their face.

⁸¹ 87 Fed. Reg. at 15,646 (emphasis added).

⁸² Release No. 34-97309 (Apr. 14, 2023), 88 Fed. Reg. 29,488 (May 5, 2023). The Commission has not finalized the rule to date.

⁸³ We submitted a comment responding to the Commission’s proposed rule as well. See Jai Ramaswamy & Miles Jennings, Letter to the Commission: Amendments Regarding the Definition of “Exchange” and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities, a16z crypto (Apr. 18, 2022), <https://a16z.com/a16z-cryptos-comment-on-sec-exchange-act-proposal/>.

⁸⁴ The Commission previously issued no-action letters stating that persons who operate passive electronic bulletin boards capable of bringing together buyers and sellers of securities, but that do not use such established, non-discretionary methods under which firm orders interact, should not be required to register as national securities exchanges or brokers/ATS. These letters provided narrow relief, and the Commission announced in 1996 that it would no longer respond to requests for no-action assurance with respect to bulletin board systems, unless they present novel or unusual issues. But given the significant technological innovations and structural market reforms since then, the Commission should consider issuing guidance or expanding these no-action letters to cover other types of systems that bring together buyers and sellers and allow them to communicate regarding securities transactions.

⁸⁵ Indeed, in a recent speech, SEC Acting Chair Mark T. Uyeda discussed the proposed expansion of definition of exchange to include “communications protocols.” He stated that, in his view, “it was a mistake for the Commission to link together regulation of the Treasury markets with a heavy-handed attempt to tamp down the crypto market,” and that he asked SEC staff for “options on abandoning that part of the proposal.” Mark T. Uyeda, SEC Comm’r, Remarks to the 2025 Annual Washington Conference of the Institute of International Bankers (March 10, 2025), <https://www.sec.gov/newsroom/speeches-statements/uyeda-remarks-institute-international-bankers-031025>.

- ***Applicability to Smart Contract Protocols*** – As explained above, by nature of their functioning, smart contract protocols replace traditional intermediaries with autonomous, self-executing algorithms, eliminating both the risks posed by intermediaries. Application of exchange regulations to them would not make sense, given that they enable peer-to-peer trading (as opposed to bringing together buyers and sellers and matching orders). Further, autonomous smart contract protocols cannot comply with subjective regulatory requirements, let alone exchange registration and the requirements of Regulation ATS, without reconstituting themselves as traditional financial intermediaries. The same reasoning also applies to smart contracts relating to automated market makers. These contracts are typically publicly available on the blockchain and transactions are automatically settled onchain. Importantly, the developer of the smart contract does not have any discretion regarding the transaction and how it is structured, and firm orders from buyers and sellers are not matched.
- ***Applicability to Front-End Interfaces & Wallets*** – While centralized entities typically exert control over front-end interfaces (and self-hosted wallets that act as a front-end to DeFi), Regulation ATS should also not apply to them. Like smart contract protocols, front-end interfaces and wallets do not exercise discretion over transactions or structure them, and users engage on a peer-to-peer basis through sharing bids, offers, and other trading interests, which undermines the application of Regulation ATS to them.

However, as with the broker-dealer regimes discussed above, it is important to similarly qualify the foregoing by noting that not every instance of an Exempt Technology will have identical function and risk. Where blockchain technologies are not disintermediated, the exchange registration regime under federal securities laws could be implicated. As a result, any guidance clarifying under what conditions the Exempt Technologies may be exempt should apply a control-based decentralization framework, as discussed below in Part 3.

3. Control-Based Decentralization Framework For Certain Exempt Technologies

As noted above, the Exempt Technologies are not one-size-fits-all categories, and they may be developed and structured in different ways. As a result, the Commission must analyze their function and risk. In particular, where blockchain networks and smart contract protocols are controlled, they could potentially expose users of those systems to the very intermediary-based risks that the broker, dealer, and exchange registration regimes under federal securities laws are intended to address. Consequently, when providing interpretive guidance, no-action relief, and exemptive relief regarding the applicability of such regimes to the Exempt Technologies, the Commission should include as “Exempt Technologies” those blockchain networks and smart contract protocols that are not subject to control-related trust dependencies.⁸⁶ This supports the establishment and use of a control-based decentralization framework.

⁸⁶ If the list of technologies and participants included as Exempt Technologies is too broad or permissive, businesses using blockchain networks or smart contract protocols that enable them to function as traditional financial intermediaries could simply evade the federal securities laws, even if they engage in what properly are considered regulated activities involving securities, by structuring their operations to seek to take advantage of the outer edges of potential Commission guidance on this matter in circumvention of the federal securities laws. On the other hand, if the list is too restrictive, blockchain networks and smart contract protocols that *do not* present or that otherwise *do* mitigate the risks securities laws are intended to address could be precluded from operating.

As discussed in Part 3 of our response to **Question #1**, a control-based decentralization framework should be tailored to the risks federal securities laws are intended to address. The broker, dealer, and exchange registration regimes are primarily intended to mitigate risks arising from intermediaries. In order for a blockchain network or smart contract protocol to successfully mitigate the intermediary-related risks that securities laws are intended to address, they must only eliminate *operational control* (*economic control* or *voting control* are less relevant for the reasons discussed below) by any person or group of persons under common control—i.e., the kind of control that is at the root of the risks that the federal securities laws were designed to regulate. Unless the blockchain network or smart contract protocol is autonomous, permissionless, credibly neutral, and non-custodial, the following risks could be present:

- If a system is not yet **autonomous**, a user can be exposed to risks stemming from the manual performance of operations, the potential for unilateral changes to the system’s functioning such that transactions are executed in unforeseen ways, and the risks of potential mistakes in calculation or data storage.
- If a system is not yet **permissionless** and **credibly neutral**, a controlling party could potentially cut-off a user’s access to the system, resulting in a loss of funds.
- If a system is **custodial**, the user is exposed to various intermediary-related risks, including loss of funds.

However, where such criteria are satisfied, a blockchain network or smart contract protocol will be effectively disintermediated—no one has *operational control*—eliminating the risks that securities laws are designed to alleviate. Of these criteria, non-custodial is the most critical, as this ensures that a user maintains control of their crypto assets and is therefore not exposed to custody risks based on the agency and behavior of an intermediary.⁸⁷

The other decentralization criteria outlined in our response to **Question #1** (open source, distributed, and economically independent) are less relevant, given that conflicts of interest risks and other intermediary-related risks are unlikely to arise even where these criteria are not satisfied. For example, in the context of a DEX that meets the decentralization criteria above, whether the system is open source or whether it is economically independent are not relevant to the risks a user encounters—neither impacts whether transactions through the DEX are disintermediated. Even if a person were to own 100% of the total outstanding token supply, such that the DEX was not “distributed,” the fact that the owner could not unilaterally impact the protocols autonomy, permissionlessness, credible neutrality, or non-custodial nature (which by definition must be true if those criteria are met), means that the owner cannot unilaterally subject users to unforeseen risks that might warrant the application of federal securities laws.

⁸⁷ In addition to decentralization requirements, the Commission could consider ways to incentivize front-end interfaces and applications that provide access to smart contract protocols and blockchain networks to ensure that such systems have undergone third-party code audits, use well-established standards, and provide minimal disclosures about functionality in order to bolster protections for market participants. However, in applying such incentives the Commission should be careful not to forestall innovation by encumbering projects with costly requirements when they have de minimis total assets or transaction volumes.

