ANDREESSEN HOROWITZ

May 1, 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 Public Offerings and Safe Harbor from Registration

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 workable and durable 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 have separated our responses to the Crypto Task Force's questions into different topic letters. In this submission, we respond to the Task Force's questions regarding public offerings of crypto assets (**Questions #7 - 9**), as well as questions regarding a safe harbor from registration (**Questions #10 - 14**). In our responses, we have applied the **control-based decentralization framework** outlined in our initial response to the Request for Information ("Request")—when control is eliminated, the application of securities laws should be limited; when control is present, traditional (but modernized) approaches should be used.[3] In the context of public offerings, modernized approaches are warranted, and in the context of the safe harbor, the application of securities laws should be limited where control has been eliminated.

---

[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.
[3] Miles Jennings et al., *SEC RFI: A Control-Based Decentralization Framework for Securities Laws,* a16z crypto (Mar. 13, 2025), https://a16zcrypto.com/posts/papers-journals-whitepapers/control-based-decentralization-framework-securities-laws/.

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 #7 - #9

Question 7: Could disclosure guidance and/or targeted relief address the concern, or are new forms or other mechanisms needed?

Federal securities laws do not apply to many crypto assets or to many transactions of crypto assets. So, many public offerings of crypto assets—whether public or private—are already outside the Commission's jurisdiction. However, the determination of whether an asset or transaction is subject to federal securities laws remains highly subjective and unpredictable, creating regulatory uncertainty that undermines both innovation and investor protection. As a result, in order to provide a workable registration pathway for crypto assets, the Commission must first establish a taxonomy that clearly identifies when crypto assets may be subject to registration requirements.

As we outlined in our first submission to the Request, we believe this can be accomplished by distinguishing between seven types of crypto assets (network tokens, security tokens, company-backed tokens, collectible tokens, arcade tokens, asset-backed tokens, and memecoins) and providing guidance with respect to each (as the Commission has already done with respect to memecoins[4] and stablecoins,[5] a type of asset-backed token).[6] Many of these assets have clear real-world analogs: security tokens[7] are traditional securities issued in tokenized form; company-backed tokens[8] resemble synthetic equity tied to centralized enterprises; and asset-backed tokens[9] function primarily as their underlying asset does. Meanwhile, arcade tokens[10] are by definition not investments and are therefore not subject to federal

[4] 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.
[5] U.S. Securities and Exchange Commission, Division of Corporate Finance Statement on Stablecoins (Apr. 4, 2025), https://www.sec.gov/newsroom/speeches-statements/statement-stablecoins-040425.
[6] Jennings et al., *supra* note 3.
[7] A "security token" is a crypto asset that represents the digital form of a security on a blockchain. *See* Jennings et al., *supra* note 3, at 12.
[8] 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). *See id.*, at 12.
[9] 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. *See id.*, at 14.
[10] An "arcade token" is a crypto asset that provides utility within a system and is not intended for investment purpose. *See id.*, at 13.

securities laws, and offerings of collectible tokens[11] are unlikely to implicate securities laws.[12] Only network tokens[13]—whose value is derived from participation in and use of decentralized, trustless blockchain systems—lack a traditional counterpart. Thus, while many of these assets may give rise to challenges in the application of federal securities laws, only network tokens introduce truly novel issues.

Given the foregoing, Commission action would be most helpful for issuers of network tokens that wish to engage in primary offerings that satisfy the criteria of the *Howey* test.[14] In such cases, in addition to the available options under existing exemptions like Regulation D, there should be a clear and workable registration pathway. Importantly, that pathway should be flexible enough to accommodate the diverse array of crypto asset issuers, including both those pursuing progressive decentralization and those intending to remain centralized, and the unique characteristics of blockchain technology.

To that end, the Commission should issue interpretive guidance and, where necessary, provide exemptive relief to:

1. Establish a tailored disclosure framework;
2. Clarify reporting requirements under the Securities Exchange Act of 1934 (the "Exchange Act");
3. Provide a pathway for decentralization under Exchange Act reporting requirements; and
4. Enable onchain transactions of registered crypto assets.

The Commission should pursue each of these solutions while adhering to its core mission, as well as the purposes motivating the federal securities laws. It is critical that any guidance promulgated by the Crypto Task Force does not come at the expense of the goals of federal securities regulation such as transparency, informed investor decision-making, and reduced information asymmetries. The approach outlined below furthers these goals while addressing the unique characteristics of blockchain projects.

1. Establish a Tailored Disclosure Framework

One of the primary challenges to registered offerings of crypto assets is the absence of a tailored disclosure framework that reflects the unique characteristics and risk profiles of different types of crypto assets. As a general matter, the Commission can—and should—remain committed to its core objective of redressing information asymmetries where a centralized team possesses material information that is not otherwise available to market participants. However, to do so effectively in the context of crypto asset offerings, the Commission should adopt a flexible, principles-based approach to disclosure—one that is grounded in materiality and tailored to the specific characteristics of the asset at issue. Rather than applying rigid forms and line-item requirements designed for conventional equity securities, the Commission should focus on eliciting relevant and useful information through guidance and, where

---

[11] A "collectible token" is crypto asset whose value, utility, or significance is primarily derived from being a record of ownership of a tangible or intangible good. *See id.*, at 13.
[12] Miles Jennings et al., *Recommendations Regarding a Safe Harbor and Crowdfunding Regime for Collectible Tokens,* a16z crypto (Mar. 27, 2025), https://api.a16zcrypto.com/wp-content/uploads/2025/03/a16z-Safe-Harbor-Proposal-Collectible-Tokens-NFTs.pdf.
[13] 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. *See* Jennings et al., *supra* note 3, at 11.
[14] *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

appropriate, exemptive relief. This would result in more concise, actionable disclosures that better promote informed decision-making and investor protection, particularly given the diversity of crypto asset types and the evolving nature of their use cases and risk profiles.

Specifically, the Staff should acknowledge that the line item disclosures called for by the relevant forms and by Regulation S-K and Regulation S-X may not always be material to purchasers of crypto assets and that, to the extent that an item is immaterial, it may be omitted. For example, where a company-backed token is designed to be a proxy for a profits interest in a business, the required disclosures in the current forms will likely be material and apply. Conversely, where a network token is designed to derive economic value from a blockchain, many of the Commission's current disclosure requirements will be irrelevant or immaterial.[15] For instance, the historic operations of the entity offering a network token may be of substantially less importance to network token purchasers than the design and functional viability of the network, the governance of the network, and the integrity of the code on which it operates.[16] Such differences warrant a flexible approach to disclosure mandates. For a discussion of fit-for-purpose disclosures tailored to network tokens, see our response to **Question #12** below.

Offerings of asset-backed tokens that implicate federal securities laws may also present disclosure considerations that are different from those of ordinary securities, network tokens, and company-backed tokens. As discussed in our response to **Question #4**, the risks posed by asset-backed tokens include those arising from trust dependencies associated with (i) the underlying asset and (ii) the issuance and structure of the asset-backed token.[17] For example, a yield-bearing stablecoin that depends upon the managerial efforts of an executive team to execute a collateral management strategy that generates yield, which would not meet the Commission's definition of a "covered stablecoin,"[18] would introduce trust dependencies relating to both the reserve backing of the stablecoin as well as the management strategy driving the yield. The issuer of such a stablecoin should therefore be subject to disclosure obligations pertaining to the composition of their reserves and their activities similar to disclosures that would be found today on an Investment Company's Form N-1A. By contrast, network tokens derive their value from the programmatic functioning of the network rather than from a backing asset. As such, disclosures pertaining to reserves, which generally do not exist in the case of network tokens, would be irrelevant and, indeed, potentially misleading to investors given the fundamentally different purpose and nature of these crypto assets as compared to stablecoins.

2. Clarify Exchange Act Reporting Requirements

A second challenge relates to the application of Exchange Act reporting requirements following a registered offering. The Commission should clarify when and how crypto assets may be deemed equity

---

[15] Justin Slaughter, Katie Biber & Rodrigo Seira, *The Current SEC Disclosure Framework is Unfit for Crypto* (Apr. 20, 2023), https://www.paradigm.xyz/2023/04/secs-path-to-registration-part-iii.
[16] Chris Brummer, *A Developer Theory of Disclosure* (Feb. 14, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5137972.
[17] Jennings et al., *supra* note 3, at 14, 15, 25-27, 41-45.
[18] U.S. Securities and Exchange Commission, Division of Corporate Finance Statement on Stablecoins (Apr. 4, 2025), https://www.sec.gov/newsroom/speeches-statements/statement-stablecoins-040425.

securities for Exchange Act purposes, and provide interpretive guidance on the resulting reporting obligations to ensure that issuers have clarity on their long-term compliance obligations.

Following a registered public offering, issuers generally become subject to periodic reporting requirements under Section 15(d) of the Exchange Act. When these obligations are triggered by the public sale of crypto assets, reporting requirements are typically limited to the filing of quarterly and annual reports.[19] Importantly, Rule 15d-6 permits issuers to suspend these reporting obligations in the fiscal year following the offering, provided that the securities are not listed on a national securities exchange and are held of record by fewer than 300 persons (or 500 persons if the issuer has less than $10 million in total assets).[20] For issuers of crypto assets that do not require a freely transferable crypto asset during the one year period following a public offering, this provides a practical, time-limited pathway for a compliant public offering without subjecting such projects indefinitely to Exchange Act reporting.

