ANDREESSEN HOROWITZ

July 31, 2025

BY EMAIL

Senate Banking Committee
United States Senate
Washington, DC 20510

Re: Response to the Senate Banking Committee Digital Asset Market Structure Request for Information

Dear Chairman Scott, Senator Lummis, Senator Hagerty, and Senator Moreno,

Andreessen Horowitz ("a16z") appreciates the opportunity to provide comments on the questions that the Senate Banking Committee ("Committee") provided to the public on July 22, 2025 alongside the market structure discussion draft (the "Discussion Draft").[1] The Committee's thoughtful approach, seeking detailed and comprehensive information about a wide range of digital asset market structure issues, is laudable. We commend the Committee 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 Committee, we are deeply committed to the development of a market structure framework for digital assets, which we believe is critical to fostering innovation while protecting market participants. Our many publications on regulatory approaches, as well as our ongoing engagement with policymakers and regulators reflect this commitment.[2] To that end, we hope that our observations, drawn from our deep experience, can be of assistance to the Committee. We believe that time is of the essence in these endeavors, so in what follows we respond to the questions where our expertise is most relevant.

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. As of 2025, a16z 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.

[1] Majority Press Release, United States Committee on Banking, Housing, and Urban Affairs, Scott, Lummis, Colleagues Release Market Structure Discussion Draft, Issue Request for Information from Stakeholders (July 22, 2025), https://www.banking.senate.gov/newsroom/majority/scott-lummis-colleagues-release-market-structure-discussion-draft-issue-request-for-information-from-stakeholders.

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

II. Responses to Committee Questions #1 - #6

Question 1: The proposed legislation aims to provide clarity on how to allocate jurisdiction over digital assets between the CFTC and the SEC. Does the legislation strike the right balance?

Yes, if appropriately narrowed and aligned with existing legal principles. The legislation moves in the right direction by affirming that primary sales of digital assets should be treated as securities transactions, while secondary sales of digital assets should fall within the CFTC's jurisdiction, subject to appropriate disclosures. This allocation mirrors the framework set forth in the Digital Asset Market Clarity Act of 2025 (the "CLARITY Act" or "CLARITY")[3] and aligns with longstanding principles of functional regulation. It preserves the role of the Securities and Exchange Commission ("SEC" or the "Commission") in protecting investors while recognizing that certain digital assets can function more like commodities over time.

However, to strike the right balance, Congress should:

- Adopt CLARITY or combine CLARITY's narrow and precise "digital commodity" construct with the structural simplicity of the ancillary asset construct (**Question #1a**).
- Bolster the Discussion Draft's implementation of the *Howey* test to eliminate loopholes in the current framework (**Question #1b**).
- Recognize *Howey* and its progeny as the legal standard for investment contracts, potentially codifying their economic reality focus and resist efforts to weaken the utility of this case law by taking a more formalistic approach (**Question #1c**).
- Clarify other definitional terms (e.g., "note") to avoid future regulatory overreach while maintaining protections (**Question #1d**).
- Implement a token taxonomy that focuses primarily on areas where new regulatory treatment is needed (**Question #1e**).
- Ensure infrastructure functions like staking, mining, and smart contract execution are regulated as financial services only when tied to intermediary control (**Question #1f**).
- Allow legacy blockchain projects to transition into compliance under a structured regime that includes mandatory disclosures and objective decentralization milestones (**Question #1g**).
- Provide retroactive relief for prior technical violations only for projects that come into compliance, while excluding fraud and primary fundraising activity (**Question #1h**).

Together, these reforms would modernize the regulatory landscape while protecting consumers, preserving U.S. capital markets, and enabling blockchain innovation to flourish in a legally durable way.

a. Should legislation rely on the concept of ancillary assets? If so, is the definition in proposed Section 4B(a) of the Securities Act appropriate? Does it exclude the right categories of assets?

The ancillary asset construct should not serve as the foundation for legislation without significant modifications. While there are many benefits in the simplicity of the approach, as we explain below, the "ancillary asset" definition as currently constructed would either enable issuers of traditional securities to

[3] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress (2025), https://www.congress.gov/bill/119th-congress/house-bill/3633.

circumvent investor protections or would introduce new ambiguities that compound the problems resulting from the *Howey* test. Such an approach will not resolve the challenges facing crypto market participants. As a result, the Committee should modify the ancillary assets construct to preserve its simplicity, while adopting the precision and certainty of the "digital commodity" construct of the CLARITY Act, which the President's Working Group on Digital Assets has called "[...] an excellent foundation for digital asset market structure in the United States."[4]

Background on Unique Characteristics of Digital Commodities

CLARITY's strength lies in its narrow and precise approach that prioritizes substance over form and provides a clear pathway for entrepreneurs to operate within the bounds of the law. It achieves this by focusing exclusively on a unique category of digital assets that do not fit within existing securities laws—digital commodities (also called "network tokens")[5]—without undermining the core protections provided by the securities framework.

Digital assets (or "tokens") serve many purposes. Some are tied to stable value, like stablecoins. Some represent digital collectibles, like non-fungible tokens ("NFTs"). But the most economically significant use-case is that of digital commodities—tokens that provide ownership rights (economic, participation, governance, etc.) in the blockchain systems to which they relate. This category includes the vast majority of valuable, widely-used tokens, including BTC (Bitcoin), ETH (Ethereum), and many others.

Because digital commodities provide their holders with ownership rights in a blockchain system, they may at first glance resemble shares of stock which give holders ownership rights in a company. But under scrutiny this comparison breaks down quickly. Investing in Apple stock means placing trust in Apple's management and board—individuals with control over business decisions, operations, and financial reporting. As a result of this control, Apple's management has access to material non-public information (e.g., quarterly sales or strategic plans) that gives rise to information asymmetries between the company and the market. Securities laws are designed to address precisely this gap through robust disclosure obligations.

By contrast, ownership of a digital commodity such as BTC or ETH provides certain ownership rights with respect to the asset's underlying decentralized, public blockchain system. These systems do not have CEOs, boards, or insiders with privileged access. They function absent human intervention and control, and their operational state is public and verifiable through onchain data. There are no quarterly earnings surprises, because there is no issuer with confidential business information. As a result, the risk

[4] Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto/.