Critically, even in cases where control-related trust dependencies have not been eliminated, it does not mean that the risks intended to be addressed by the broker, dealer, and exchange registration regimes are present or that federal securities laws should apply—it merely means that the Commission’s approach should conform to traditional (but modernized) approaches. As a result, as part of its guidance, the Commission should specify when these regimes may be applicable to systems that have not yet fully eliminated *operational control*, balancing the need for nascent projects to pursue decentralization over time and security concerns that might arise if projects are incentivized to move too quickly, with the need to protect market participants.

One of the key promises of blockchain technology is the development of decentralized systems that are not possible to replicate through traditional, centralized systems. Namely, the disintermediation made feasible through the various technological functions that are inherent to the operation of blockchain technology, including the Exempt Technologies. As described above, the application of regulations designed for intermediaries to these technologies would present insurmountable technical challenges and force them to choose between extinction or reconstituting themselves as traditional centralized financial intermediaries and thus shedding all of the benefits that blockchains provide. In addition, it would not be necessary given that they do not subject users to the same risks as centralized intermediated systems. Accordingly, the Commission’s suggestion—that regulators distinguish between these technologies and traditional financial intermediaries—is correct and critical, and we applaud the Commission for soliciting public feedback on this topic.

Question 4: Users of liquid staking applications receive a so-called “liquid staking token.” This token represents their staked crypto asset, and the token can be used in other activities, all while continuing to participate in the proof-of-stake protocol. Should the Commission address the status of liquid staking tokens under the federal securities laws, and, if so, what issues should it address?

Liquid staking tokens (“LSTs”) are best categorized as asset-backed tokens—they derive their value from a claim on, or economic exposure to, one or more underlying assets. They can be issued manually by centralized issuers or autonomously by decentralized smart contract protocols, and there are a number of different ways that they can implicate federal securities laws, including under both the *Reves*⁸⁸ test and the *Howey*⁸⁹ test. The Commission should issue guidance, grant no-action relief, and direct its enforcement efforts to provide clarity with respect to the regulatory status of LSTs under federal securities laws, thereby preventing overregulation that could hinder innovation, while also protecting market participants. Given the inherent similarities between LSTs and many other asset-backed tokens (stablecoins, wrapped tokens, deposit-receipt tokens, liquidity provider tokens, etc.), the Commission should ensure its efforts are broadly applicable and consistent across these categories.

The control-based decentralization framework proposed above can be applied to asset-backed tokens like LSTs. This means that where LSTs eliminate control, the application of securities laws should be limited; but when control-related risks are present, the Commission’s approach should conform to traditional (but modernized) approaches. To do this, the Commission should first analyze the function and risk of the underlying asset and the manner in which the LST is structured and issued, focusing on the trust dependencies of the LST and the presence of potential information asymmetries.

For purposes of this analysis, it is helpful to divide LSTs into two categories: (1) LSTs autonomously issued by decentralized smart contract protocols and (2) LSTs issued by a centralized company, typically as part of a “staking-as-a-service” operation.

1. Decentralized Smart Contract Protocol LSTs

As a threshold issue, no investment relationship is ordinarily formed between a user and a liquid staking smart contract protocol for several reasons, including: (a) users interact directly with a smart contract protocol, not with an identifiable issuer or counterparty; and (b) the liquid staking smart contract protocol does not raise capital for ongoing business operations—it facilitates staking participation, which is functionally different from an investment scheme. However, the foregoing depends upon the function and risks arising from use of the smart contract protocol.

The trust dependencies of asset-backed tokens like LSTs are a function of (i) the underlying asset (e.g., ETH) and (ii) the issuance and structure of the LST (e.g., a centralized issuer or a decentralized smart contract protocol).

- LSTs primarily reflect the value of the underlying staked asset and do not inherently represent a “note” under *Reves* or a separate “investment contract” under *Howey*. Rather, they are claims on

⁸⁸ *Reves v. Ernst & Young*, 494 U.S. 56 (1990).

⁸⁹ *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

an already staked asset, much like a deposit receipt or warehouse receipt in traditional finance. As a result, the risk profile of an LST is primarily tied to the staked asset itself, meaning if the underlying asset is a commodity, the LST should likely be treated as a commodity as well (e.g., stETH mirroring ETH).⁹⁰

- LSTs may also derive value from the manner in which they are issued and structured. For example, an LST autonomously issued by a decentralized smart contract protocol has different risks from an LST issued by a centralized company. And an LST that is structured so that its value is derived from the non-discretionary and purely technical staking of the underlying asset has a very different risk profile from an LST that derives its value from a highly discretionary staking scheme, involving ongoing material investment management decisions to maximize profits from the staking of the underlying asset.

Given these trust dependencies, the Commission should establish a control-based decentralization framework to mitigate the risks arising from control-related trust dependencies and use supplemental disclosure to mitigate the risks of information asymmetries arising from ongoing efforts-related trust dependencies. This approach would be consistent with the approach to network tokens outlined in Part 5 of our response to **Question #1** and other asset-backed tokens outlined in Part 2 of our response to **Question #2**.

Where a liquid staking smart contract protocol issues an LST, the risk of information asymmetries is likely to be high where such system is controlled—whoever controls a system can unilaterally affect or structure the risk associated with that system.⁹¹ For example, where a single person controls a protocol, that person may exercise discretion to maximize the profits of the arrangement (or even unilaterally steal user deposits), exposing users to significant risks that may implicate an investment contract and warrant the application of federal securities laws. But where a smart contract protocol is decentralized and not *operationally controlled*—autonomous, permissionless, credibly neutral, and non-custodial—the risks that the federal securities laws address are unlikely to be present:

- If the system is **autonomous**, the protocol will operate absent human intervention and control, and without the potential for unilateral changes to the system’s functioning, ensuring that the user’s collateral is staked in accordance with the algorithms and source code of the protocol.
- If the system is **permissionless** and **credibly neutral**, a controlling party cannot cut-off a user’s access to the system, thereby guarding them against a loss of funds.
- If the system is **non-custodial**, the user remains in control of their funds.⁹²

⁹⁰ This approach aligns with the principle of economic equivalence discussed in our response to Question #1—LSTs should not be treated differently from the underlying asset unless additional trust dependencies create a relationship that warrants the application of federal securities laws.

⁹¹ Dennis S. Corgill, *Securities as Investments at Risk*, 67 Tul. L. Rev. 861 (1992), <https://www.tulanelawreview.org/pub/volume67/issue4/securities-as-investments-at-risk>.

⁹² The non-custodial nature of ordinary liquid staking smart contract protocols is worthy of additional analysis. There are several reasons why these protocols can be considered non-custodial even though they are much more complex than liquidity pools of common decentralized finance protocols and decentralized stablecoin protocols. First, when user assets are contributed to the protocol’s smart contracts, they are typically assigned to a whitelisted set of validators, who cannot move or access the funds, or deploy them for purposes other than staking. There is no discretion. If these validators go rogue or fail, they may get slashed, but they cannot seize user funds. Second,

The elimination of *operational control* also reduces risk potentially arising from any ongoing efforts. For example, the removal of control over the underlying staked asset contributed to the smart contract protocol limits the discretion exercisable by any third party with respect to the management of such collateral. This means that the LST itself is more likely to be *economically independent*—the economic mechanisms that drive value to the LST are derived from the underlying asset and staking mechanism of the system, not dependent on any development company or issuer. Further, where liquid staking smart contract protocols are not *operationally controlled*, all relevant information (staking rewards, smart contract risks, protocol governance) is publicly available onchain. As a result, the need for supplemental disclosure to mitigate the risk of information asymmetries arising is substantially reduced.