However, this pathway is available only if the sold crypto assets do not constitute "equity securities." If crypto assets are classified as a class of equity securities under the Exchange Act, the issuer becomes subject to more extensive and enduring regulatory obligations. These include not only ongoing Exchange Act reporting, but also the application of additional regulatory requirements such as proxy rules, tender offer rules, and insider trading restrictions. As such, it is critical for crypto asset issuers to understand whether the crypto assets they issue—particularly when offered through a registered public offering—may be deemed equity securities for Exchange Act purposes.

To that end, the Commission should clarify when and how a crypto asset may be treated as an equity security. In relevant part, Rule 3a11-1 defines an "equity security" to include "any stock or similar security, certificate of interest or participation in any profit-sharing agreement, […] transferable share, voting trust certificate or certificate of deposit for an equity security, limited partnership interest, interest in a joint venture, or certificate of interest in a business trust."[21] Many crypto assets should not fall within these definitions, but clarity is nonetheless needed so that issuers understand when such classification might apply.

As we discussed in our response to **Question #2**, network tokens should not be deemed to be equity securities merely because they confer network rights (e.g., use, profit sharing, governance rights, residual claims on assets) to network tokenholders.[22] Where network tokens confer governance rights, such rights are typically more akin to participation in a technical governance process than to the governance rights held by residual claimants in a business enterprise. Moreover, the granting of economic rights in a decentralized network should not be equated to the granting of economic rights in a business

[19] Section 15(d) requires issuers to file periodic reports with the SEC after registering securities under the Securities Act—regardless of whether the issuer lists those securities on a national exchange. By contrast, Section 12 applies when securities are listed on a national securities exchange or when certain thresholds are met (e.g., assets >$10 million and 2,000 holders of record, or 500 non-accredited holders for equity securities). Section 15(d) obligations are often more limited in duration and scope, and may be suspended under Rule 15d-6 when thresholds for holders of record are not met in the following fiscal year.
[20] 17 CFR § 240.12h-3 (Suspension of duty to file reports under section 15(d)), https://www.law.cornell.edu/cfr/text/17/240.12h-3.
[21] 17 CFR § 240.3a11-1 (Definition of the term "equity security"), https://www.law.cornell.edu/cfr/text/17/240.3a11-1.
[22] *See* Jennings et al., *supra* note 3, at 24-27.

enterprise—network tokens derive their value from the functioning of an operational blockchain network, rather than from the profits or assets of a centralized company, which means their trust dependencies and risk profiles can differ significantly from equity securities.

Conversely, certain crypto assets may properly be classified as equity securities. For example, a security token that is just a digital wrapper around a conventional equity instrument (e.g., tokenized public company stock) would clearly be appropriately classified as such. Further, a company-backed token with profit sharing and governance rights that derives its value from an offchain system operated and controlled by a centralized company could have many of the same trust dependencies and risks of ordinary equity securities. As a result, where a company-backed token introduces such trust dependencies, it should therefore likely meet the criteria of an equity security and be classified as such.

Finally, it is important to underscore that whether a security is considered an equity security depends on the nature of the claim it represents—not on whether it was issued to raise capital. Capital can be raised through a variety of non-equity instruments (e.g., debt securities), and the fact that a crypto asset is involved in a capital raising should not change this core economic analysis. We therefore urge the Commission in crafting a clear and functional taxonomy to provide explicit guidance on how crypto asset classification affects Exchange Act obligations—including when a crypto asset is, and is not, an equity security.

3. Provide a Pathway for Decentralization Under Exchange Act Reporting

Another reason projects have been reluctant to raise capital through registered public offerings of network tokens is the absence of a clear pathway for evolving Exchange Act compliance obligations as the underlying network decentralizes. The Staff has previously acknowledged that the evolution of a network through decentralization may render the ongoing application of securities laws unworkable and unnecessary.[23] However, the current structure of Exchange Act reporting—particularly its periodic reporting and, where applicable, listing requirements—is predicated on the existence of a centralized management team responsible for ongoing oversight and compliance. As a result, significant uncertainty remains as to whether—and how—decentralization provides a pathway to reduced reporting or eventual deregistration. Moreover, these potentially ongoing obligations may unintentionally entrench centralization, even where a project's design is intended to eliminate managerial control over time—as noted in Part 3 of our response to **Question #1**, any requirements that necessitate centralization, whether de jure or de facto, will prevent blockchains from realizing their full potential, undermining technological innovation.[24] For that reason, we believe the Commission should resolve this uncertainty by establishing a tiered compliance framework that adjusts reporting obligations based on the extent to which a project has achieved both control-based decentralization (the elimination of mechanisms of operational, economic, and voting control) as well as the elimination of ongoing managerial efforts.

---

[23] 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.

[24] Jennings et al., *supra* note 3, at 7-11.

As we noted in Part 5 of our response to **Question #1**, while a control-based decentralization framework provides an objective and administrable standard, it may not eliminate all investor risks that animate federal securities laws.[25] In particular, where identifiable entrepreneurs or other participants continue to engage in ongoing managerial efforts that are material to the success of the project, information asymmetries may remain. Accordingly, we recommend that the Commission permit full deregistration under the Exchange Act only when both (i) control-based decentralization has been achieved and (ii) ongoing managerial efforts have ceased.

In the event that control-based decentralization has been achieved, but ongoing managerial efforts continue, we recommend a transition to reduced, commensurate disclosure obligations. This transition recognizes that the issuer is no longer in a position to manage the project or coordinate disclosures in the same manner as a traditional corporate issuer, while also acknowledging the potential for ongoing information asymmetries. The Commission could implement this through a combination of staff guidance and exemptive relief, consistent with the tailored disclosure approach proposed in Part 1 of our response to this question. Such an approach would provide a clear, gradual, and risk-calibrated off-ramp for projects that are progressing toward decentralization.

Bitcoin and Ethereum offer illustrative examples. These networks are fully operational and transparent, yet lack centralized teams capable of preparing or certifying disclosures. A reporting framework that assumes a centralized issuer is not only inapplicable to such projects—it is fundamentally misaligned with the regulatory goals of investor protection and market efficiency. In the case of Ethereum, had its initial coin offering originally been conducted as a registered public offering, the ongoing regulatory obligations that follow the Commission's current registration pathway would not have permitted the project to achieve the level of control-based decentralization it has today—nor the cessation of ongoing managerial efforts that have led to ETH's widely accepted status as a true commodity. As a consequence, ETH would continue to exhibit certain trust dependencies akin to securities, and therefore neither the network nor market participants would realize the benefits of Ethereum's decentralization.[26] However, had a multi-stage reporting framework been available, the Ethereum team and its broader community could have elected to continue pursuing centralized development activities material to the network while complying with a lower-tier disclosure regime tailored to reflect the reality of a network that increasingly operates without human control. This example underscores why a rigid, one-size-fits-all reporting regime is not compatible with decentralized systems—and why a graduated approach to Exchange Act compliance is essential to enable lawful public offerings without sacrificing the risk-mitigating benefits that decentralization affords.

In summary, the Commission should establish a multi-stage pathway under which registered network tokens may move from full Exchange Act reporting to focused, project-specific disclosures, and ultimately to deregistration, based on the cessation of ongoing managerial efforts. This structure would facilitate responsible capital formation, promote the benefits of decentralization, and protect investors in a manner consistent with the actual risks presented by the project. We provide an example of such tapering in Part 3 of **Question #10** below.

---

[25] *Id.*, at 15-21.
[26] *Id.*, at 7-11.

4. Enable Onchain Transactions of Registered Crypto Assets

For any registration pathway to be workable in practice, registered crypto assets must be capable of being used and transacted onchain—for example, to pay network fees or participate in decentralized protocols—without such use triggering additional or conflicting regulatory obligations. Likewise, registered crypto assets must be capable of being traded via decentralized exchanges or appropriately regulated alternative trading systems in a manner that reflects the technical and operational realities of blockchain-based markets. Any failure to modernize these frameworks will undermine the utility and accessibility of compliant crypto assets, discouraging use of any registration pathway. We intend to address these implementation issues in our responses to **Questions #40** through **#46**, and we encourage the Commission to ensure that any registration regime it adopts does not inadvertently inhibit lawful onchain utility for registered crypto assets.

***

A registration pathway that incorporates tailored disclosures, clear Exchange Act reporting obligations, a graduated compliance framework for projects pursuing decentralization, and the facilitation of onchain transactions would give crypto asset issuers far greater flexibility in determining how to raise capital and whether—and to what extent—to pursue decentralization. Together, these reforms would allow the federal securities laws to function as intended: protecting investors and facilitating responsible innovation.

Any such pathway should be carefully scoped to remain consistent with and complementary to broader legislative reforms, including the market structure legislation currently under consideration in Congress. Ensuring harmony between Commission-administered frameworks and future statutory regimes will be essential to supporting capital formation, maintaining U.S. competitiveness, and safeguarding investor interests in the emerging digital asset economy.