[5] Under the CLARITY Act, a "digital commodity" is defined as "a digital asset that is intrinsically linked to a blockchain system, and the value of which is derived from or is reasonably expected to be derived from the use of the blockchain system." Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress (2025), https://www.congress.gov/bill/119th-congress/house-bill/3633. In the President's Working Group on Digital Assets, a "network token" is defined as "[...] a token that is intrinsically connected to the functioning of a decentralized network or protocol." The report goes on to elaborate that "Importantly, to the extent that a token's network is sufficiently decentralized, its continued value is not dependent on the intervention or control of a single person or group." Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto/.

profile of digital commodities is fundamentally different from that of traditional securities. Even the SEC under Chairman Gensler acknowledged that BTC and ETH operate more like commodities than securities and that their investors do not need the protections of traditional disclosure regimes.

Yet the dividing line between when a digital commodity behaves like a security and when it behaves like a commodity is unclear because, as the President's Working Group on Digital Assets suggests, its risk profile can change over time depending on whether its underlying blockchain system is centralized (controlled by an individual or a group of coordinated actors) or whether it is decentralized (not controlled by anyone other than its broad community or users).[6] Although blockchain-based projects may start out with tokens that pose securities-like risks—by virtue of having centralized teams, managerial efforts, and information asymmetries—they can evolve into decentralized systems that no longer pose those risks. This dynamic is unique to blockchain systems and digital commodities. **They are the first digital networks that can truly function in a decentralized and autonomous manner, absent any need for human intervention and control.** It is this breakthrough that necessitates tailored treatment under federal securities laws.

Comparison of CLARITY and the Discussion Draft Approaches

The CLARITY Act addresses the novel nature of digital commodities through a principled regulatory framework built on a narrowly-tailored and precise definition of "digital commodity" that constrains the framework's suitability to only those digital assets that provide ownership rights in decentralized blockchain systems. This includes digital assets that have economic rights in a blockchain system's functioning, like ETH, and the definition makes allowances for decentralized governance systems. The digital commodity definition further excludes assets that function as securities or that have securities-like characteristics. Through this approach, CLARITY provides regulatory certainty to entrepreneurs building blockchain systems and preserves the core architecture of securities laws, ensuring that the new regulatory framework is not used to circumvent securities laws.

In contrast, the definitional approach to "ancillary assets" proposed in Section 4B(a) of the Discussion Draft lacks specificity and creates ambiguities. Rather than narrowly targeting digital commodities, it creates a new regulatory framework for any asset that was once the object of an investment contract. This could apply not only to digital commodities, but to any commodity or, indeed, essentially any asset ever sold in an investment scheme. Such a sweeping change to securities law introduces significant uncertainty and goes far beyond what is necessary to resolve the questions posed by digital assets and blockchain technology. As a result, this approach risks eroding federal securities laws without any tangible benefit.

In addition, the ancillary asset construct's definitional exclusions are formalistic and fragile. Section 4B(a) excludes from the definition of "ancillary asset" only those assets that confer formal rights—such as equity, dividends, or liquidation preferences. This approach reverses the bedrock principle of U.S. securities law that form must yield to substance. As articulated in *Howey*, the test for an

[6] The report asserts that "Efforts to regulate network tokens should focus on ensuring that tokens, even if initially issued as part of an investment contract in a securities transaction, are not classified as securities once the network becomes fully functional and sufficiently decentralized." Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto/.

investment contract is based on economic realities, not labels or formal contractual terms.[7] What is primarily at issue in determining whether the transaction in a particular asset, including digital commodities, involves the sale of a security is not the asset itself, but how it is being sold, the economic and non-economic attributes of the arrangement, and the reasonable expectation of purchasers.[8] But the ancillary asset construct's prioritization of form over substance invites circumvention by encouraging issuers to create synthetic securities that function like investments but avoid customary labels. This invites abuse: issuers can design investment schemes that avoid securities regulation simply by omitting formal legal rights, despite replicating the economic realities and risks that securities laws are intended to capture.

So, whereas CLARITY is limited to a ***single asset class***—digital commodities—and then further constrains that class by excluding digital commodities that have ***securities-like qualities in substance***, the ancillary asset construct in the Discussion Draft permits ***all assets*** to be "ancillary assets" and then excludes only certain assets that have ***securities-like qualities in form***. The expansive scope of the ancillary asset construct thus increases the risk of unintended consequences, regulatory circumvention, and market abuse. This is not only a flawed way to approach the regulation of digital assets, it also opens the door to weakening the U.S. securities laws protections for any nontraditional investment opportunities sold pursuant to investment contracts.

These risks are not theoretical. The shortcomings of an expansive and form-over-substance approach are illustrated by the FTT token, the defunct FTX's exchange token. FTT holders were not granted any "right" to the profits of FTX, but the economic reality was that FTX publicly committed to using exchange revenues to buy and burn FTT in order to drive up its price, creating the expectation of profit from the managerial efforts of FTX. Investors priced the token accordingly, and when FTX collapsed, the token—and its holders—were wiped out. The risks embedded in that type of economic relationship are exactly what the securities laws are designed to mitigate: individuals that invested in FTT were exposed to the risk of information asymmetries about FTX (the public did not know that FTX was committing widespread fraud), and those information asymmetries eventually resulted in investor harm. Yet under a formalistic interpretation of the ancillary asset definition, FTT would have been excluded from securities laws as an "ancillary asset" because no formal "right" was conferred to FTT tokenholders.[9] By comparison, FTT would *not* qualify as a "digital commodity" under CLARITY.

The risk is not limited to just one failed exchange. On a go-forward basis, this ancillary asset construct could enable synthetic securities like FTT to propagate. For example, with the rise in popularity of stablecoins, many businesses are beginning to accept stablecoin payments to access and use software (like AI agents). Under the ancillary asset construct, these businesses would be able to tokenize ownership of the smart contracts that underpin the stablecoin businesses, effectively routing some percentage of inbound revenues relating to their offchain businesses to tokenholders, much as FTX did with its exchange revenues. These schemes would effectively function as a securitization of the underlying software products, without granting any "rights" in a "person," but they could potentially make use of the ancillary asset construct to avoid securities laws. This is a bad result, as such arrangements pose all the hallmark risks of securities—any company controlling such products could

[7] 328 U.S. 293 (1946).
[8] *Id*., at 298.
[9] Miles Jennings, Scott Duke Kominers & Eddy Lazzarin, *Network Tokens vs. Company-Backed Tokens* (Mar. 5, 2025), https://a16zcrypto.com/posts/article/network-tokens-vs-company-backed-tokens/.

unilaterally alter the risk associated with token ownership, including by shutting down the product, and investors would be subject to significant information asymmetry risks. Yet if enacted as written, a formalistic interpretation of the ancillary asset definition would invite precisely this kind of abuse. By contrast, due to its narrow construction of the term "digital commodity," the CLARITY Act avoids this risk.