Conversely, where liquid staking smart contract protocol is *operationally controlled*, it is more comparable to an LST issued by a centralized company and is better evaluated under that criteria.

2. Centralized Issuer LSTs

Operational control is not possible to eliminate in the case of centralized companies providing “staking-as-a-service” services and issuing LSTs—the issuer takes control of user assets to deploy them for staking. This increases the risk of an investment relationship being formed between the user and the issuer because the user interacts directly with an identifiable issuer or counterparty. However, similar to liquid staking smart contract protocols above, these services are not ordinarily for capital raising purposes—they facilitate staking participation, which is functionally different from an investment scheme, a relationship that reflects a commercial or consumer purpose. Critically, the mere presence of control-related trust dependencies does not mean that an investment relationship is formed or that federal securities laws should apply—it merely means that the Commission’s approach should conform to traditional (but modernized) approaches.

Given the foregoing, in order to determine whether an investment relationship has formed, additional analysis of the ongoing efforts-related trust dependencies is needed. In particular, the way in which LSTs are issued and managed could, in some cases, increase the risk that an investment relationship is being formed and that risks of information asymmetries are being introduced. Specifically, it is worth considering:

- The level of discretion that may be exercised by the issuer in the generation of profits for LST holders—does the issuer exercise significant discretion to maximize profits or does the issuer exercise little or no discretion and profits are directly tied to the underlying blockchain protocol’s consensus mechanism?
- The comparability of the issuer’s services with that of an ordinary “software-as-a-service” provider—is the economic arrangement comparable to commercial or consumer arrangements that are not historically subject to federal securities laws?

holders of LSTs can typically redeem them at any time proportionally to the total underlying assets in the staking pool. That means any slashing and loss of staked funds is shared equally across the LST holders, further reducing the risk to any individual user.

- The ongoing efforts of the issuer or another third party, if any, to actively manage liquidity or intervene in pricing of the LSTs—does the issuer actively support the secondary market for LSTs such that the market price may not reflect the actual value of the LST?⁹³
- The statements of the issuer in advertising their services—does the issuer make affirmative statements that create a reasonable expectation of profit based on the issuer’s ongoing managerial or entrepreneurial efforts?

Where discretion is minimal, where the issuer’s services are economically comparable to other SAAS offerings, and where the issuer does not advertise profit potential based on their ongoing efforts, the application of federal securities is likely unwarranted. Any lingering risks arising from the custodial relationship may therefore be addressed through intermediary based regulation (e.g., regulation applicable to custodians of commodities/securities) as opposed to necessitating a separate securities classification although the application of that regulation still needs to be adapted to be workable in light of the blockchain technology applications to which it might be found to apply.

Based on the foregoing, through the issuance of guidance, granting of no-action relief, creation of safe harbors, and tailoring of registration pathways, the Commission should: (1) clarify that liquid staking tokens should generally be treated the same as their underlying staked asset (e.g., if ETH is not a security, then stETH is not a security); (2) apply a control-based decentralization framework to the issuance of LSTs by smart contract protocols focused on the elimination of *operational control*; and (3) provide factors for assessing issuer activity that could influence whether “staking-as-a-service” and LST issuance by a centralized issuer and transactions in such LSTs are subject to federal securities laws. This approach would be consistent with the core principle of this response—when control is eliminated, the application of securities laws should be limited; but when control is present, their application should conform to traditional (but modernized) approaches.

This principle-based approach would ensure that securities laws are applied where necessary to protect investors while avoiding overreach that could harm innovation.

⁹³ William Hinman, *Digital Asset Transactions: When Howey Met Gary (Plastic)*, U.S. Securities and Exchange Commission, June 14, 2018, <https://www.sec.gov/newsroom/speeches-statements/speech-hinman-061418>.

Question 5: Should the security status of certain categories of crypto assets be addressed, such as stablecoins, wrapped tokens, and NFTs?**1. Asset-Backed Tokens**

Stablecoins and wrapped tokens are best categorized as asset-backed tokens—they derive their value from a claim on, or economic exposure to, one or more underlying assets.

a. Stablecoins

Current legislation in both chambers of Congress proposes a regulatory pathway for certain “payment stablecoins” issued by “permitted payment stablecoin issuers,” exempting such assets from U.S. securities laws. As currently contemplated, these bills do not generally prohibit the issuance of stablecoins by smart contract protocols.⁹⁴ However, there is already significant uncertainty as to what standards of decentralization are required for the stablecoins issued by smart contract protocols to be exempt from securities laws, including under *Reves*. The passage of stablecoin legislation is likely to compound this confusion and increase the need for a principled solution. The Commission should therefore direct guidance, no-action relief, and enforcement efforts to exclude decentralized stablecoins from securities laws in accordance with the control-based decentralization framework proposed throughout this response. Doing so would help to bolster whatever stablecoin regulatory framework is adopted by Congress, while guarding against bad actors that may seek to exploit regulatory uncertainty in order to subject market participants to potential harms. For additional discussion about the application of securities laws to asset-backed tokens, including stablecoins, see our responses to **Question #2** and **#4**.

b. Wrapped Tokens

Similar to stablecoins and LSTs, wrapped tokens may be issued by centralized issuers and relate to physical-world collateral or be autonomously issued by decentralized smart contract protocols. As a result, the value of a wrapped token typically reflects the value of the underlying unwrapped asset, but takes on the risks associated with how they are structured and issued. The Commission could address the regulatory status of wrapped tokens under federal securities laws by providing guidance in conjunction with any guidance on stablecoins and LSTs and consistent with the control-based decentralization framework proposed throughout this response. For additional discussion, see our responses to **Questions #2** and **#4**.

2. Collectible Tokens

Collectible tokens are crypto assets whose primary value, utility, or significance is derived from being a record of ownership of a tangible or intangible good. For instance, a collectible token may be a digital analog or representation of a work of art, a musical composition, or a literary work; a collectible or merchandise, like a ticket stub from a concert; membership in a club or community; or an asset in a game or metaverse, like a digital sword or plot of metaverse land. The Commission’s enforcement efforts have

⁹⁴ Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025, 119th Congress (introduced February 4, 2025), <https://www.hagerty.senate.gov/wp-content/uploads/2025/02/GENIUS-Act.pdf>.

resulted in significant uncertainty regarding the applicability of federal securities laws to collectible tokens. As a result, the Commission should use guidance, no-action relief, and enforcement efforts to address such uncertainty, recognizing that the inherent value of collectible tokens is embedded in the asset itself, rather than controlled by any third party, and that offerings of collectible tokens typically do not include any post-sale obligations or marketing of the asset as an investment opportunity. Providing objective criteria for artists, creators, and other market participants to be able to assess and follow without engaging legal counsel is necessary to ensure that the federal securities laws do not encroach upon their livelihoods. In the coming weeks, we expect to submit a safe harbor proposal for collectible tokens meeting certain conditions, addressing the principles of economic equivalence and control discussed throughout this response.