Question 8: Should the Commission develop tailored disclosure requirements for offerings or classes of specific categories of crypto assets? What types of disclosures would be important for investor protection? Should disclosure occur both at the time of sale and on an ongoing basis? If so, what information should the ongoing disclosure contain and how should that disclosure occur?

As discussed in Part 1 of our response to **Question #7** above, the Commission should develop a tailored disclosure framework for registered offerings of crypto assets. A taxonomy that distinguishes crypto assets based on their trust dependencies, control structures, and investor risks would help inform the types of disclosures needed to reduce information asymmetries. In particular, supplemental disclosures beyond the baseline Regulation S-K requirements are likely to be most appropriate for network tokens, which intrinsically relate to and derive value from blockchain networks rather than from conventional enterprises. For a discussion of fit-for-purpose disclosures tailored to network tokens, see our response to **Question #12** below.

We support the Commission's recent recognition that crypto assets raise novel disclosure questions and that standard corporate reporting frameworks may be ill-suited for this domain.[27] However, while the Staff's guidance outlines important categories of information, we believe that disclosure requirements must go further: they must be functionally tied to risk. As we have proposed, disclosure obligations should be structured around control and ongoing managerial efforts, which are the actual sources of information asymmetry and investor harm. By contrast, descriptive disclosures alone—absent an overarching risk-based framework—may provide little value to market participants and could even obscure the material differences between centralized and decentralized systems in a manner that may mislead and ultimately harm investors.

As discussed in Parts 2 and 3 of our response to **Question #7** above, we believe that disclosure obligations for crypto assets should generally track the cadence of Exchange Act reporting requirements, including both time-of-sale and ongoing disclosures. However, for projects utilizing network tokens and pursuing decentralization, the Commission should implement a graduated compliance framework—with disclosures tailored to the project's current level of control and ongoing managerial involvement. As control is eliminated and ongoing managerial efforts cease, disclosure obligations should decline accordingly.

Such a framework would align regulatory obligations with the economic realities and risk profiles of blockchain networks, providing investors with meaningful transparency without imposing unnecessary burdens on decentralized systems. By enabling disclosures that are proportional to issuer control and material activity, the Commission can reinforce the investor protection goals of the federal securities laws and preserve the core innovation potential of blockchain-based systems, decentralization.[28]

Question 9: Does Regulation A under the Securities Act, including the disclosure and ongoing reporting requirements, provide a useful vehicle to conduct offerings of crypto assets? Would revising aspects of Regulation A make it more useful for crypto asset offerings?

Amendments for Small and Additional Issues Exemptions Under the Securities Act ("Regulation A") can serve as a useful starting point for a registration pathway for crypto assets that remain subject to centralized control like security tokens and company-backed tokens. However, Regulation A—particularly its disclosure obligations, offering limits, and ongoing reporting framework—is not currently a useful vehicle for conducting offerings of network tokens and thus requires targeted revisions to be workable and effective in this context. In particular, the challenges associated with the use of Regulation A for network token offerings include:

- **Inflexible Disclosure Requirements –** As with the Exchange Act's disclosure requirements, Regulation A's disclosure framework is modeled on traditional corporate equity offerings and is not well suited to address the unique features of certain crypto assets including network tokens and asset-backed tokens. As discussed in our responses to **Questions #7** above and **Question #12**

[27] U.S. Securities and Exchange Commission, Division of Corporation Finance, *Offerings and Registrations of Securities in the Crypto Asset Markets* (Apr. 10, 2025), https://www.sec.gov/newsroom/speeches-statements/cf-crypto-securities-041025.
[28] *See* Miles Jennings, *Defining decentralization: It comes down to control*, a16z crypto (Feb. 13, 2025), https://a16zcrypto.com/posts/article/defining-decentralization-control/.

below, additional categories of disclosure are essential for investor protection and must be incorporated into a calibrated disclosure framework for network tokens.

- **Ongoing Reporting Obligations at Odds with Decentralization –** Regulation A's ongoing reporting obligations presume the existence of a centralized, perpetual issuer, which is inconsistent with projects that are explicitly designed to eliminate control over time, as is the case with most network tokens. As discussed in Part 3 of our response to **Question #7** above, the Commission should apply a graduated reporting framework—under which projects that meet measurable decentralization milestones (e.g., elimination of voting, economic, or operational control) may transition to reduced disclosure obligations and ultimately—in the event that all mechanisms of control and ongoing managerial efforts are eliminated—deregister. Incorporating this pathway into Regulation A would make ongoing compliance more workable while creating a regulatory pathway for projects to decentralize responsibly. We provide an example of such tapering in Part 3 of **Question #10** below.
- **Exclusion of Airdrops and Incentive-Based Rewards** – The offering caps of Regulation A may not align with the scale of network launches, particularly if distributions via airdrops and incentive-based rewards count towards such caps. As a result, the Commission should adopt a safe harbor for such distributions under certain circumstances. In a companion submission, we have elaborated a five-part approach to assessing whether an exclusion would be appropriate for a given airdrop or incentive-based reward program.[29] Alternatively, revisiting these limits or allowing non-monetary consideration (e.g., labor or governance participation) in a token-specific Regulation A context would improve flexibility.
- **Uncertainty Around Secondary Market Trading** – Although Regulation A securities are permitted to trade freely, it remains unclear whether this includes tokenized assets that trade via decentralized exchanges or alternative trading systems. To avoid regulatory uncertainty, a revised Regulation A framework should explicitly contemplate secondary token trading, so long as the project meets certain disclosure or decentralization thresholds (see Part 5 of our response to **Question #10** below).

With these modifications, Regulation A could become a more viable and appropriately scoped pathway for compliant public offerings of crypto assets—particularly for issuers with centralized operations or those pursuing a gradual transition to decentralization. Importantly, any revision to Regulation A should be designed to complement the broader graduated compliance model we recommend under the Exchange Act in Part 3 of our response to **Question #7** above. This will ensure consistent treatment across offering and post-offering obligations and provide crypto asset projects with a coherent framework for registration, disclosure, and exit.

Finally, we encourage the Commission to ensure that any modifications to Regulation A remain consistent with broader market structure reforms anticipated in legislation currently under consideration by Congress. A harmonized approach across regulatory regimes will help promote U.S. leadership in digital asset innovation while maintaining robust investor protection.

---

[29] Miles Jennings et al., *SEC RFI: Safe harbor for certain airdrops & incentive-based rewards of network tokens*, a16z crypto (Mar. 13, 2025), https://a16zcrypto.com/posts/papers-journals-whitepapers/sec-rfi-safe-harbor-airdrops-network-tokens.

III. Responses to Crypto Task Force Questions #10 - #14

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

We strongly support the goal of the Token Safe Harbor Proposal (the "Proposal") to provide a safe pathway for entrepreneurs to facilitate the participation in and development of functional and decentralized networks without triggering the registration provisions of federal securities laws. We are especially grateful for your commitment to iterating upon the Proposal based on stakeholder feedback, as evidenced by its publication on the developer collaboration platform GitHub.[30]

However, we believe that, in the long run, the Crypto Task Force can best achieve its mandate by deferring this matter to Congress in the near term. Comprehensive legislation is required for the blockchain technology industry to thrive and to ensure that users are safeguarded. Just as the passage of the U.S. Scientific and Advanced Technology Act of 1992 paved the way for a commercial internet boom,[31] and the Telecommunications Act of 1996 enabled the rapid expansion of the U.S. technology economy,[32] the next era of the internet, "web3," requires congressionally sanctioned regulatory clarity to thrive. As we have elaborated elsewhere, rules for the blockchain ecosystem are necessary, welcome, and warranted.[33] But the Commission does not currently have the authority to provide regulatory clarity beyond the application of the federal securities laws and, given that many crypto assets have been recognized as being outside the reach of current securities and commodities laws, comprehensive regulation will likely require legislation. Moreover, no matter how effectively crafted, rules promulgated by regulatory agencies can be rolled back, decisions altered, and new frameworks introduced. In short, legislative solutions can be more enduring and comprehensive. As with any innovation, it will take time for blockchain technology to develop. A holistic, long-term solution is required, so the Task Force should prioritize supporting lawmakers in the creation of a federal crypto regime that builds upon previous bipartisan efforts to give blockchain projects a pathway to safely and effectively launch in the United States while protecting consumers.[34]

Should the Commission nonetheless decide to proceed with the implementation of a version of Rule 195, changes must be made in order to ensure that the Proposal aligns with the Task Force's mission. While we appreciate the spirit and objectives of Rule 195, the current design—centered on functionality and intent, with a three-year window—fails to address the core regulatory risks posed by crypto asset offerings. As we discuss in further detail below, the Proposal does not currently distinguish between crypto asset types and does not protect investors from projects that have similar trust dependencies as

---

[30] Statement, Securities and Exchange Commission, Hester M. Peirce, Token Safe Harbor Proposal 2.0 (Apr. 13, 2021), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-token-safe-harbor-proposal-20.
[31] Fostering Research on the Economic and Social Impacts of Information Technology, National Research Council, National Academies Press (1998).
[32] Alice M. Rivlin & Robert E. Litan, The Economy and the Internet: What Lies Ahead, Brookings Institution (Dec. 1, 2001), https://www.brookings.edu/articles/the-economy-and-the-internet-what-lies-ahead/.
[33] Miles Jennings, *Regulate Web3 Apps, Not Protocols*, a16z crypto (Sep. 29, 2022), https://a16zcrypto.com/posts/article/web3-regulation-apps-not-protocols/.
[34] 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.

ordinary securities—projects that remain subject to centralized control. It therefore risks penalizing good-faith entrepreneurs pursuing control-based decentralization and enabling opportunistic behavior by centralized issuers. As such, we believe the Proposal must be restructured if it is to achieve its goals.