Ultimately, taking an expansive approach that prioritizes formalistic requirements over substance would be a grave mistake. Allowing issuers of securities to circumvent securities laws merely through superficial structuring (i.e., not granting formal rights, but creating expectations of investment returns based on their ongoing efforts) threatens investor protection, market integrity, and the credibility of the securities regulatory framework itself. This risk extends far beyond digital assets, threatening to undermine the very foundation of the U.S. capital markets.

Proponents of the proposed ancillary asset construct may challenge the notion that it is formalistic, and instead argue that it is substantive—that its use of words like "rights" and "interest" give the SEC sufficient flexibility to target projects that use superficial structuring to circumvent securities laws by probing the economic reality of those structures. That interpretation may be correct, but the fact that reasonable minds can disagree about whether the definition is formalistic or substantive means there is significant risk of future regulatory uncertainty.

Further, even if the substantive interpretation is correct, then the ancillary asset construct reintroduces the same subjectivity that has plagued *Howey*—empowering the SEC to make a subjective determination as to whether or not securities laws apply to a given asset. This does not resolve the current regulatory uncertainty under the *Howey* test; it compounds it. Specifically, under this framework entrepreneurs would be confronted with the ambiguity of the *Howey* test in determining whether their initial offering was an investment contract, as well as a new ambiguous test relating to whether the assets originally offered as part of an investment contract are "ancillary assets." Moreover, this new second test would not even have the benefit of decades of *Howey* case law. This is a significant step backwards in the arena of regulating digital assets—as noted earlier, because any asset can be sold pursuant to an investment contract, the approach invites regulatory arbitrage for all types of novel fundraisings.

Further, if the ancillary asset construct does prioritize substance over form, then the ambiguities of the definition necessitate that digital commodities be granted a specific safe harbor from being excluded from the definition of "ancillary asset." This is precisely the approach that the CLARITY Act took, and CLARITY achieved this without overhauling existing securities laws only to produce a subjective and untested framework for investment contracts.

Section 104 of the Discussion Draft proposes to provide this safe harbor for digital commodities, but it does so in a far less effective way than CLARITY. It grants the SEC significant discretion to dictate whether digital commodities qualify as ancillary assets, particularly when those assets grant holders ownership rights regarding the underlying blockchain system. Further, the rulemaking instructions include no allowances for decentralized governance or legal entities that may be used by decentralized governance, which could effectively ban such activities. This broad authority would enable the SEC to continue treating such assets as securities—even when they relate to decentralized systems—merely because they incorporate certain economic features or utilize governance. This not only contravenes the recommendations of the President's Working Group on Digital Assets, but also effectively invites the

SEC to preserve and expand its jurisdiction by designating any economically meaningful digital commodity as a security.[10] Even under a supportive administration, it is risky to legislate in a way that relies on the SEC to voluntarily constrain its own authority. Under a hostile administration, this approach creates even greater risk. Moreover, to avoid this regulatory uncertainty, this structure could incentivize entrepreneurs to develop digital assets without real value (e.g., memecoins) in order to avoid the ambiguities and uncertainty created under the law, thereby frustrating efforts to realize the full potential of blockchain technology.[11]

In sum, one of the following must be true about the proposed ancillary asset construct. Either:

1. The test prioritizes **form over substance**, in which case it would potentially allow issuers of securities to circumvent securities laws merely through superficial structuring (i.e., not granting formal rights, but creating expectations of investment returns based on their ongoing efforts), undermining the broader U.S. securities framework; or
2. The test prioritizes **substance over form**, in which case it compounds the ambiguities and regulatory uncertainty created by the *Howey* test rather than resolves them, and provides the SEC with significant discretion to dictate whether a given digital asset is subject to securities laws. This could worsen precisely the regulatory uncertainty that the Discussion Draft aims to remedy.

Market structure legislation can and must do better to protect investors and resolve the challenges facing entrepreneurs and slowing the pace of innovation in the U.S.

The CLARITY Act avoids these problems. Rather than providing a broad exemption from securities laws, CLARITY ensures that digital assets are excluded from securities laws *only* when they are "digital commodities," a term that is narrowly defined to require that a digital asset's function, economic characteristics, and trust dependencies are not securities-like. This precise approach prioritizes substance over form and leaves little ambiguity over the regulatory treatment of digital commodities—for instance, it provides regulatory certainty with respect to economic rights, value accrual, and decentralized governance. Further, it aligns the treatment of digital commodities with the foundational objectives of investor protection and market fairness.

All that said, the "digital commodity" approach in CLARITY is not without flaws. Like the ancillary asset construct, CLARITY's regulatory framework assumes that primary transactions in digital assets are "investment contracts" under the *Howey* test and subject to securities laws.[12] As discussed

[10] The report asserts that "Efforts to regulate network tokens should focus on ensuring that tokens, even if initially issued as part of an investment contract in a securities transaction, are not classified as securities once the network becomes fully functional and sufficiently decentralized." Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto/

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

[12] We presume that the intention of Congress in both the CLARITY Act and the Discussion Draft are that primary transactions in digital assets will be subject to securities laws. This view is supported by the crowdfunding exemptions in both bills, which would not be necessary if primary transactions of digital assets were not subject to securities laws. However, as discussed in response to **Question #1b**, the applicability of securities laws to primary transactions is far from settled.

further in response to **Question #1b**, given the uncertainty and subjectivity involved with the application of *Howey*, this leaves open the possibility that a digital asset issuer could seek to circumvent the regulatory frameworks provided by CLARITY and the Discussion Draft by challenging the application of *Howey* to their primary transactions. This would clearly frustrate the intent of Congress in adopting a regulatory framework through market structure legislation. If Congress's goal is to bring legal clarity to digital assets, relying on the *Howey* test as a threshold inquiry undermines that purpose. It retains the ambiguity of current law, forcing innovators to litigate the application of *Howey* just to qualify for a supposedly new and clear regulatory regime. Though, as discussed in our response to **Question #1c** below, this does not mean that *Howey* should be rewritten.