3. Company-Backed Tokens

Company-backed tokens are intrinsically linked to, and primarily derive or are expected to primarily derive their value from, offchain applications, products, or services operated by a company (or other centralized organization).⁹⁵ This relationship is most often explicit—for instance, when the token’s price is tied to the profits of an offchain application, product, or service, or when the token has utility in such systems. But it can also be implicit. Given this, even though company-backed tokens do not grant the holder a defined right, title, or interest like a traditional security, they may have trust dependencies that are similar to securities and constitute an “economic reality” that implicates an investment contract.

Under the Commission’s 2019 Framework, the difference between network tokens and company-backed tokens was difficult to discern, essentially requiring a subjective value judgement by regulators—are the efforts of a development team with respect to a given blockchain or smart contract protocol and its underlying token different from the efforts of a development team building an offchain application, product, or service?

However, if the Commission were to adopt a control-based decentralization framework as suggested throughout this response, the contrast between network tokens and company-backed tokens would become more clear.⁹⁶ Under this framing, network tokens are intrinsically dependent on systems that operate transparently and can operate without human intervention or control. Company-backed tokens are inherently dependent upon systems whose results of operations are not transparently onchain, and cannot ever operate without human intervention and centralized control. Two examples help further highlight the distinction:

- ETH is a network token. It enables holders to transact on the Ethereum Network and provides holders with an economic interest in the network. The network is decentralized and functions autonomously (with no one person or management team in control of it).
- FTT is a company-backed token. Its value was entirely dependent on the ongoing operation of the FTX exchange, which itself was a centralized exchange operated and controlled by a company.

⁹⁵ Miles Jennings, Scott Duke Kominers & Eddy Lazzarin, *Defining Tokens* (Mar. 5, 2025), <https://a16zcrypto.com/posts/article/defining-tokens/>.

⁹⁶ Miles Jennings, Scott Duke Kominers & Eddy Lazzarin, *Network Tokens vs. Company-Backed Tokens* (Mar. 5, 2025), <https://a16zcrypto.com/posts/article/network-tokens-vs-company-backed-tokens/>.

FTX, the company, took a portion of company profits from operating the exchange and used them to buy back FTT, thereby driving its economic value. As a result, FTT's value and utility was controlled by FTX.

In accordance with control-based decentralization framework, where control-related trust dependencies are not eliminated, the application of federal securities laws is not necessarily warranted. Rather, in such cases the Commission's approach should conform to traditional (but modernized) approaches to the application of federal securities laws. That means further analysis of ongoing efforts-related trust dependencies is necessary in order to determine the applicability of federal securities laws given the risk such efforts may introduce information asymmetries.

In the case of company-backed tokens, the Commission's analysis should focus on whether it is reasonably expected that the value of the crypto asset will primarily be based on the asset's utility, consumptive purpose, general market forces, the efforts of a widely dispersed group of non-extrinsically-affiliated persons, or the adoption of the network to which it is related; or whether such value will be primarily derived from the profits and losses or equity value of any single extrinsic enterprise related to the crypto asset. In the case of the former, the application of federal securities laws may be unnecessary. In the case of the latter, securities laws are likely appropriate.

The distinction between network tokens and company-backed tokens is a particularly challenging issue, but it is also one of the most critical to resolve. Regulatory clarity can create a level playing field upon which entrepreneurs, investors, and technologies can compete. However, efforts to empower entrepreneurs to use blockchains and smart contract protocols to build innovative products that mitigate the risks targeted by federal securities laws, do not necessitate that businesses be permitted to securitize centralized technology products that only tangentially make use of a blockchain. Removing risk is a difficult task undertaken by entrepreneurs building with blockchain technology but is in-line with the mission of the Commission. It is therefore critical to align the incentives of entrepreneurs with the goals of the regulatory scheme applicable to crypto assets. Conversely, an approach that is too permissive creates perverse incentives—rewarding those that seek to circumvent the law and punishing those that expend great effort to obey the spirit of it. This dynamic has already stifled blockchain innovation in the U.S. and put market participants at risk.

Given the foregoing, the Commission should use guidance, no-action relief, and enforcement efforts to identify pathways by which transactions in company-backed tokens may comply with or run afoul of federal securities laws consistent with the control-based decentralization framework proposed throughout this response.

Question 6: How can the Commission establish a workable taxonomy while remaining merit- and technology-neutral?

The Commission can establish a workable, predictable taxonomy that remains merit- and technology-neutral by focusing on the economic function and risk profile of a given asset or function, rather than the underlying technology itself, taking into consideration the purposes the federal securities laws were established to advance. As discussed throughout our responses to **Questions #1** through **#5**, this can be framed through the lens of a control-based decentralization framework, which is both merit- and technology-neutral:

**When control is eliminated, the application of securities laws should be limited;
When control is present, traditional (but modernized) approaches should be used.**

A merit-neutral approach ensures that the Commission does not judge the desirability or potential success of a given blockchain network or crypto asset. Instead, the focus should remain on whether the economic characteristics of an asset justify its classification as a security or as a commodity or other financial instrument as a threshold determination in assessing the applicability of the federal securities laws and the Commission's related jurisdiction. The taxonomy proposed establishes a control-based decentralization framework that is not merit-based—it does not require regulators to assess whether a particular blockchain network is useful, successful, or desirable, it only requires regulators to assess whether it has abrogated control in a manner that mitigates the risks that securities laws are designed to address.

By focusing solely on verifiable, objective measures of control, this approach ensures that regulatory classification is determined by the asset's functional and economic characteristics rather than subjective judgments about its potential value or societal benefit. This prevents regulators from picking winners and losers while maintaining clear, enforceable standards that foster innovation and protect market participants.

A technology-neutral approach does not necessitate ignoring blockchain technology's ability to eliminate mechanisms of control that may otherwise give rise to the specific risks securities laws were designed to mitigate, including fraud, information asymmetry, and reliance on centralized managerial efforts. All asset classes present different risks to holders—transactions in U.S. government bonds are not regulated in the same way as transactions in shares of Apple stock because the risk profile of those assets are different—and it would be illogical for a regulatory framework to fail to account for the potential of an asset class to mitigate the risks that framework was intended to address. As a result, the Commission's framework should capitalize on blockchain technology's abrogation of control, which can drive the trust dependencies of network tokens to look more like U.S. government bonds and less like a share of Apple stock.

A control-based decentralization framework is a technologically neutral way to achieve that. The control criteria proposed herein that are capable of being achieved by any blockchain network, regardless of underlying technology. And as technologies increasingly operate absent human intervention (demonstrating autonomy, decentralization, transparency, and trustlessness), the principles identified in

the taxonomy will remain valuable guideposts. For example, a similar control-based framework could be applied to artificial intelligence in the future, once such systems are able to operate on a trustless, rather than a trusted basis.⁹⁷

III. Conclusion

We greatly appreciate the opportunity to provide comments on these matters, and we look forward to continued engagement with the Commission. We urge the Commission to continue to seek industry and public input as it fashions guidance and relief in the areas discussed above, including solicitations for comment on any proposed guidance the Commission may be considering prior to adopting it in final form.