As a preliminary manner, the Commission should bolster its control-based decentralization framework. By doing so, the Commission can put forth a holistic and consistent approach to providing regulatory clarity while promoting innovation and protecting market participants. Critically, this approach will ensure that the Proposal remains sufficiently constrained so as not to allow the circumvention of federal securities laws by projects that present risks that federal securities laws were intended to address.

To align the Proposal with the Commission's investor protection mandate and ensure it is both workable and resistant to abuse, we recommend a series of focused revisions based on bolstering the Proposal's control-based decentralization framework:

1. Constrain the scope to apply only to "network tokens," the sole category of tokens capable of both implicating securities laws and, through decentralization, mitigating the risks that those laws address.
2. Modify the "Network Maturity" concept to align with its control-based decentralization framework, conforming it to the approach included in our response to **Question #1**[35] and the specified control-criteria proposed by the Decentralization Research Center.[36]
3. Restructure the expiration and exit mechanisms to reflect this revised framework, ensuring that entrepreneurs are not incentivized to abandon their projects to avoid registration requirements and that disclosure obligations persist where ongoing managerial efforts remain.
4. Limit the aggregate amount that may be sold in primary offerings.
5. Incorporate transfer restrictions and sales-volume limitations to mitigate information asymmetry risks during the developmental period.

Each of these changes would improve the Proposal's alignment with the practicalities of token-based innovation while upholding the goals of the federal securities laws. We discuss each in greater detail below.

1. Constrain the Scope to Network Tokens

At present, the Proposal makes no distinction between types of crypto assets, providing initial development teams a time-limited exemption regardless of the type of crypto asset they issue. As we explained in our response to **Question #1**[37]—and as elaborated in our safe harbor proposal for airdrops and incentive-based rewards[38]—not all tokens present the same risks, nor are they equally capable of mitigating risks through decentralization. To achieve its intended purpose, the Proposal must be narrowly

[35] Jennings et al., *supra* note 3, at 3-23.
[36] Decentralization Research Center, *Designing Policy for a Flourishing Blockchain Industry* (Apr. 29, 2025), https://thedrcenter.org/wp-content/uploads/2025/04/DRC-Flourishing-v2.pdf.
[37] Jennings et al., *supra* note 3, at 3-23.
[38] Jennings et al., *supra* note 27.

tailored to tokens that (i) may implicate federal securities laws and (ii) are capable of mitigating the risks those laws are designed to address.

That category is limited to network tokens—tokens that derive their value from the functioning and adoption of a blockchain network and that are capable of achieving control-based decentralization. As discussed in response to **Question #7**, network tokens are a truly novel asset class that lack a traditional counterpart, and consequently present unique challenges under federal securities laws. Specifically, network tokens may initially exhibit securities-like features, but can eliminate the traditional trust dependencies typically associated with ordinary securities through decentralization. They are therefore uniquely suitable for and would benefit from a structured exemption focused on decentralization. By contrast, company-backed tokens—whose value is tied to offchain, centralized operations—cannot be meaningfully decentralized, and thus cannot eliminate the information asymmetries and control-related risks that securities laws are intended to mitigate. Consequently, extending the Proposal to such tokens would be inconsistent with the Task Force's investor protection goals.[39]

We therefore recommend that the Proposal be expressly limited to network tokens, and that the Commission adopt a formal definition of "network token" that is consistent with our previous submissions to the Request.[40] To avoid circumvention, the Commission should further clarify that such tokens must not grant a right, title, or interest in any issuer, promoter, or business entity that would create post-sale obligations or trust dependencies. This definition is broad enough to capture all forms of network tokens, while excluding company-backed tokens and other crypto assets that may superficially resemble them but do not share the same capacity to eliminate risk.

2. Modify "Network Maturity" Construct to Align with Control-Based Decentralization

We applaud the Commission for focusing the definition of "Network Maturity" on the degree to which a blockchain network is, or may become, controlled. However, the Proposal currently uses an ambiguous conceptualization of "Network Maturity" that may introduce many of the same challenges as the Commission's 2019 Framework for "Investment Contract" Analysis of Digital Assets (the "2019 Framework")—namely, confusion for market participants and perverse incentives (see Part 5 of our response to **Question #1**).[41] In particular:

- ***Lack of Objectivity*:** The Proposal's concept of economic and operational control is neither sufficiently clear nor readily evaluable enough to enable market participants to confidently determine when a network has reached maturity and, therefore, when a transaction in a related

[39] If the Commission nevertheless wishes to provide a pathway for company-backed tokens in the Proposal, the provisions proposed by Gabriel Shapiro regarding the achievement of Token Maturity by Qualifying Consumer Applications would help mitigate much of the risk posed by company-backed tokens. *See* Gabriel J. Shapiro, *Token Safe Harbor Proposal 3.0* (Mar. 14, 2025), https://www.sec.gov/files/ctf-input-shapiro-2025-03-14.pdf.
[40] Specifically, a "network token" should be defined as "a digital commodity that is intrinsically linked to the functioning of a blockchain system and whose market value is substantially derived from, or is reasonably expected to be substantially derived from, the adoption and use of such blockchain system." *See* Miles Jennings et al., *SEC RFI: Safe harbor for certain airdrops & incentive-based rewards of network tokens*, a16z crypto (Mar. 13, 2025), https://a16zcrypto.com/posts/papers-journals-whitepapers/sec-rfi-safe-harbor-airdrops-network-tokens.
[41] Jennings et al., *supra* note 3, at 15-21.

crypto asset no longer constitutes a securities transaction. Indeed, with the exception of a specific threshold for networks that are substantially owned or governed by an initial development team, the Proposal does not include any other objective measures with which to assess the degree to which a blockchain network is "economically or operationally controlled." Further, as discussed in our response to **Question #13a** below, control-based decentralization is not merely about dispersing ownership—it requires the *elimination* of mechanisms of control (including operational, economic, and voting control), ensuring that blockchain systems function autonomously and without reliance on, or interference from, any central party.

- ***Lack of Clarity Regarding Functional Networks*:** The "Network Maturity" construct's distinction between "decentralized or functional" networks is difficult to interpret. We believe the intention here is to provide a path for projects that are seeking to decentralize and those that are not, but for the reasons discussed in Part 1 above, we do not believe the Commission should provide a pathway that would permit the inclusion of company-backed tokens—by definition such crypto assets cannot eliminate trust dependencies and derisk in a manner that warrants exclusion from federal securities laws (or a reduced regulatory burden). Enabling them to exist within the Proposal would be at odds with the Proposal's threshold requirement regarding an intention to decentralize and could allow them to proliferate without sufficient regulatory guardrails. Alternatively, if the intention is to provide a pathway for non-speculative utility crypto assets like arcade tokens, which derive all their value from their functionality, such inclusion would not trigger the same concerns as company-backed tokens. However, we do not believe the Proposal need apply to such crypto assets as they are by definition not investable and therefore do not implicate federal securities laws. Further, such assets could likely be better dealt with through guidance and no-action relief that expands upon the no-action relief granted to Pocketful of Quarters, Inc. in 2019.[42]
- ***Potential Perverse Incentives*:** The "Exit Report" construct further confuses "Network Maturity" by introducing ongoing efforts-related criteria. If this criteria is interpreted to mean that a project may need to register upon the expiration of the safe harbor in cases where the initial development team continues to engage in ongoing managerial efforts, the inclusion of such criteria could discourage builders from improving upon networks following the expiration period, introducing new operational and execution risks and hampering innovation (an issue we discussed in Part 5 of our response to **Question #1** in regards to the 2019 Framework).[43] Alternatively, if ongoing managerial efforts do not impact the registration requirements of the project, then the expiration of the safe harbor would result in tokenholders potentially being exposed to information asymmetries resulting from such ongoing managerial efforts. We discuss solutions to the exit and expiration mechanisms further in Part 3 below.