Further, the ancillary asset construct does have advantages over CLARITY. First, it does not modify securities laws with respect to a single asset class created by a specific technology. While this necessitates greater deference to regulators in interpreting the law and widens the scope of possible unintended consequences beyond the sphere of digital assets, it does enable the regime to be more flexible over time. Second, the ancillary asset construct produces a regulatory framework that is more simple than CLARITY's. CLARITY relies on a layered set of provisions—including a crowdfunding regime and amendments to existing exemptions under the securities laws—to ensure adequate disclosures are provided when tokens trade on secondary markets during periods when issuers are still engaged in ongoing managerial efforts. By contrast, the ancillary asset framework applies a straightforward disclosure obligation post-sale, which persists only as long as managerial efforts continue. This simplicity is appealing. However, simplicity should not come at the expense of regulatory coherence or investor protection.

Given the foregoing, Congress should not pursue the ancillary assets construct without making significant modifications. Rather it should either adopt CLARITY's approach, or pursue a combination of the two frameworks—combining CLARITY's narrow and precise "digital commodity" construct with the structural simplicity of the ancillary asset construct. In particular, this would include:

- Removing any ambiguity over whether the ancillary asset construct is formalistic rather than substantive—Congressional intent should be clear that the test prioritizes substance over form.
- Constraining the definition of "ancillary assets" to focus on digital commodities.
- Providing greater regulatory clarity regarding the treatment of digital assets that have economic rights in an underlying blockchain system, including where such systems utilize decentralized governance.

Key Recommendations:

1. Adopt CLARITY.
2. Alternatively, combine CLARITY's narrow and precise definition of "digital commodity" with the structural simplicity of the ancillary asset construct.

b. Should legislation rely on existing concepts, such as from SEC v. W.J. Howey Co. (Howey), when defining which digital assets are securities?

Yes, but with clear limitations. Congress should preserve the core principles of *SEC v. W.J. Howey Co.*, but not retain the test itself as a threshold question in digital asset regulation. A new

legislative framework should codify *Howey's* principles—particularly its substance-over-form logic—while avoiding the subjectivity and unpredictability that have made *Howey* unworkable in the digital asset context.[13]

The *Howey* test remains an essential tool under federal securities law because it is a flexible, substance-over-form framework that captures investment schemes that are not explicitly enumerated in the definition of "security." Its emphasis on "economic reality"—rather than rigid formal categories—helps guard against regulatory arbitrage and ensures that schemes presenting the risks characteristic of securities remain within the regulatory perimeter.[14] However, the application of *Howey* to digital assets—especially in the secondary market context—has produced confusion and legal uncertainty. While *Howey's* core logic remains sound, legislative action is needed to clarify its application to digital assets and to preserve its role as a catchall without allowing it to be applied in ways that undermine innovation or depart from first principles. We outline how that can be accomplished below.

As we noted in our initial response to the SEC Crypto Task Force's February 2025 Request for Information (the "SEC RFI"),[15] the application of *Howey* to primary transactions is relatively straightforward: the issuer's promotional and sales efforts typically create a reasonable expectation of profit for purchasers.[16] As such, these transactions should be subject to securities laws. Nevertheless, the application of *Howey* to primary transactions of digital assets has been inconsistent. While some courts have affirmed that primary transactions in digital assets are subject to securities laws,[17] others have disagreed.[18]

Compounding the uncertainty, applying *Howey to* secondary transactions of digital assets is exceedingly complicated because the buyer may have no relationship with the issuer, the issuer's efforts may have diminished or disappeared, and there may be no obligations embedded in the digital asset itself. Further, many digital assets are autonomously issued by software, meaning that there is no issuer. Yet any application of *Howey* to secondary market transactions of digital assets conceptually demands that an issuer exists and that the digital asset itself "embodies" obligations of that issuer such that the asset is conceived of as the representation of certain rights and obligations that make up the transaction's "economic realities." Conventional securities, such as stocks or bonds, do not create similar confusion as there is always an issuer and secondary-market purchasers have enforceable rights against that issuer.

These factors have confused market participants and created uncertainty as to whether federal securities laws apply to a given digital asset transaction. Compounding this confusion, the SEC's

---

[13] 328 U.S. 293 (1946).
[14] *Id.*
[15] 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.
[16] 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/.
[17] *SEC v. Terraform Labs Pte. Ltd.*, No. 23-cv-1346, 2023 WL 4858299 (S.D.N.Y. July 31, 2023).
[18] *SEC v. Ripple Labs*, 2023 WL 4507900 (S.D.N.Y. July 13, 2023) (differentiating between the circumstances surrounding Institutional Sales and those attending Programmatic Sales); *SEC v. Telegram Grp. Inc.*, 448 F. Supp. 3d 352 (S.D.N.Y 2020).

application of the *Howey* test has exposed several issues that must be addressed to provide predictability and legal precision, including:

- **Lack of Predictability** – The subjective nature of the *Howey* test leads to high regulatory uncertainty, forcing crypto market participants to rely on *ex post* enforcement actions rather than clear *ex ante* rules in trying to discern whether federal securities laws apply. This is at odds with the need for a predictable regulatory environment.
- **Difficult to Enforce** – The subjective nature of the *Howey* test also means the SEC needs to expend considerable resources to determine whether the criteria of the test are satisfied and the SEC has jurisdiction. Bad actors have taken advantage of this slow and ununiform enforcement to harm market participants.
- **Impractical to Apply** – Many digital assets may satisfy the criteria of the *Howey* test one day only to fail it another depending on a subjective assessment of third party "ongoing efforts," which neither regulators nor digital asset market participants can effectively assess; *Howey* provides no clear framework for recognizing when a transaction in a digital asset is out of the reach of federal securities laws when the relevant facts and circumstances change over time.
- **Boundless Reach** – Without statutory guardrails, the test's flexibility can be misused—empowering regulators to stretch jurisdiction to target disfavored transactions.