Respectfully submitted,

Miles Jennings, General Counsel
a16z crypto

Jai Ramaswamy, Chief Legal Officer
a16z

Scott Walker, Chief Compliance Officer
a16z

Michele R. Korver, Head of Regulatory
a16z crypto

⁹⁷ Aaditya Shidham, *Trusted Execution Environments (TEEs): A Primer*, a16z crypto (Feb. 19, 2025), <https://a16zcrypto.com/posts/article/trusted-execution-environments-tees-primer/>.

than \$74 billion in assets under management across multiple funds, with more than \$7.6 billion in committed capital for crypto funds. In crypto, we primarily invest in companies using blockchain technology to develop protocols that people will be able to build upon to launch Internet businesses. Our funds typically have a 10-year time horizon, as we take a long-term view of our investments, and we do not speculate in short-term crypto asset price fluctuations.

I. Introduction

We strongly support the goals of the Commission’s Crypto Task Force (“Task Force”) to offer guidance on the application of federal securities laws to the crypto asset market and recommend pragmatic policies capable of promoting innovation and protecting investors. As the Task Force carries out its mandate, we urge it to specifically provide clarity on the application of federal securities laws to airdrops and incentive-based reward programs by creating a safe harbor for such crypto asset distributions that meet certain criteria. The goals of this submission are to elucidate the benefits of this approach and to propose conditions for a safe harbor to ensure that it helps fulfill the Task Force’s dual mandate of fostering innovation and safeguarding investors in the market for crypto assets.

Crypto assets are often distributed to third parties via airdrops and incentive-based rewards for free or de minimis consideration. These distribution mechanisms are critical to enable blockchain projects to function,² but also enable them to achieve decentralization—they not only enable projects to disperse control of the underlying blockchain or smart contract protocol (each, a “blockchain network”), they ensure that the blockchain network can operate autonomously.³ When a blockchain network achieves decentralization, it provides substantial benefits such as promoting competition, safeguarding freedoms, rewarding stakeholders, reducing information asymmetries, and otherwise mitigating risks for market participants (see Section II). Crucially, because blockchain networks are capable of decentralization, they can function more like public infrastructure than proprietary software, enabling developers to bootstrap a wide variety of applications onto a single network, such as decentralized social media networks, identity management protocols, and video games.

At present, market participants face significant uncertainty when assessing whether a given airdrop or incentive-based reward program constitutes a securities transaction and therefore may require registration under Section 5 of the Securities Act. Subjecting airdrops and incentive-based reward programs to registration is not only unnecessary when certain conditions are met (see Section III), but would also impinge upon a blockchain network’s ability to achieve and maintain decentralization because it would force such networks to reintroduce centralized intermediaries in order to comply with the requirements of federal securities laws (see Section II). This would vitiate the essence of blockchain networks, whose fundamental purpose is decentralized operation—operation without human intervention or control. It would also in many cases be incorrect as a matter of law. To be an investment contract, there must be an “investment of money” by the recipient in a common enterprise with a reasonable expectation of profit derived from the efforts of others.⁴ But airdrops and incentive-based rewards do not typically

² Tim Roughgarden, *An Axiomatic Approach to Block Rewards*, YouTube (Jul. 2020), <https://www.youtube.com/watch?v=WyRyWQwm0x0>.

³ a16z Crypto, *Defining Decentralization: Control* (Mar. 2024), <https://a16zcrypto.com/posts/article/defining-decentralization-control/>.

⁴ *SEC v. W. J. Howey Co.*, 328 U.S. 293 (1946).

require an investment of money—they are free or executed for de minimis consideration—and should not be regulated as securities offerings.

However, in the Commission’s 2019 *Framework for “Investment Contract” Analysis of Digital Assets*, the SEC asserted that “[...] an airdrop may constitute a sale or distribution of securities, regardless of whether there is a lack of monetary consideration.”⁵ For the reasons further elaborated below (see Section III.C.) this position misstates the law, creates confusion for businesses and consumers, and hampers innovation. Worse, uncertainty in this area has led to numerous projects excluding U.S. persons, meaning that U.S. regulatory policy has effectively precluded U.S. persons from receiving ownership (for free) of the networks that will underpin the future internet.

Recognizing this lack of clarity and the benefits of airdrops and incentive-based reward programs (as well as the unsuitability of traditional regulatory frameworks for certain airdrops and incentive-based reward programs), recent legislative and regulatory efforts have endeavored to create rules that are fit-for-purpose: mitigating risks while facilitating innovation. H.R. 4763, the Financial Innovation and Technology for the 21st Century Act (“FIT21”),⁶ proposed an exemption from Section 5 of the Securities Act of 1933 for issuances of digital assets that meet certain criteria. Commissioner Peirce’s Token Safe Harbor Proposal 2.0⁷ likewise seeks to provide developers with a “grace period” during which, subject to specific conditions, they would be exempted from the registration provisions of federal securities laws.

In line with these proposals, we strongly recommend that the Commission create a safe harbor for airdrops and incentive-based rewards programs meeting certain conditions. As mentioned above, not all airdrops and distributions of incentive-based rewards will be able to avail themselves of this safe harbor. On the contrary, *only* those airdrops and incentive-based reward programs which *do not* engender the risks that Section 5 was designed to address should be eligible. Importantly though, the failure to meet the conditions specified herein and qualify for the safe harbor should not create a presumption that any given airdrop or incentive-based reward is subject to federal securities laws. Rather, such distributions should be assessed under traditional approaches to the application of the federal securities laws.

II. Airdrops and Incentive-Based Rewards of Network Tokens Help Facilitate Decentralization and Mitigate Risks

Blockchain networks are often started by traditional private development companies (“DevCos”). At a project’s inception, DevCos undertake critical tasks including developing and launching a blockchain network. As with traditional tech startups, DevCos also raise capital in private placements of their equity to institutional investors to resource their efforts.

Once development of a blockchain network is substantially advanced and the network is “functional” (see Section III.A.), DevCos typically seek to publicly launch their networks, which is a key step in the real-world deployment of blockchain technological innovation. In the case of layer-1

⁵ SEC, *Framework for “Investment Contract” Analysis of Digital Assets* (Apr. 3, 2019), <https://www.sec.gov/files/dlt-framework.pdf>

⁶ 118th Congress (2023-2025), H.R. 4763 - Financial Innovation and Technology for the 21st Century Act (introduced July 20, 2023), <https://www.congress.gov/bills/118/congress/house-bills/4763>.

⁷ SEC, Statement on Token Safe Harbor Proposal 2.0 (Apr. 13, 2021), <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-token-safe-harbor-proposal-20>.

blockchains, this often coincides with the launch of the network token (as defined below). For layer-2 blockchains and smart contract protocols, the network may be live well before launch of the network token. At some point during the development cycle, the generation of the native asset of the network occurs, with a portion of those network tokens then being distributed to employees, investors, advisors, and others subject to extended transfer restrictions.

These crypto assets are intrinsically linked to, and primarily derive their value from or are expected to primarily derive their value from, the programmatic functioning of the network (“network tokens”).⁸ Network tokens often have embedded utility; they may be used for network operations, to form consensus, to coordinate protocol upgrades, or to incentivize network actions. The networks to which these tokens relate also often (and in most cases should) contain economic mechanisms that drive the value of the token. These may include programmatic purchases, distributions, and other changes to the total token supply via token creation or burning to introduce inflationary and deflationary pressures in service of the network.