Thus, we believe that the Proposal advances an inadequate conception of "Network Maturity." The Commission can address these shortcomings by modifying the Proposal's definition of "Network Maturity" to use principles and rules-based tests that are focused on control-based decentralization in a manner consistent with the framework we proposed in Part 5 of our response to **Question #1**.[44] Amending

[42] Pocketful of Quarters, Inc., SEC No-Action Letter (July 25, 2019), https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1.
[43] Jennings et al., *supra* note 3.
[44] *Id.*

the definition in this way would pair a subjective overarching control-based framework that would provide regulators with sufficient flexibility to evaluate new use cases over time, with an objective and readily measurable control-based decentralization test that would give builders clear rules of the road and accelerate the pace of innovation. This can be accomplished with four distinct parts:

- **First**, "Network Maturity" should be defined using a principles-based approach to mean the point at which a network token and its underlying network are not controlled by any person or group of persons under common control and certified as such by the Commission.
- **Second**, a rules-based rebuttable presumption should be established that a network token and its underlying network ***have*** reached "Network Maturity" if the system meets certain specified objective criteria introduced in Part 3 of our response to **Question #1**, including that the network is open, autonomous, permissionless, credibly neutral, non-custodial, economically independent, and distributed.[45] We discuss each of these criteria further in our response to **Question #14** below.
- **Third**, a rules-based rebuttable presumption should be established that a network token and its underlying network ***have not*** reached "Network Maturity" if the system meets certain specified objective criteria indicative of the system still being subject to control. For instance, if a system is not yet functional or if more than 30% of the network tokens of such a system are owned by an individual, a rebuttable presumption should be established that "Network Maturity" has not been achieved.
- **Fourth**, the process for certification should require an initial development team to certify to the Commission that the network token and its underlying network have reached "Network Maturity" based on due inquiry and supported by reasonable evidence in line with the criteria specified in the two rules-based tests.

By adopting a revised definition of "Network Maturity" grounded in control-based decentralization and incorporating these four elements, the Commission can provide market participants with a clear, predictable, and objective pathway to compliance—while preserving flexibility for novel architectures. The combination of a principles-based framework with objective rules-based tests would give regulators the tools to assess substance over form and ensure that only systems that have truly eliminated trust dependencies are exempted from the securities laws. This would also provide a foundation upon which the Commission could issue future guidance about control in novel use cases, thereby ensuring that the Proposal can evolve over time. Collectively, this approach would not only enable the Commission to clarify the application of federal securities laws in this domain, but also encourage responsible decentralization and long-term network development in a manner that protects investors and supports innovation.

3. Restructure the Expiration and Exit Mechanisms to Enable Gradual Off-ramping

The Proposal currently provides for an expiration of the safe harbor after three years. If a network has achieved "Network Maturity" during this period, an exit report must be filed that details ongoing development efforts, presumably so that the Commission can determine whether the network token of the network might satisfy the criteria of the *Howey* test and be subject to securities laws following exit from

[45] For a description of these criteria, see Part 3 of our response to **Question #1**. *Id.*, at 7-11.

the safe harbor. If a network has not achieved "Network Maturity," an exit report is filed and registration is required. This construct introduces the same perverse incentives as the 2019 Framework—projects that have achieved "Network Maturity" but that are still subject to ongoing efforts will likely either cease or obfuscate those efforts in order to avoid their network token becoming subject to federal securities laws.

The expiration and exit mechanisms should be modified to better align the incentives of entrepreneurs with federal securities laws, thereby protecting tokenholders.[46] In particular, projects should remain eligible for the safe harbor so long as they have achieved "Network Maturity" during the three-year period. This change would mean that projects have three years to achieve "Network Maturity" (the elimination of control via control-based decentralization), and if control has not been eliminated in that time, projects would exit the safe harbor and become subject to federal securities laws and their potential registration requirements. But if control is eliminated, projects would continue to be eligible for the safe harbor so long as they continue to comply with the disclosure requirements required by the safe harbor and insider selling restrictions (as discussed in Part 5 below). These projects would then only be permitted to forgo such ongoing disclosure requirements and insider selling restrictions once they demonstrate that their ongoing managerial efforts are no longer material to the functioning of the network.

By modifying the "Network Maturity" construct and the expiration and exit mechanisms in this manner, the Proposal would effectively incentivize investor protection through disclosure obligations and insider restrictions pending the elimination of control, while continuing to enable ongoing managerial efforts of builders. Such an approach would address the deficiencies of the 2019 Framework while providing a clear, gradual, and risk-sensitive off-ramp for projects that are progressing toward decentralization. This multi-stage pathway could similarly be used under the Exchange Act, as discussed above in our response to **Question #7**.

4. Limit Aggregate Primary Offering Amounts

The Commission should impose a limitation on the aggregate amount of a given crypto asset that an issuer may sell in reliance upon the Proposal. Most primary offerings of crypto assets in capital raising transactions easily satisfy the criteria of the *Howey* test, meaning that such offerings are typically subject to federal securities laws. Yet the Proposal does not impose threshold caps on the amount issuers can raise. This represents a significant departure from existing exemptions that may apply to issuers raising capital, such as Regulation Crowdfunding ("Reg CF"), without sufficient justification. The Proposal currently only requires that the initial development team *intends* for the network on which the token functions to reach maturity within three years of the date of the first token sale. But *intention* is notoriously difficult to assess and easy to fabricate. This is particularly true under the Proposal, where the only objectively measurable criteria relates to ownership thresholds. Further, unless the Proposal is modified pursuant to our suggestion in Part 1, it would not restrict the type of crypto assets that can be offered.

[46] The gradual exit approach outlined here aligns with the approach outlined in other submissions to the Commission. *See, e.g.*, DeFi Education Fund, *Token Safe Harbor Guiding Principles* (Apr. 18, 2025), https://www.sec.gov/files/ctf-written-input-defi-education-fund-041825.pdf.

Given the foregoing, the Commission should add a limitation on the aggregate amount of tokens that may be sold by an issuer pursuant to the Proposal. For example, imposing a ceiling of $25,000,000 or 10% of the total amount of the then outstanding units of the token would be sufficient to mitigate investor risks while fostering innovation. These thresholds would be simple to administer and enforce, as well as consistent with comparable rules. For example, Reg CF imposes a capital raising limit of up to $5 million within a 12-month period, while also limiting the participation of non-accredited investors based on income or net worth.[47] Likewise, Regulation A imposes a limit of $20 million in a 12-month period in Tier 1, and up to $75 million in a 12-month period in Tier 2.[48] Adding such a limitation would also be consistent with proposed legislation. H.R. 4763, the Financial Innovation and Technology for the 21st Century Act ("FIT21"), for instance, provides that to be exempted from registration under the federal securities laws, "transactions involving the offer or sale of units of a digital asset [...] during the 12-month period preceding the date of such transaction, including the amount sold in such transaction, is not more than $75,000,000" and that, for transactions involving non-accredited investors, "the transaction does not exceed 10% of the person's annual income or net worth."[49]

Ultimately, caps are necessary not only to mitigate investor risk, but also to preserve the broader incentive structure of the Proposal. Without a cap on primary sales, projects may use the Proposal to facilitate large-scale distributions that function more like exit liquidity events than capital-raising transactions intended to fund network development. Worse still, if insiders can freely extract value by receiving revenue or dividends from the issuer or affiliated entity—without ever needing to liquidate tokens—they will have no incentive to pursue investor protection through control-based decentralization (or comply with insider transfer restrictions as proposed in Part 5 below), thereby defeating the very justification for the Proposal's approach to treat network tokens differently from ordinary securities. Caps help ensure that token-based fundraising remains congruent with the goals of decentralization and investor protection, and that the Proposal cannot be used to circumvent disclosure or control-elimination requirements through unchecked token monetization.

5. Incorporate Transfer Restrictions and Limitations on Insider Token Sales

At present, the Proposal provides an exemption from the Securities Act of 1933 for transactions involving tokens that meet certain requirements, including that the "initial development team **intends** for the network [...] to reach Network Maturity within three years" (emphasis added). Conditioning this exemption on the development team's intention is an important means by which the Proposal may promote decentralized innovation. However, as discussed above, an *intention* to eliminate control associated with a network token and its underlying network is not equivalent to having actually eliminated control. While an initial development team retains control of a network token and its underlying network, tokenholders are at the greatest risk of harm stemming from information asymmetries about a project, and

[47] Crowdfunding, Title 17, Code of Federal Regulations, Part 227 (current as of 2024), https://www.ecfr.gov/current/title-17/chapter-II/part-227?toc=1.
[48] Amendments for Small and Additional Issues Exemptions Under the Securities Act (Regulation A), Securities and Exchange Commission, 80 Federal Register 21806 (Apr. 20, 2015), https://www.govinfo.gov/content/pkg/FR-2015-04-20/pdf/2015-07305.pdf.
[49] 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.

the trust dependencies of such network token may be similar to that of an ordinary security. As a result, the Proposal must incorporate additional restrictions and limitations to protect investors from insiders and ensure general congruence with federal securities laws.