Ultimately, the SEC's recent unbounded application of the *Howey* test to digital assets has been counterproductive to its stated mission; this approach has failed to protect market participants, has not facilitated fair and efficient markets, and has hindered capital formation.

Furthermore, the SEC's weaponization of the "efforts of others" prong of *Howey* has created significant perverse incentives: projects are effectively encouraged to cease public engagement, obscure development work, or offload responsibilities to opaque intermediaries to avoid securities regulation. This undermines transparency, leaves users exposed to undisclosed risks, and forestalls innovation. Put simply, efforts-based decentralization is not a suitable legal framework and is unlikely to ever work in practice.

Fully abandoning *Howey*, or attempting to limit it through formalistic requirements, however, would make possible significant circumvention of federal securities laws.[19] Special treatment should not be given to transactions in investment contracts where the nature and structure of those transactions (and the assets to which they relate) do not mitigate the risks of ordinary securities transactions that federal securities laws are intended to address.[20]

None of this, however, should imply that the application of *Howey* principles cannot be improved. A better approach is possible. Congress can preserve *Howey* and address its limitations in a

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

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

merit- and technology-neutral way by codifying a refined application of *Howey* through the following steps:

(1) Subject primary transactions in ancillary assets to securities laws.

Whether or not a digital asset is subject to the market structure regulatory framework should not hinge on a subjective test like *Howey*, which has a history of inconsistent interpretation in federal courts.[21] Doing so would leave open the possibility that a digital asset issuer could avoid the regulatory framework adopted under CLARITY and the Discussion Draft by challenging the application of *Howey* to their primary transactions. This would frustrate Congress' intent in creating a market structure regulatory framework in the first place.

Congress should therefore make clear that primary transactions of ancillary assets (including digital commodities) are subject to securities laws. Regardless of whether they involve formal legal rights, primary transactions of ancillary assets (including digital commodities) typically create a clear and reasonable expectation of profits based on the issuer's efforts. They thus fit squarely within the *Howey* framework and should be regulated as securities transactions.

We appreciate that the Discussion Draft and CLARITY align with this principle by affirming that primary sales of ancillary assets (or digital commodities in the case of CLARITY) should be treated as securities transactions.

(2) Exclude secondary transactions in ancillary assets from securities laws.

In secondary transactions of ancillary assets (including digital commodities), there is typically no relationship between the buyer and the original issuer, and thus no objective way to determine whether the buyer was reasonable in their reliance on the issuer's managerial efforts. Applying securities laws to these transactions has led to the problems discussed above. Moreover, doing so fails to recognize that if a project eliminates control, then its digital commodity's trust dependencies become very different from those of an ordinary security.

We appreciate that the Discussion Draft and CLARITY align with this principle by affirming that secondary transactions in ancillary assets (or digital commodities in the case of CLARITY) should be treated as commodities transactions and regulated accordingly.

(3) Apply transfer restrictions to insiders where control persists (pre-decentralization).

This combination of securities regulations for primary transactions and commodity regulations for secondary transactions creates an obvious loophole: issuers can easily circumvent securities laws through a two-step transaction: the issuer sells ancillary assets (such as digital commodities) to insiders (employees, underwriters, early investors) under existing exemptions, and those parties then resell in the public markets without complying with securities laws. This would effectively enable "schemes" where

[21] *SEC v. Ripple Labs*, 2023 WL 4507900 (S.D.N.Y. July 13, 2023); *SEC v. Telegram Grp. Inc.*, 448 F. Supp. 3d 352 (S.D.N.Y 2020).

assets with securities-like risks are distributed to the public without registration, defeating the core purpose of *Howey*.

To prevent circumvention of securities laws and exploitation of information asymmetries, transfer restrictions, such as those contemplated in the Discussion Draft and CLARITY, must be imposed on insiders until the trust dependencies and risk profile of the underlying asset have been mitigated such that they function more like a commodity than a security. This necessitates that those projects pursue and achieve decentralization by eliminating mechanisms of control. Applying transfer restrictions in this manner can close loopholes that would otherwise arise from exempting all secondary market transactions of ancillary assets (including digital commodities) from securities laws. Doing so also prevents insider enrichment at the expense of public investors and ensures that the distinction between primary and secondary markets remains meaningful. Once control is relinquished and the project is decentralized, those restrictions should fall away, as the asset's trust dependencies now resemble those of a commodity.

Both the Discussion Draft and CLARITY use transfer restrictions to bolster investor protections, but the Discussion Draft introduces critical loopholes that will likely undermine their effectiveness. Most notably:

- **Insider Sales Pre-Decentralization** – The Discussion Draft **permits insiders to sell up to 60% of their holdings per year** before a project has eliminated control through decentralization. This legalizes the kind of scheme that *Howey* was designed to prevent: insiders offloading tokens to the public while retaining centralized control, all without complying with securities laws. Allowing insiders to extract value from tokens that they control—without the robust disclosure or registration requirements of securities laws—defeats the purpose of the transfer restrictions and exposes retail participants to significant risks during the period of greatest information asymmetry. These lax requirements also invite regulatory arbitrage—the easier it is for insiders to enrich themselves via the ancillary asset construct, the more likely the pathway will be used by people seeking to avoid securities laws, rather than entrepreneurs building blockchain systems with digital commodities.
- **Use of Crowdfunding to Exit** – The crowdfunding provision in the Discussion Draft creates a second major loophole. The bill **permits projects to raise up to $75 million per year** from the public via a token crowdfunding exemption before the project decentralizes. While there are benefits to this approach, like giving retail investors earlier access to projects and facilitating price discovery, the proposed structure undermines the transfer restriction framework. In particular, this mechanism acts as a backdoor for secondary sales—entrepreneurs and insiders could route distributions through primary offerings and extract value from the system without facing any of the constraints imposed by securities law. Once capital is raised and teams disband, the harm to investors cannot be undone.

Together, these provisions—pre-maturity insider sales and the exorbitant crowdfunding exemption—greatly weaken the investor protection benefits of the transfer restriction construct. Legislation should not create legal pathways for insiders to distribute assets with securities-like risk profiles to the public during the phase of project development when information asymmetries are most likely. If projects wish to access public markets while retaining control and without any obligation to relinquish control, they should be subject to the disclosure, liability, and oversight regime that securities laws provide. Otherwise, the control-based framework becomes an empty shell, and the regulatory

framework loses its protective function. Therefore, if the control-based framework is to function as intended, these provisions must be narrowed.