In most cases, the public launch of the network token is accompanied by a public distribution for no or de minimis consideration (an “airdrop”), such as historical engagement with or participation on the network. By broadly disseminating its network token via an airdrop, a blockchain network can help mitigate the risk that any single party or commonly orchestrated or centralized group can control the network. In addition, airdrops can drive the network effects of the network and ensure users are able to continue using and building on the network.

Following public launch, many blockchain networks rely on incentive-based reward programs for maintenance and security, which facilitate its autonomous operation. For example, both mining, in the case of Proof-of-Work (“PoW”), and staking, in the case of Proof-of-Stake (“PoS”) blockchains, are consensus mechanisms used to ensure network security and incentivize stakeholders to perform operational activities. In a PoS blockchain, transactions are added by “validators,” who are similar to “miners,” only instead of performing calculations to “mine” new blocks, validators “stake” an amount of crypto assets as a pledge that they will perform validation work honestly. PoS blockchains then programmatically distribute rewards to validators for performing validation services, which are necessary for the system to function.

In addition, incentive-based rewards can be used to drive network effects by incentivizing more user activity that is beneficial to the network and its users.⁹ The range of activities incentivized might include providing liquidity to a decentralized finance network, participating in decentralized governance, or posting to a decentralized social media network.

Airdrops and incentive-based rewards are therefore critical for blockchain projects to distribute control and to facilitate autonomy of the network. While these are just two critical aspects of decentralization, they better position the network to pursue decentralization along other measures, including to become permissionless, credible neutral, non-custodial, and economically independent.¹⁰ All

⁸ a16z Crypto, *Defining Tokens* (Feb. 2024), <https://a16zcrypto.com/posts/article/defining-tokens/>.

⁹ a16z Crypto, *The Web3 Playbook: Using Token Incentives to Bootstrap New Networks* (Feb. 2024), <https://a16zcrypto.com/posts/article/the-web3-playbook-using-token-incentives-to-bootstrap-new-networks/>.

¹⁰ Decentralization Research Center, *Designing Policy for a Flourishing Blockchain Industry* (Feb. 2025), <https://thedrcenter.org/wp-content/uploads/2025/02/DRC-Designing-Policy-Final.pdf>.

of which is to say that airdrops and incentive-based rewards typically are preconditions for blockchain technology to be deployed in practice on a widespread basis.

Once achieved, decentralization engenders myriad benefits:

- **Promoting Competition:** Decentralization enables blockchain networks to be credibly neutral¹¹ and composable.¹² This ensures that they function like public infrastructure and makes them attractive to build on top of. This then lowers the barrier to entry for anyone wanting to build an Internet business, as it provides the Internet infrastructure upon which they can build. As a result, decentralization promotes competition and the creation of new types of goods and services.
- **Safeguarding Freedoms:** Decentralization necessitates the broad distribution of control of blockchain networks among their stakeholders and ensures that the network effects of such systems accrue to such stakeholders, not just the companies that created them. By limiting the power that can accrue to companies in this manner, decentralization limits corporate power to gatekeep, censor, or otherwise infringe individual liberty. As a result, decentralization safeguards user freedoms as well as ameliorates the agency costs and conflict of interest concerns often associated with centralization.
- **Rewarding Stakeholders:** Decentralization enables the design of systems that prioritize stakeholder involvement – systems that are designed broadly serve the interests of all stakeholders, rather than a certain subset of stakeholders. For example, web3 systems can be designed to more equitably reward users and contributors, rather than being designed to maximise value of shareholders, as is the case with the corporate networks of web2.

In addition to these benefits, decentralization provides substantial protections to market participants by mitigating the risks arising from trust dependencies associated with network tokens, thereby justifying a different regulatory approach from what applies to ordinary securities.¹³ Through the lens of a control-based framework for decentralization, network tokens can be insulated from control-related risks.¹⁴ This is critical because whoever controls a system (a company, a network, etc.) controls the risks associated with the underlying asset of that system and can unilaterally affect or structure the risk associated with that asset.¹⁵ Removing control via decentralization means more than just dispersing ownership though; it means eliminating mechanisms of control so that systems are

¹¹ See Vitalik Buterin, *Credible Neutrality As A Guiding Principle*, Nakamoto (Jan. 3, 2020), <https://nakamoto.com/credible-neutrality/>.

¹² Smart Contract Composability, Ethereum, <https://ethereum.org/en/developers/docs/smartcontracts/composability/> (last updated Aug. 15, 2022).

¹³ See Miles Jennings, *Defining decentralization: It comes down to control* (Feb. 13, 2025), <https://a16zcrypto.com/posts/article/defining-decentralization-control/>.

¹⁴ Miles Jennings, Jai Ramaswamy, Scott Walker, Michele Korver, David Sverdlov, & Aiden Slavin, *SEC RFI: A Control-Based Decentralization Framework for Securities Laws*, a16z crypto, (March 13, 2025), <https://a16zcrypto.com/posts/papers-journals-whitepapers/control-based-decentralization-framework-securities-laws/>.

¹⁵ Willa E. Gibson, *Securities as Investments at Risk: A Market Theory of Investment Contracts*, 67 Tul. L. Rev. 981 (1993), <https://www.tulanelawreview.org/pub/volume67/issue4/securities-as-investments-at-risk>.

autonomous, permissionless, credibly neutral, non-custodial, and economically independent.¹⁶ It also means that participants in decentralized systems are not subject to traditional principal-agent problems and corporate informational asymmetries.

Because blockchain networks are capable of decentralization,¹⁷ they can function more like public infrastructure than proprietary software, enabling them to derive their value from many independent sources, such as market forces, user demand for the underlying network, and the number of developers building on the network, rather than the managerial efforts of a single development team or managerial team. This substantially reduces or eliminates the risks associated with traditional securities where shareholders own shares but depend on directors and officers to set corporate strategy and run the business day-to-day, giving rise not only to information asymmetries but also to the kind of potential agency costs that corporate law addresses. Once decentralization is achieved, such information asymmetries and principal-agent problems do not exist. Consider, for example, Bitcoin and Ether, the value of which is determined independently of the efforts of any controlling party, with Apple stock, the value of which is dependent on the efforts of Apple Inc.'s management team and the performance of its business.

These benefits of decentralization can be achieved without subjecting holders of network tokens to additional risks. Because airdrops and incentive-based rewards are distributed programmatically in exchange for the ongoing performance of services, they do not in general pose the same risks that Section 5 was designed to address (see Section III.D.), and so should not be required to be registered. Further, whatever risks they do pose to token holders can be mitigated through well-tailored conditions unique to the underlying blockchain technology, as another dimension of differentiation as compared to the typical corporate form.

For these reasons, the Commission should, under the circumstances detailed below, exclude airdrops and other incentive based rewards of network tokens that are distributed in exchange for limited consideration from registration under Section 5 of the Securities Act of 1933.

III. Conditions Under Which Airdrops and Incentive-Based Rewards Should be Excluded

While airdrops and incentive-based rewards are key to facilitating and maintaining decentralization as a means of promoting blockchain network and application innovation, the distribution of crypto assets pursuant to these mechanisms may admittedly still pose risks. As such, only distributions that do not give rise to the risks Section 5 of the Securities Act of 1933 is intended to address should be eligible for the safe harbor under consideration. Further, in order to facilitate the ongoing functionality of the blockchain network, the safe harbor should specify that secondary market transactions of network tokens originally distributed in compliance with the safe harbor are similarly excluded from the application of federal securities laws, absent a significant change in circumstances following the qualifying distribution that materially alters the “economic reality” of ongoing transactions in the previously distributed assets.