Specifically, the Proposal should be amended to expand the definition of "Related Persons" and to subject such persons to transfer restrictions until the network token and underlying network have achieved "Network Maturity" (as modified to focus on the elimination of control):

- The Proposal's existing definition of "Related Person" should be expanded to include parties that are most likely to have access to asymmetric information pertaining to a project, including officers, directors, employees, consultants, advisors, promoters, underwriters, equity and security holders, as well as immediate family members of such persons. Further, a catchall could be included to capture any person who acquires 1% or more of the then outstanding units of a network token from the issuer. The current definition only applies to the initial development team, their immediate family members, and its directors and advisors, which is not sufficient to limit risk to tokenholders more broadly.[50]
- The Proposal should then be modified to restrict the ability of related persons to participate in secondary markets unless certain conditions are met. These conditions should be similar to Rule 144 and include that: (i) current disclosure requirements must be satisfied (as the Proposal requires); (ii) the holder of the network token must hold the asset for not less than 12 months (to guard against underwriting); (iii) "Network Maturity" must be achieved; and (iv) insiders meeting "affiliate" thresholds could be subject to volume and manner of sale limitations. These restrictions would prevent related persons from selling, distributing, transferring, or otherwise disposing of their assets unless the risk of information asymmetries is sufficiently low, such that the trust dependencies associated with the network token are significantly reduced as compared to an ordinary security, thereby justifying the safe harbor from securities laws.

The foregoing modifications would effectively restrict insiders (the persons most likely to exercise control over a network, and therefore, the persons most likely to possess asymmetric information) from participating in secondary markets while a network is still controlled, providing significant investor protection. Simultaneously, it would enable non-insiders (including those receiving airdrops and incentive-based rewards) to participate in secondary markets from the initial launch of the token, thereby providing a pathway to progressive decentralization.[51] Once the network reaches maturity—ensuring that control-based decentralization has been achieved and that minimum disclosures have been provided—insiders are far less likely to possess a competitive informational advantage, thereby minimizing risks to other market participants.

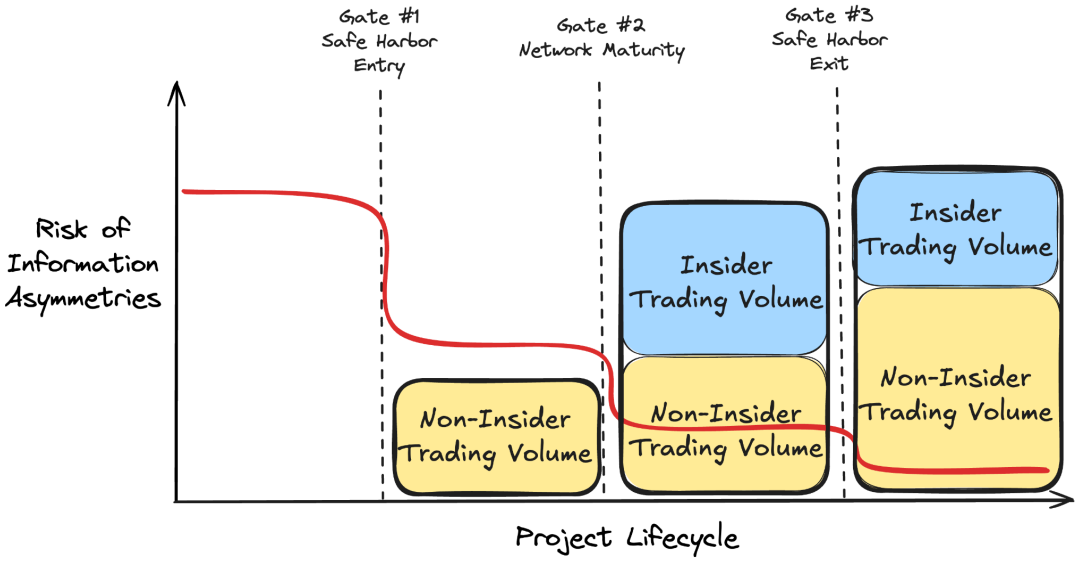
Importantly, for transfer restrictions to be effective, they must be designed to prevent insiders from exploiting any loopholes that would allow them to leverage asymmetric information to the detriment

[50] *Supra* note 29 (defining "Related Person" as "the Initial Development Team, directors or advisors to the Initial Development Team, and any immediately family member of such persons.").
[51] 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/.

of consumers, a consideration that we have elaborated upon elsewhere.[52] While such blanket restrictions on related persons are the most effective way to protect investors against these risks, if the Commission wishes to provide greater flexibility, it could consider allowing certain investors to sell before the network reaches maturity at a restricted rate and subject to certain restrictions, like ensuring disclosure obligations are fulfilled and requiring transaction-based disclosures. Further, in order to prevent persons from gaming the "Network Maturity" concept, any person that exerts control over a network post "Network Maturity" should be restricted from further participation in secondary markets on a similar basis as that described above.

***

As a result of the foregoing changes, the life cycle of a project entering and exiting the safe harbor can be charted against the risk of information asymmetries of its network token, while reflecting market access by insiders and non-insiders:



- **First**, in a project's initial stage, it could raise seed capital via private placement pursuant to existing securities laws. During this phase, the risk of information asymmetry is highest and securities laws most clearly apply to investments in the project, but no network token has been launched and no secondary markets for such token exist.
- **Second**, upon entry into the safe harbor (**Gate #1**), a project would begin providing disclosures pursuant to the Proposal, thereby lowering the risk of information asymmetries. During this stage, projects could launch their network token and conduct airdrops, incentive-based rewards, and crowdfunding activities all in compliance with the Proposal. However, because the project's network and network token could still be at risk of being under significant influence or control during this stage, insiders would be restricted from participating in secondary markets and taking advantage of potential information asymmetries arising from such control.
- **Third**, upon the achievement of "Network Maturity" (**Gate #2**) within three years of entering the safe harbor, the trust dependencies and information asymmetries arising from control would be eliminated, and insiders would be able to participate in secondary markets.

[52] Jennings et al., *supra* note 27.

- **Fourth**, upon the cessation of any ongoing managerial efforts, a project could exit the safe harbor (**Gate #3**). At such time, disclosures would no longer be necessary as the risk of information asymmetries with respect to the network token would be no different than an ordinary commodity.

By conditioning market access on the risk of information asymmetries dissipating, this framework ensures that market participation expands only as the trust dependencies associated with the network token diminish. In doing so, it supports progressive decentralization, guards against get-rich-quick schemes fueled by insider advantage, and provides a measured, compliance-friendly pathway for projects to responsibly transition from centralized development to fully decentralized public infrastructure.

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

Yes, the Commission should seek to provide both transitional relief (for projects that intend to meet the distribution requirements of Rule 195 on a go-forward basis) and post-hoc relief (for projects that may not meet the distribution requirements of Rule 195, but do meet certain specified criteria established by the Commission).[53]

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

The Proposal includes several helpful disclosure obligations—including source code, transaction history, and token economics (i.e., "tokenomics")—but its current framework is incomplete and insufficient to adequately inform market participants. As we have emphasized in our responses to **Question #1** in our initial submission, and **Questions #7** and **#8** above, disclosure requirements should be tailored to address the unique risk profile of blockchain-based systems and, in particular, the control and ongoing managerial efforts that may persist after launch for projects that are pursuing progressive decentralization.

Our position is similar to and builds on the work of other industry leaders. As Professor Chris Brummer has argued in his work on developer-centric disclosure,[54] disclosure for blockchain projects must evolve to meet the needs of decentralized systems. Brummer proposes that disclosure should prioritize governance, incentives, token economics, and protocol design—areas that impact investor risk in ways that traditional SEC forms were not designed to capture. Attorney Rodrigo Seira has likewise emphasized that project-specific context and decentralized architecture must guide disclosure obligations

[53] *See* Sarah Brennan, *2025 Safe Harbor Framework Overview*, https://www.sec.gov/files/ctf-input-brennan-2025-03-10.pdf.
[54] Chris Brummer, *A Developer Theory of Disclosure* (Feb. 14, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5137972.

if registration is to become a meaningful option for crypto asset issuers.[55] We agree and believe that the Proposal should reflect this evolution.

Disclosure requirements under the Safe Harbor should therefore be designed to address material trust dependencies, particularly those related to (1) centralized control and (2) ongoing managerial efforts. If a network is decentralized and free of ongoing managerial efforts, the need for ongoing disclosure disappears. Until that point, however, projects should provide material updates on governance, token allocation, control structure, and any ongoing risks related to insider influence or protocol development.

As outlined in our response to **Question #8**, disclosures should be provided both at the time of sale and on an ongoing basis—but only so long as the project remains subject to meaningful control or ongoing managerial efforts. Once a project achieves Network Maturity and demonstrates the elimination of both control and ongoing managerial efforts, ongoing disclosures are no longer necessary. All information about the network and its token should be publicly and transparently available onchain. This approach is consistent with Coinbase's recommendations in its response to the Request, which similarly proposes a tailored, risk-based disclosure regime that focuses on project-specific information such as token governance, source code, token economics, and decentralization plans, and supports the suspension of ongoing reporting once decentralization is achieved.[56]

We have provided the categories of information and subsets thereof that we believe would provide token purchasers with the necessary tools to assess risks related to control, governance, and ongoing activity in **Annex A** hereto.

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

Yes, the Commission should modify the "Network Maturity," expiration and exit mechanisms to align with the Proposal's current control-based decentralization framework with objective control criteria. See Parts 2 and 3 of our response to **Question #10**. For a broader discussion of control-based decentralization, see Part 1 of our response to **Question #1** in our initial submission, as well as our responses to **Questions #13a** and **#13b**.