(4) Apply disclosure obligations to reduce information asymmetries.

Even when secondary transactions are excluded from securities laws, information asymmetries may persist, especially if a project is controlled by a small group that is engaged in managerial efforts. Tailored disclosure obligations, such as those contemplated in CLARITY and the Discussion Draft, are essential to ensuring transparency and accountability during this phase. However, because these obligations are less robust than traditional securities disclosures, they must be paired with transfer restrictions to preserve investor protection. As a project decentralizes and control is relinquished, the risk of information asymmetries is reduced and disclosure obligations can appropriately taper off.

(5) Adopt a control-based decentralization framework.

The legislation should make clear that a control-based decentralization framework—not an efforts-based framework—is the appropriate way to evaluate the evolution of an ancillary asset's risk profile. A control-based approach fixes the problems of the SEC's historic "efforts-based decentralization" *Howey* test framework. With respect to digital commodities, this should be focused on whether any party retains unilateral authority—operational, economic, or governance—over the blockchain system. This approach permits continued development and support activities, provided those efforts are not accompanied by control. This distinction provides a clear, objective, and enforceable basis for applying securities laws that aligns with the *Howey's* economic reality standard, and better serves both innovation and investor protection.[22]

In conclusion, *Howey* should not be abandoned. Instead, Congress should codify the principles underlying *Howey* for assets under a control-based decentralization framework. Adapting those principles will preserve a substance-over-form approach and close critical gaps that enable regulatory evasion. A modernized framework grounded in primary transaction regulation, secondary transaction exclusion, pre-decentralization transfer restrictions, control-based disclosures, and a clear decentralization standard ensures investor protection while enabling responsible innovation.

Key Recommendations:

1. Codify *Howey's* principles by applying securities laws to primary transactions and commodities laws to secondary transactions of ancillary assets.
2. Impose pre-decentralization transfer restrictions on insiders and disclosure obligations on issuers to prevent exploitation of the above framework.
3. Reduce the potential for insiders to circumvent transfer restrictions, including through use of the new crowdfunding exemption.
4. Adopt a control-based decentralization framework.

[22] 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/.

c. Should legislation mandate, as under proposed discussion draft Section 105, that the SEC undertake a rulemaking to clarify the definition of "investment contract" as articulated in Howey ? If so, how?

No. The *Howey* test remains a critical component of U.S. securities law. It provides a flexible, substance-over-form framework that captures investment arrangements that may not fall within the formal definition of a stock or bond but present the same economic risks and information asymmetries. Rather than replacing or rewriting this test, Congress should codify a modernized application suited to ancillary assets as outlined in our response to **Question #1b**.

The proposed rulemaking in Section 105 is unnecessary—and dangerous—because it seeks to rewrite *Howey* in a way that departs from settled law and undermines investor protections. The proposed constraints are inconsistent with decades of case law, would fundamentally narrow *Howey's* application and create exploitable loopholes. For example:

- (b)(2) would require that an investment be made in a "business entity." This would exclude many arrangements from securities laws that have long been regulated as securities transactions. For instance, investments in individual athletes' future earnings, which entail similar risks to those associated with a share of stock in a company, have long been viewed as securities offerings under the Howey test (see *Fantex*).[23] This change would enable such offerings to circumvent securities laws. That result alone demonstrates the risk of reverting to a formalistic framework that ignores economic substance.
- (b)(3) would require an "express or implied agreement," significantly narrowing the scope of *Howey's* reach. *Howey* explicitly applies to a "contract, transaction or scheme," a broader formulation that captures investment relationships even in the absence of traditional contractual privity.[24] The proposed clause would enshrine the "predicate contract" theory, which courts have repeatedly rejected, and would foreclose application of the test to secondary market transactions—eviscerating regulatory oversight of digital assets and other novel instruments traded in non-traditional ways.[25]
- (b)(4) would turn the entire *Howey* doctrine into a form-over-substance test, elevating legal formalisms over the economic realities of transactions. This is not only inconsistent with *Howey*, but with the entire structure and purpose of the securities laws.

These changes are not merely problematic—they are incompatible with the broader architecture of U.S. securities law. The investment contract test was designed to be a catchall, and it is one of the few flexible tools regulators have to address novel financial instruments that function like securities. Moreover, this proposal is not just inconsistent with *Howey*—it is incongruent with other "economic reality" tests under U.S. securities law. The *Reves* test for notes, and the multi-factor analyses used to determine broker, dealer, and adviser status, all prioritize substance over form. Adopting a uniquely

[23] Wikipedia, Fantex, https://en.wikipedia.org/wiki/Fantex (last edited Feb. 16, 2025).
[24] 328 U.S. 293 (1946).
[25] *See, e.g.*, *SEC v. Ripple Labs, Inc.*, 2023 WL 4507900, at *23 (S.D.N.Y. July 13, 2023) (stating that "whether a secondary market sale constitutes an offer or sale of an investment contract would depend on the totality of circumstances and the economic reality of that specific contract, transaction, or scheme."); Transcript of Motions Hearing, *SEC v. LBRY*, No. 1:21-cv-260 (D.N.H. Jan. 30, 2023) (declining to extend holding to include secondary sales), ECF No. 105 at 34:14-16.

formalistic approach here would be a radical and unjustified departure. If the *Howey* test is weakened, traditional securities could be restructured to escape through newly created loopholes. The likely result: a slow but systemic erosion of the securities regulatory perimeter, undercutting the integrity of the U.S. capital markets.

Furthermore, this rulemaking mandate undermines the broader coherence of the bill. The proposed legislation is premised on creating a regulatory framework for "ancillary assets" originally offered as part of an investment contract (including digital assets). In other words, in order for an asset to be an "ancillary asset" and be subject to the regulatory framework, it must have first been offered as part of an investment contract. Consequently, if the scope of the definition of "investment contract" is narrowed via the proposed rulemaking so that the vast majority of digital asset transactions would not be categorized as investment contracts, then the bill's entire regime—including its investor protections—would fail to apply to those digital assets. As a result, Section 105 would exempt most digital assets, including those initially sold in ICOs, from securities laws and the "ancillary asset" regulatory framework—an outcome that is incoherent with the intention of the legislation and is self-defeating.