¹⁶ Decentralization Research Center, *Designing Policy for a Flourishing Blockchain Industry* (Feb. 2025), <https://thedrccenter.org/wp-content/uploads/2025/02/DRC-Designing-Policy-Final.pdf>.

¹⁷ Jennings, Ramaswamy, Walker, Korver, Sverdlov, & Slavin, *supra* note 14.

A five-part approach can be used to assess whether an exclusion would be appropriate for a given airdrop or incentive-based reward program. The safe harbor should require that: (1) the distribution is of a network token; (2) the blockchain network with which the network token is intrinsically linked is “functional;” (3) the distribution is broad and equitable; (4) the distribution is effected for limited consideration; and (5) transfer restrictions apply to certain related persons. Only distributions meeting each of these requirements should be excluded.

However, the failure to meet these conditions and qualify for the safe harbor should not create a presumption that any given airdrop or incentive-based reward is subject to securities laws. Rather, such distributions should be assessed under traditional approaches to the application of federal securities.

Each condition for the safe harbor is discussed in detail below.

A. Network Tokens

As a threshold question, only crypto assets that are properly designed and structured as network tokens should qualify for the safe harbor. As described above, network tokens primarily derive their value or are expected to primarily derive their value from blockchain networks, which are capable of decentralized operation—operation without human intervention or control. This means their trust dependencies are inherently different from ordinary securities, whose value is dependent on systems or sources that are not capable of decentralized operation—centralized systems that require human intervention and control.¹⁸

Importantly, the investor-protection benefits of decentralization are applicable to a number of types of crypto assets, including “asset-backed tokens” like stablecoins, liquidity provider tokens and liquid staking tokens. But these benefits **cannot** be achieved by “company-backed tokens”—crypto assets that are intrinsically linked to, and primarily derive or are expected to primarily derive their value from, offchain systems or sources that are not capable of decentralized operations. These centralized systems require human intervention and centralized control, and consequently have trust dependencies that are similar to those associated with typical securities. For instance, if a token derives its value from a closed system controlled by a single entity, that entity can unilaterally alter the expected value of the token—the controlling entity could alter the purpose of the token or inflate the supply of the token, or even turn off the entire system, at will. Given such risks, where transactions of such crypto assets would be likely to attract investment, it is difficult to justify a safe harbor from federal securities laws for airdrops and incentive-based rewards that might facilitate the creation of a market that promotes investments in company-backed tokens.¹⁹

By limiting any safe harbor to network tokens, the Commission can ensure that such safe harbor is not used for assets that more squarely fall within the jurisdiction of the Commission.

¹⁸ Jennings, Ramaswamy, Walker, Korver, Sverdlov, & Slavin, *supra* note 14.

¹⁹ For more information on company-backed tokens and how they compare to network tokens, see: Miles Jennings, Scott Duke Kominers and Eddy Lazzarin, *Network Tokens vs. Company-Backed Tokens* (March 5, 2025), <https://a16zcrypto.com/posts/article/network-tokens-vs-company-backed-tokens/>.

B. Functional Network

As a general matter, prior to a blockchain network becoming “functional,” the network is de facto controlled by the DevCo and the potential for information asymmetries between the DevCo and network participants is extremely high. Without a functioning network, there is no way to ground expectations about the network’s functioning in the observable reality of how the network has functioned in the past or is functioning in the present. With no information about the functioning of the network publicly available, and where there is no actual functioning to observe, promoters could make misleading statements if not subject to appropriate accountability or could withhold valuable information about the network functionality that they control. This subjects recipients of airdrops and incentive-based rewards pre-network functionality to the kind of risk that federal securities laws are geared toward remedying. Further, if a network is not yet functional, investors’ and users’ dependence on the DevCo in control of the pre-functional network inherently exposes them to considerable risks, including those stemming from the manual performance of operations and the risks of potential mistakes in calculation or data storage, as well as the ability for a controlling DevCo to make unilateral decisions and benefit insiders (including officers, directors, employees, shareholders, investors, advisors and consultants). For these reasons, airdrops and incentive-based rewards associated with blockchain networks that are not functional should not be considered for the safe harbor.²⁰

Consequently, only airdrops and incentive-based rewards that are associated with “functional” blockchain networks should be eligible for this safe harbor. This functionality requirement need not rise to the level of requiring a project’s entire development roadmap be achieved, but should mandate a baseline functionality which every qualified project should be capable of satisfying. In assessing whether a blockchain network is functional, regulators should require that it exhibits basic operational capacity and is capable of fulfilling its essential purposes absent the intervention of individual actors. This can be evaluated using the network’s source code or can be attested to by the DevCo. A functional network is one that enables participants to transact through the updating of the state of the network, including, but not limited to, by transmitting and storing value, taking part in staking or other method of securing the blockchain network, participating in services provided by or an application running on the blockchain network, or partaking in a decentralized governance system.²¹

Importantly, this definition of functionality aligns with key legislative and regulatory proposals. It derives from FIT21 which, in May 2024, passed the U.S. House of Representatives with strong bipartisan support.²² Likewise, it also aligns with the Token Safe Harbor Proposal 2.0, which would include a requirement to analyze whether a blockchain network is functional.²³ In line with these positions, regulators should seek to determine whether a network is functional to assess whether these exclusions would be appropriate for a given airdrop or incentive-based reward program.

²⁰ 118th Congress (2023-2025), H.R. 4763 - Financial Innovation and Technology for the 21st Century Act (introduced July 20, 2023), <https://www.congress.gov/bill/118th-congress/house-bill/4763>.

²¹ Jennings, Ramaswamy, Walker, Korver, Sverdlov, & Slavin, *supra* note 14.

²² U.S. House Financial Services Committee, *House Passes Financial Innovation and Technology for the 21st Century Act with Overwhelming Bipartisan Support* (May 22, 2024), <https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409277>

²³ SEC, *Token Safe Harbor Proposal 2.0* (Apr. 13, 2021), <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-token-safe-harbor-proposal-20>

C. Broad and Equitable Distribution

Another key consideration is whether the distribution is effected in a broad and equitable manner. Contrary to the goal of decentralization, network token distributions that are limited to a narrow group can, instead, serve to reify and enrich insiders. Inequitable distributions, where insiders received the majority, or a considerable minority, of network tokens, can likewise hold decentralization in abeyance by reinforcing the *voting control* of insiders. Similarly, if concentrated in a single party or group under common control, the dissemination of incentive-based rewards would also serve to undermine decentralization, reintroducing legacy risks such as agency costs, information asymmetries, and trust dependencies.