Question 13a: Is dispersion of control a better framework than decentralization? If so, how should ownership of governance tokens and voting rights be considered in assessing dispersion of control? How should the delegation of voting rights be taken into account?

---

[55] Justin Slaughter, Katie Biber & Rodrigo Seira, *The Current SEC Disclosure Framework is Unfit for Crypto* (Apr. 20, 2023), https://www.paradigm.xyz/2023/04/secs-path-to-registration-part-iii.
[56] Coinbase Global, Inc., *There Must Be Some Way Out of Here: Recommendations on the Regulation of Digital Securities Markets* (Mar. 19, 2025), https://www.sec.gov/files/ctf-input-grewal-2025-3-19.pdf.

While the broad distribution of token ownership and governance rights is helpful, it is insufficient on its own to eliminate the investor protection concerns that animate the securities laws. As the Commission has recognized in other contexts, interests in partnerships—where ownership and governance are widely held—can be securities. The same logic applies in the blockchain context. Projects that are operationally and economically controlled—even if token ownership is dispersed—can still present many of the same trust dependencies and risks as centralized enterprises. For example, even if voting control (governance tokens and/or voting rights) is dispersed, a network could still contain hard-coded permissions that allow a single party to deplatform users and extract value. Or consider a blockchain system that is broadly owned and nominally governed by a dispersed community. Even if no single entity controls a majority of governance tokens, the system could still impose significant risks if, for example, a developer retains a privileged key that enables arbitrary protocol upgrades that modify network behavior or access to user wallets. These systems, despite being dispersed, would retain all the hallmarks of a centralized intermediary or principal—just without a visible corporate wrapper.

By contrast, systems built using blockchain technology are uniquely able to *eliminate* trust dependencies in a manner that is impossible with traditional technologies and a significant improvement over other systems that only allow for dispersion of control. This is because blockchain technology empowers users with direct agency rather than requiring that agents act on their behalf. When blockchain systems are open source, autonomous, permissionless, credibly neutral, non-custodial, and economically independent, they can remove all meaningful trust dependencies, even if a small number of actors continue to participate in the ecosystem. This removes intermediary-related risks—such as conflicts of interest, value extraction, and information asymmetries—that often trigger the application of federal securities laws that simply cannot be eliminated through the dispersion of control.

This *elimination* of control cannot be achieved with traditional technologies. For example, Meta controls the application WhatsApp and can modify the risks associated with using the messaging platform by corporate fiat, including by ousting users from the platform. Meta's own ownership may be distributed and ownership of WhatsApp could even be distributed, but only with blockchain technology could control-related risks be eliminated. A similar dynamic can be seen in emerging federated platforms like BlueSky. While these systems may appear decentralized because they allow for multiple independently operated servers, they often fail to eliminate control—they simply distribute it across semi-centralized domains. In practice, users still rely on administrators who can impose discretionary rules, moderate access, or exercise de facto custody over content and metadata. The result is a network of feudal intermediaries, where power is fragmented but not eliminated. These systems remain susceptible to many of the same trust dependencies—such as censorship risk, gatekeeping, and value extraction—as traditional social media platforms. In contrast, a truly decentralized protocol removes these risks not by dispersing control among smaller intermediaries, but by eliminating the capacity for unilateral decision-making altogether. This distinction—between distribution and disintermediation—is fundamental. Ultimately, whoever controls the system (whether that be an individual or many people), can uniquely affect or structure the risk associated with that system.

For the foregoing reasons, we urge the Commission not to overindex on the dispersion of control as a proxy for decentralization. In order to justify a different treatment of network tokens from ordinary securities under federal securities laws, a control-based decentralization framework must be defined to

mean the elimination of control, not just its dispersion. Dispersion is not equivalent to elimination, and it fails to capture several critical mechanisms of control that must be removed to mitigate investor risk. These include:

- **Operational control** – The ability of one or more persons to unilaterally change network rules or smart contract logic (e.g., via upgrade keys or admin permissions) to access, freeze, or reallocate user assets, or to prevent users from interacting with the system or arbitrarily alter their permissions.
- **Economic control** – The ability to influence or determine the value that accrues to the system's asset or the utility of such asset (e.g., changing economic mechanisms like fee models or manipulating treasury assets).
- **Voting control** – The ability to use concentrated influence over decentralized governance systems to change the functioning of the system.

Where systems eliminate these mechanisms of 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. But a credible decentralization framework must require the elimination of all such mechanisms of control.

Accordingly, we recommend that any control-based decentralization framework adopted by the Commission: (1) focus on the elimination—not merely the dispersion—of control; (2) require disclosures sufficient to evaluate whether the system is operationally, economically, and politically controlled; and (3) as proposed in our response to **Question #10**, enable projects to exit compliance obligations only after control and ongoing managerial efforts have ceased. Dispersion of control may be a helpful indicator, but it is not a sufficient threshold for excluding a project from the application of federal securities laws. Decentralization must be functional and structural, not just optics. A blockchain network should be considered "mature" only when it has eliminated all mechanisms of centralized control, consistent with the objective criteria we outline in our response to **Question #14**.

Question 13b: If an exit marker is achieved, who should be responsible for notifying the Commission?

As discussed in Part 3 of our response to **Question #10**, the exit criteria should be modified to permit issuers to remain in the safe harbor so long as (1) control-based decentralization is achieved within three years and (2) ongoing managerial efforts continue. Under this framework, the issuer should be responsible for notifying the commission once the exit criteria have been achieved.

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

The decentralization of a deployed protocol should be evaluated using a control-based decentralization framework—where control is eliminated, the trust dependencies of an arrangement are

reduced such that the application of federal securities laws is unwarranted. As discussed in Part 2 of our response to **Question #10**, this framework could be constructed to include a top-level principles-based test focused on control, with rules-based safe harbors identifying criteria that, if satisfied, would establish that a system is not controlled. There are potentially many ways to define the elimination of control in the context of a blockchain system, so this kind of pairing would provide market participants with a clear, predictable, and objective pathway to compliance—while preserving flexibility for novel architectures.

We believe the following seven criteria are the most effective, comprehensive, easily verifiable, and broadly applicable criteria that could be used for purposes of a control-based decentralization framework:[57]

1. Open source
2. Autonomous
3. Permissionless
4. Credibly neutral
5. Non-custodial
6. Economically independent
7. Distributed

Each criterion mitigates a specific category of control-related risk. As elaborated in **Question #13a**, this framework must be applied holistically—not in a piecemeal fashion—because each mechanism of control introduces distinct risks. A system that has distributed governance tokens, but remains operationally dependent on a single entity, may still retain many of the trust dependencies that the federal securities laws are designed to address. Similarly, a system that has eliminated operational and voting control, but where the economic value of a network token is still dependent on a single entity, would likewise expose market participants to risks that warrant the application of federal securities laws. Importantly, these criteria are verifiable at the code or network level, making them practical for implementation and oversight. Below, we explain why each mechanism of control introduces risk and why its removal is necessary to establish that a protocol has achieved decentralization.[58]

1. Open Source

Open source means that a blockchain network's source code is open source and freely and publicly available to all. A blockchain system that is not open source creates reliance on a centralized operator and deprives users of the ability to inspect, verify, or fork the network. Open source networks enable participants to independently evaluate decentralization claims and freely exit by migrating to systems that are derived, or "forked," from it. This promotes transparency, accountability, and user choice, and ensures that intellectual property rights are not used as indirect mechanisms for value extraction from tokenholders. Each of these benefits reduce control-related risk.

[57] For more discussion of these criteria, see: Decentralization Research Center, *Designing Policy for a Flourishing Blockchain Industry* (Apr. 29, 2025), https://thedrcenter.org/wp-content/uploads/2025/04/DRC-Flourishing-v2.pdf.
[58] See our response to **Question #10** for a discussion of how these criteria could form the basis of a certification regime for Network Maturity under the Proposal.

2. Autonomous

Autonomous means that the blockchain network 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. This removes single points of failure and limits the ability of any actor to alter network behavior through discretionary control. Autonomy need not exclude human involvement entirely so long as it is rule-bound, transparent, and non-discretionary, and therefore does not amount to a unilateral authority to alter the functionality, operation, or rules of the system. This significantly diminishes control-related risks for all participants.

For example, traditional internet protocols—such as TCP/IP, HTTP, and DNS—are considered autonomous despite ongoing human input through standard-setting organizations like the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). While these bodies propose updates and maintain protocol standards, they do not exercise discretionary control over individual user interactions with the system. Once implemented, the protocols function according to transparent, predetermined rules without requiring human intervention to validate or process each transaction. Similarly, blockchain networks can retain their autonomy even if human actors contribute to protocol upgrades.

3. Permissionless

Permissionless means that 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.