In sum, Section 105 should be removed. If Congress wishes to clarify *Howey's* application, it should do so in a way that retains its reach, preserves its substance-over-form orientation, and clarifies existing case law. It should not seek to rewrite securities laws based on the crypto industry's interpretations of *Howey* that are inconsistent with the principles underpinning securities laws.

Key Recommendations:

1. Remove Section 105 from the Discussion Draft.
2. Reject formalistic revisions that narrow Howey's scope or require a predicate contract.
3. Preserve Howey's economic reality standard as a flexible, substance-over-form tool.

d. Should Congress revisit other terms within the existing definition of security, such as note, to accommodate digital assets and to prevent a later SEC from inappropriately construing these terms?

Yes. As discussed in our initial submission to the SEC RFI,[26] the Commission and courts have at times applied other terms within the definition of "security"—such as "note," "profits interest," and "transferable share"—in ways that introduce significant ambiguity for digital commodities. Applying those terms too broadly risks sweeping in open, decentralized blockchain systems that pose none of the risks the securities laws are meant to address. In particular, without clarification these terms could be stretched to cover digital commodities based solely on the ownership rights they grant to holders—such as voting rights, economic rights, or participation rights. This would both frustrate Congressional intent regarding the creation of a new regulatory framework for digital commodities and further propagate valueless tokens (as we have seen with the rise of memecoins in response to regulatory uncertainty).

[26] 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/.

In the vast majority of cases, the ownership rights associated with digital commodities should not implicate securities laws. For example, economic mechanisms that drive value to a digital commodity from the underlying decentralized blockchain system's operation are not dependent on any development company or issuer, and therefore do not implicate the same risks that securities laws are intended to address. Ultimately, because blockchain systems can operate autonomously and without human intervention or control, their digital commodities can provide holders with many ownership rights without creating trust dependencies on any issuer or controlling person. Conversely, when a token's price is tied to the profits of an offchain application, product, or service, the risks securities laws were intended to address are implicated, as such systems are inherently reliant on human intervention and control.

Given the foregoing, the Discussion Draft should be modified to reaffirm that a digital commodity is not a "note", "profits interest" or "transferable share" unless it embodies the same legal claims and investor risks associated with those traditional securities.

The CLARITY Act addresses these concerns directly. Its definition of "digital commodity" expressly includes digital assets even when they entitle users to certain governance and economic rights within a decentralized blockchain system.[27] CLARITY's approach is difficult to replicate in the Discussion Draft because the currently proposed ancillary asset construct limits the "investment contract" security designation for all assets, but the definitions of "note", "profits interest" or "transferable share" cannot similarly be limited for all assets without rendering those terms meaningless. As a result, the Discussion Draft must be amended to exclude digital commodities that meet certain characteristics from these alternative securities designations without introducing inconsistencies with the ancillary asset construct. At a minimum, the Discussion Draft should adopt a functional definition that explicitly distinguishes them from other securities categories—consistent with CLARITY's framework—even if it retains the ancillary asset construct for investment contracts.

In short, Congress should clarify that legacy terms in the securities laws—like "note", "profits interest" and "transferable share"—should not be construed in ways that undermine the regulatory distinctions this legislation aims to establish. Doing so would ensure consistent application, limit overreach, and support a principled digital asset regulatory regime.

Key Recommendations:

1. Clarify that legacy terms like "note" and "transferable share" must be interpreted in economic context.
2. Prevent these terms from being used to capture decentralized assets that lack the trust dependencies that merit securities regulation.

e. Should legislation provide for a specific token taxonomy based on the underlying characteristics of an asset? If so, what approach? How could such a taxonomy remain merit and technology neutral?

Yes. A fit-for-purpose token taxonomy is essential to providing legal clarity, regulatory consistency, and eliminating reliance on litigation-prone threshold tests like *Howey* to determine whether

[27] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress § 504 (2025).

digital assets fall within the scope of a new regulatory regime. As outlined in our initial submission to the SEC RFI,[28] such a taxonomy should classify tokens based on their functional characteristics and risk profiles, not on subjective value judgments or underlying technology. This ensures that the regime remains merit- and technology-neutral while aligning with longstanding principles of securities regulation.

Any such taxonomy must distinguish between the classification of the token itself and the nature of the transaction in which it is used. This reflects the approach in *Howey*, which recognized that an orange grove is not itself a security, even if the scheme involving its sale might be.[29] Clarifying this distinction would eliminate much of the confusion surrounding digital assets and reduce the risk of overregulation. Yet, it would still enable a regulatory framework whereby primary transactions of digital assets are subject to securities laws, whereas secondary transactions of digital commodities are excluded from securities laws, consistent with the approach we outlined in response to **Questions #1a** and **#1b**.

Among digital assets, digital commodities are the only asset class that raise unique questions that need addressing under securities laws. As discussed above, this is because the risks they present shift depending on the degree of control retained over the underlying blockchain system. When that system is subject to ongoing managerial control, the risks resemble those of traditional securities—such as information asymmetry and reliance on issuer efforts. But when the system becomes decentralized and no party retains unilateral control, those risks dissipate, and the asset therefore functions more like a commodity. A tailored legal framework is needed to address this unique trajectory.

By contrast, other token categories fit more cleanly within existing regulatory regimes and do not require bespoke treatment. Company-backed tokens—a digital 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)—present clear securities-like risks and should fall within the remit of securities laws.[30] In no case was this more clearly demonstrated than FTX's FTT. Asset-backed tokens—a digital asset that primarily derives its value from a claim on, or economic exposure to, one or more underlying assets—are already being addressed under securities laws and the GENIUS regulatory framework for stablecoins. Memecoins, arcade tokens, and collectible tokens (NFTs), generally do not exhibit the features of investment contracts or other securities and should not be regulated as such.[31]

The CLARITY Act adopts precisely this targeted approach. It focused exclusively on digital commodities and established a disclosure regime that applies when a project retains control over the underlying system.[32] CLARITY does not seek to reclassify or create new frameworks for company-backed tokens, stablecoins, collectible tokens, or other categories—because doing so is unnecessary or

[28] 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/.
[29] 328 U.S. 293 (1946).
[30] Miles Jennings, Scott Duke Kominers & Eddy Lazzarin, *Network Tokens vs. Company-Backed Tokens*, a16z crypto (Mar. 5, 2025), https://a16zcrypto.com/posts/article/network-tokens-vs-company-backed-tokens/.
[31] Miles Jennings, Scott Duke Kominers & Eddy Lazzarin, *Defining Tokens*, a16z crypto (Mar. 5, 2025), https://a16zcrypto.com/posts/article/defining-tokens/.
[32] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress § 504 (2025).

can otherwise be dealt with through guidance and rulemaking at the relevant regulatory agencies.[33] These assets already fall within the appropriate legal regimes, whether securities, commodities, or other regulated instruments.