Thus, this exclusion should only apply to network token distributions that are broad and equitable. Any participant in a blockchain network should be capable of accessing an airdrops or incentive-based reward program. As with the abovementioned “functionality” criteria, this requirement also derives from FIT21, which requires that airdrops and incentive-based rewards be distributed in a wide and equitable manner.²⁴ Specifically, FIT21 required that airdrops and incentive based rewards be distributed in a broad, equitable, and non-discretionary manner based on conditions capable of being satisfied by any participant in the blockchain network, including as incentive-based rewards: (A) to users of the network token or any blockchain network to which the network token relates; (B) for activities directly related to the operation of the blockchain network, such as mining, validating, staking, or other activity directly tied to the operation of the blockchain network; or (C) to the existing holders of another network token, in proportion to the total units of such other network token as are held by each person.²⁵

D. Limited Consideration

A defining feature of airdrops is that they are distributed for free or de minimis consideration. This characteristic is what distinguishes them from traditional sales. Likewise, distributions of network tokens via incentive-based reward programs are not made in exchange for monetary consideration. Rather they programmatically distribute network tokens to participants who support the ongoing maintenance and security of the network, or to users who help to drive network effects of the network. These forms of crypto asset distribution therefore do not pose the same risks as traditional sales. Crypto assets that are distributed in exchange for substantial monetary consideration, on the other hand, engender risks similar to traditional securities transactions, a distinguishing characteristic of which is the investment of financial value as consideration for an economic interest in, or claim to, a business enterprise.

It is also important to note that treating airdrops and incentive-based rewards of network tokens that occur for free or in exchange for de minimis consideration as securities transactions may be inconsistent with *Howey*.²⁶ The SEC has previously conceived that this investment prong of the *Howey* test could be satisfied by any theoretical benefit, writing that “the investment of ‘money’ need not take the form of ‘cash.’”²⁷ But this is an overly broad interpretation of the law. To be an investment contract, there

²⁴ 118th Congress (2023-2025), H.R. 4763 - Financial Innovation and Technology for the 21st Century Act (introduced July 20, 2023), <https://www.congress.gov/bill/118th-congress/house-bill/4763>.

²⁵ *Id.*

²⁶ *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

²⁷ SEC, *Framework for “Investment Contract” Analysis of Digital Assets* (Apr. 3, 2019), <https://www.sec.gov/files/dlt-framework.pdf>

must be an “investment of money” by the recipient in a common enterprise with a reasonable expectation of profit derived from the efforts of others. Although the courts have read *Howey* to not require cash consideration, they all require some form of meaningful consideration. In most airdrops of network tokens, recipients either do nothing to become eligible for the crypto asset, or they take an action that involves no money or meaningful consideration, like simply using the network or “following” a project on social media. They do not pay any money or provide valuable compensation, so no investment of money is made. Similarly, incentive-based rewards of network tokens are not distributed in exchange for meaningful monetary consideration, but rather transmitted for useful work such as securing a blockchain network or driving the network’s network effects. In other words, where the user activity giving rise to an airdrop or incentive-based reward is most likely to benefit the network, rather than the DevCo, such activity may even facilitate its decentralization. So, in cases in which there is no payment of money or provision of valuable compensation is made, an airdrop or an incentive-based reward of network tokens should not satisfy the *Howey* test.²⁸

Because airdrops and incentive-based rewards of network tokens that occur for free or in exchange for de minimis consideration should not satisfy the *Howey* test, and because they pose negligible risks, they should be eligible for this safe harbor. Recent legislative proposals concur with assessment, with FIT21 enabling end user distributions that do not involve an exchange of “more than a nominal value of cash, property or other assets.”²⁹ Airdrops and incentive-based rewards exchanged for free or de minimis consideration should thus be eligible for this safe harbor, while those that occur in exchange for a more than nominal value of cash, property, or other assets should not. It is important to note that the creation of a liquid market could be viewed as “meaningful consideration” to insiders promoting airdrops. The proposed Safe Harbor should be structured to address this concern.

E. Robust Transfer Restrictions

In July 1999, the Commission brought a number of actions against issuers of “free stock” for violating the registration provisions of federal securities laws. These cases often revolved around dubious actors creating fraudulent companies and offering “free stock” as part of a broader scheme to generate public trading of their shares, boost stock prices and consummate other sales.³⁰ Many entrepreneurs offered free stock to people who agreed to provide information about themselves or pass information on to others. Seeking to promote their new internet domains, these businesses offered a quid pro quo: bring traffic to the website in exchange for shares. Given the broader context in which the “free stock” was being distributed, the Commission was reasonable in its actions against these schemes—these companies were offering shares in exchange for something of value, an action that would require them to be registered under federal securities laws.³¹ In particular, the free distributions generated market interest to the benefit of insiders.

²⁸ While this would mean that no safe harbor is required under Section 5 of the Securities Act, given the uncertainty that market participants face in evaluating whether even these airdrops amount to a securities transaction, we urge the Commission to clarify its position by creating a safe harbor along the lines proposed herein.

²⁹ 118th Congress (2023-2025), H.R. 4763 - Financial Innovation and Technology for the 21st Century Act (introduced July 20, 2023), <https://www.congress.gov/bill/118th-congress/house-bill/4763>.

³⁰ SEC, *Administrative Proceeding Against Joe Loofbourrow*, Exchange Act Release No. 41631 (July 21, 1999), <https://www.sec.gov/enforcement-litigation/administrative-proceedings/34-41631>.

³¹ New York Times, *S.E.C. Settles 4 Cases Offering ‘Free Stock’* (July 23, 1999), <https://www.nytimes.com/1999/07/23/business/sec-settles-4-cases-offering-free-stock.html>.

Understandably, the Commission’s initial reaction to airdrops and incentive-based reward programs was to view them as posing similar risk as the “Free Stock” cases of the 1990s—these distribution mechanisms can certainly be structured in a manner that subjects investors to similar risks. However, they can also be structured to mitigate the risks the “Free Stock” cases exemplified. The conditions described above help to do so. However, once a DevCo disseminates network tokens via an airdrop the value of its asset may be highly volatile in response to increased demand, giving insiders (including officers, directors, employees, investors, and advisors) the potential opportunity to sell into the market before the value of that network token becomes seasoned and is effectively stabilized by the market.

To guard against such risk, transfer restrictions should be a condition of the safe harbor. Transfer restrictions, or “lockups,” prevent holders from selling for a predetermined amount of time. In essence, insiders agree for a given period not to sell, contract to sell, or otherwise transfer or dispose of any crypto asset that it holds. A sufficiently long token lockup (such as the holding periods specified under Rule 144 and Regulation S, one year) can ensure that insiders are effectively restricted from using any asymmetric information and capitalizing on the volatility that may come with an airdrop, thereby protecting consumers and investors. During this restriction window, the network may mature and become decentralized. Once the transfer restrictions have expired, the network token will be more seasoned and its price more effectively stabilized by market forces.

For transfer restrictions to be effective, they must be robust, eliminating the possibility of insiders exploiting asymmetric information by other means. For example, insiders should be restricted from selling crypto assets they receive in any airdrop, as otherwise DevCos could structure further airdrops to enrich insiders. However, the broad and equitable distribution requirements set forth above help to mitigate this risk. More generally, transfer restrictions must be structured such that insiders cannot easily circumvent them.

For these reasons, only airdrops that include robust transfer restrictions for network tokens held by insiders should be eligible for the safe harbor under consideration.

* * * *

We greatly appreciate the opportunity to provide comments on these important matters, and we welcome engagement with the SEC on these issues.

Respectfully submitted,

Miles Jennings, General Counsel
a16z crypto

Jai Ramaswamy, Chief Legal Officer
a16z

Scott Walker, Chief Compliance Officer
a16z

Michele R. Korver, Head of Regulatory
a16z crypto