If a tokenholder's ability to use or participate in a blockchain network can be unilaterally restricted, then they face significant control-related risks due to the lack of transparency, as well as the potential for censorship and collusion. A third party with such authority could exercise it arbitrarily, undermining user rights and enabling value extraction from tokenholders. In contrast, where no such control exists, tokenholders are free to engage with the network on their own terms and can enter or exit the system at any time, thereby reducing risks associated with information asymmetries, conflicts of interest, and centralized control. As such, it is crucial that permission-based mechanisms of control are eliminated to protect users. Notably, this criterion derives from legislation, having originally been proposed as part of FIT21.[59]

4. Credibly neutral

Credibly neutral means that 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.

[59] 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.

Credible neutrality is a core advantage of decentralized blockchain networks compared to closed, controlled systems. Because blockchain networks can make verifiable guarantees about how they operate, they eliminate the potential for arbitrary or discriminatory treatment of specific users or use cases, thereby ensuring broad and equitable access. In contrast, systems that lack credible neutrality inherently favor certain participants over others, fostering environments where information asymmetries and value extraction are more likely to occur. Neutrality fosters fair access, open competition, and system integrity—key values aligned with investor protection.

5. Non-custodial

Non-custodial means that users retain full control over their assets. In the context of blockchain systems, that requires that the system provide users with exclusive control over their assets via private keys. This removes reliance on intermediaries and reduces risks of misappropriation, censorship, and loss. The Financial Crimes Enforcement Network's 2019 guidance applies a similar "total independent control" test, which is relevant in assessing this criterion.[60] Key factors of a system being non-custodial include that: (a) the value remains under the ownership of the user; (b) the user initiates transactions by interacting with software or technology and providing the necessary credentials; and (c) any third party offering software tools, validation, or auxiliary services at the user's request does not possess total independent control over the assets involved. Technologies that meet these conditions ensure that no intermediary possesses the power to unilaterally steal user funds, which is a mechanism of control that substantially impacts the risk associated with a given network and its underlying token.

6. Economically independent

Economically independent means that the economic mechanisms of the system that are designed to drive the value of any network token of the system are functional and not dependent on any development company or issuer, or any exclusive offchain service provider or gatekeeper. Because network tokens derive their value from the operation of the underlying blockchain network, it is essential that value-generating mechanisms be implemented in a way that reduces control-related risks for tokenholders. A foundational example of such economic independence is a blockchain that enables tokens to be redeemed for digital products or services—such as paying gas fees on a layer-1 blockchain.[61] This mechanism effectively embeds supply-and-demand dynamics into the network token, grounding its value in network activity. Similarly, a token that derives its value via a smart contract fee mechanism that collects fees on every smart contract transaction would be economically independent so long as such transactions are not dependent on an exclusive offchain service provider or gatekeeper. By contrast, in cases where a centralized team has not yet deployed economic functionality or where such economic functionality is dependent on an exclusive offchain service provider or gatekeeper, the network token's value is more vulnerable to information asymmetries, manipulation, and misaligned incentives. As such, the implementation of a robust token economic model that is independent of any person or service provider substantially mitigates risks to market participants—not only does it remove risk, but also by

[60] United States Department of the Treasury, Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.
[61] *What are gas fees?*, Coinbase, https://www.coinbase.com/learn/crypto-basics/what-are-gas-fees.

anchoring profit expectations to the functioning of the blockchain network itself, rather than to any centralized company.

7. Distributed

Distributed means that 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. When a person or group under common control can unilaterally alter a blockchain network, it introduces significant risks related to information asymmetries, conflicts of interest, inadequate disaffiliation, and value extraction. This criterion was initially proposed in FIT21,[62] as well as in Commissioner Peirce's Token Safe Harbor Proposal.[63]

***

Each of the foregoing criteria addresses a distinct class of trust dependency. A protocol that satisfies all seven criteria substantially reduces the risks that federal securities laws are designed to address, and should be treated accordingly. By contrast, a system that falls short on even one dimension may retain concentrated power and impose risks on participants, despite appearing decentralized.

Importantly, in creating statutory definitions of these criteria, certain concessions must be made for decentralized governance systems. In particular, in adopting any control-based decentralization framework, the Commission should permit delegations of certain functional and administrative authority to decentralized governance systems as well as subdelegations of such authority to persons acting on behalf of such systems, so long as such delegations meet certain specified criteria that do not fundamentally conflict with or undermine the principles of control-based decentralization. For example, such decentralized governance systems themselves should not be subject to unilateral control of any person(s), delegations should generally be codified in protocol rules, enforceable via verifiable mechanisms, limited in scope, and narrowly defined, ensuring that any persons acting on behalf of a decentralized governance system can be held accountable to it. These types of governance mechanisms are critical not only for safeguarding the security of blockchain networks in emergency scenarios but can also help to ensure efficient operation, such as in the case of oracles. As a result, the Commission should take a permissive view with respect to such delegations so long as they do not expose tokenholders to undue risk that the application of federal securities laws might otherwise ameliorate.

[62] 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.
[63] Statement, Securities and Exchange Commission, Hester M. Peirce, Token Safe Harbor Proposal 2.0 (Apr. 13, 2021), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-token-safe-harbor-proposal-20.

IV. 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, Head of Policy & General Counsel
a16z crypto

Jai Ramaswamy, Chief Legal Officer
a16z

Scott Walker, Chief Compliance Officer
a16z

Michele R. Korver, Head of Regulatory
a16z crypto

ANNEX A

Network Token & Blockchain Disclosure

The categories identified below focus on the information most relevant to token purchasers in early-stage blockchain projects. They are designed to surface risks related to control and ongoing managerial efforts. We view the risks arising from control to be more significant than ongoing managerial efforts, because while a dependence on the ongoing managerial 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. Control and ongoing managerial efforts are the principal sources of trust dependencies and risk in early-stage blockchain projects, and the disclosures we propose are targeted at those dependencies—rather than attempting to replicate corporate-style financial reporting obligations that may not apply. These categories are generally consistent with frameworks proposed by market participants, including Coinbase, which has advocated for a flexible, disclosure-based exemption grounded in decentralization milestones and the public availability of core technical and economic information.[64]

- **Token issuer, related persons, and development team information.** Information sufficient to assess:
    - The issuer's executive officers, directors, and related persons who would provide essential ongoing efforts towards the creation and development of the crypto asset and its associated blockchain network.
    - Other relevant third parties or affiliates that provide essential ongoing efforts towards the development of the token or associated network.

- **Development plan.** The current state and timeline for the development of the network to demonstrate how and when the initial development team intends to achieve Network Maturity (as redefined per our response to **Question #10**), including anticipated development costs relative to the amount of funding sought or secured and the anticipated use of proceeds raised in the offering including as relevant:
    - Plan of distribution for tokens sold in the offering.
    - Control-based decentralization plan.
    - Description of native blockchain to the extent one exists for a token.
    - Anticipated post-launch support activities.
    - Existence of critical operational dependencies that may persist offchain.
    - Development team statement of the risk associated with the above plan.

- **Source code and cybersecurity.** The source code and cybersecurity information pertaining to any blockchain system to which the token relates:
    - Blockchain level source code details, including permissions (to enable the ready evaluation of whether parties can make additional changes without approval).

---

[64] Coinbase Global, Inc., *There Must Be Some Way Out of Here: Recommendations on the Regulation of Digital Securities Markets* (Mar. 19, 2025), https://www.sec.gov/files/ctf-input-grewal-2025-3-19.pdf.

- Information pertaining to hacks or other previous security issues relevant to the token and its associated network.
- Results of any completed third party audits.

- **Token governance.** Information pertaining to:
  - Governance mechanisms for implementing changes to the associated network or forming consensus among holders of such network tokens, including any decentralized governance system.
  - Smart contract governance control mechanisms and permissions, including if a specific person possesses material influence, authority, or control over permissions.
  - If, how, and when the token issuer intends for the blockchain system to become decentralized, and a review of progress achieved in fulfilling the criteria required for certification.

- **Token Economics & Allocations.** Network token supply and distribution information, pricing, lockups, and release schedules, including:
  - Current circulating supply and total token supply.
  - Information explaining the token launch and supply process and amount, including the number of tokens to be issued in an initial allocation, the total number of tokens ever to be created on the associated network, the release schedule for the tokens, the total number of tokens then outstanding, and other details regarding whether the token supply is intended to be inflationary vs. deflationary and whether issuance is intended to be fixed vs. variable.
  - Allocations and prior sales to the issuer, initial development team, and other related persons (as defined in our response to **Question #10**), as well as any rights held by such persons. Details pertaining to any limitations on token sales by the initial development team or related persons, including unlock schedule.
  - Projected distribution of token rewards, if any, whether through staking, reallocation of network fees, or some other mechanism.
  - Description of how the issuer or relevant governing body will manage and use tokens held in "treasury" or by "Foundation" or any other similar arrangement.
  - Description of any retail purchaser offering limit.
  - Information explaining the primary economic mechanisms of the network token, including information on token rewards for any applicable consensus mechanism or process for validating transactions, method of generating or mining network tokens, and any process for burning or destroying tokens on the blockchain system.
  - Sufficient information for a third party to create a tool for verifying the transaction history of the token.

- **Additional disclosures.** Description of any:
  - Material conflicts of interest and related party transactions.
  - Material agreements the issuer has entered into with respect to the development and ongoing support of the tokens or associated network.