CLARITY's design is both merit- and technology-neutral. It avoids defining assets based on subjective claims of utility or innovation, and instead focuses on objective indicators of control and economic substance. This ensures regulatory consistency across analogous risk profiles regardless of whether an asset is digital or traditional, onchain or offchain.

Key Recommendations:

1. Adopt a functional, risk-based taxonomy that differentiates based on control and trust dependencies.
2. Limit bespoke treatment to digital commodities; apply existing regimes to other asset types (e.g., stablecoins, NFTs).
3. Use CLARITY's "digital commodity" definition as the model for digital commodities.

f. Should legislation clarify the status of certain technology functions that are inherent to the operation of a distributed ledger network? This could include technology functions such as running consensus algorithms, executing smart contracts, or engaging in activities like staking and mining.

Yes. Legislation should clarify that core technology functions necessary for the operation of decentralized blockchain systems—such as running consensus algorithms, mining, staking, and executing smart contracts—do not, in and of themselves, constitute regulated financial activity under U.S. securities or commodities laws.

This principle has long been supported by industry participants and regulators, and was articulated in our initial submission to the SEC RFI.[34] Just as internet law has long distinguished between communications protocols (e.g., TCP/IP, SMTP) and the applications that run on top of them (e.g., email services, social media platforms), blockchain legislation must clearly delineate between infrastructure-level functions and intermediated user-facing activities. Infrastructure actors who do not perform intermediary roles—such as validators, miners, and smart contract executors—should not be regulated as if they were providing financial services or participating in transactions of regulated financial instruments (including securities and derivatives).

Importantly, CLARITY provides a robust and nuanced model for implementing this principle. In particular, Sections 309 and 409, along with the definitions of "decentralized finance messaging system"

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

[34] 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/.

and "decentralized finance trading protocol," establish a high threshold for exclusion: these provisions ensure that safe harbor treatment is available only to actors who are not acting as intermediaries and not in a position to exert unilateral control or cause user harm (see our response to **Question #26** below).[35] Importantly, this comports with the recommendations of the President's Working Group on Digital Assets, which emphasizes that the extent to which an application exercises control over user assets is a key factor in determining the appropriate regulatory treatment of DeFi.[36]

This is a critical distinction. A blockchain validator participating in a credibly neutral consensus process should not be subject to regulation merely by virtue of validating a block that includes a securities transaction—just as an internet service provider is not liable for a website that violates securities laws. By contrast, a centrally-controlled blockchain where a single validator can censor transactions or misappropriate user funds is functionally indistinguishable from a traditional intermediary and should be regulated accordingly. CLARITY draws this line effectively by conditioning exclusion on decentralization, absence of control, and non-custodial design.[37]

The risk of failing to provide these guardrails is significant. Without them, regulators could assert jurisdiction over core infrastructure actors by mischaracterizing the technical role these actors play, which would chill innovation, fragment global protocol participation, and push core infrastructure development offshore, at odds with the aims of the Committee.[38]

To remain technology- and merit-neutral, legislation should focus on the function being performed, not the medium through which it occurs. It should ensure that exclusions are narrowly-tailored to protect consumers but broad enough to avoid inadvertently treating software, infrastructure operators, or permissionless protocols as financial intermediaries.

In short, Congress should adopt the CLARITY model—ensuring that participation in decentralized consensus, mining, staking, or smart contract execution does not trigger regulatory liability unless those functions involve intermediary-like control, custodial access, or user-specific influence over outcomes. This distinction will ensure robust consumer protection while preserving the core technological foundations of decentralized systems.

Key Recommendations:

1. Exclude core protocol functions (e.g., staking, mining, smart contract execution) that do not intermediate transactions from financial regulation.
2. Implement CLARITY's model, which conditions exclusions on decentralization, non-custodial design, and lack of control.

---

[35] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress § 504 (2025).
[36] Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto.
[37] *Id.*
[38] Majority Press Release, United States Committee on Banking, Housing, and Urban Affairs, Scott, Lummis, Colleagues Release Market Structure Discussion Draft, Issue Request for Information from Stakeholders (July 22, 2025). https://www.banking.senate.gov/newsroom/majority/scott-lummis-colleagues-release-market-structure-discussion-draft-issue-request-for-information-from-stakeholders.

g. Should existing tokens be grandfathered into a new token classification framework created by Congress? If so, how?

Yes, but not automatically or unconditionally. Any grandfathering of existing tokens must be structured in a way that incentivizes decentralization and prevents legacy projects from securing a regulatory advantage by being grandfathered-in while remaining centralized. A principled framework should provide a clear path forward for good-faith actors while ensuring a level playing field across the ecosystem.

Without appropriate guardrails, broad grandfathering could allow incumbent projects to operate indefinitely in centralized configurations while being exempt from the disclosure obligations, decentralization milestones, and transfer restrictions that future projects would be subject to. This would disincentivize decentralization—subjecting investors to risk—and distort competition. To avoid that outcome, Congress should establish a transition framework that requires compliance with disclosure obligations and creates a structured timeline of requirements that incentivize decentralization.

At a minimum, all existing projects should be required to begin complying with a disclosure regime within one year of the bill's enactment. In line with the CLARITY Act, disclosure obligations should be tailored based on the level of control and activity associated with the project:

- Where issuers retain control and are engaged in ongoing managerial efforts, full disclosures should be required.
- Where control has been eliminated and ongoing efforts continue, a reduced disclosure regime may be appropriate.
- Where control has been eliminated and there are no ongoing efforts, disclosures may be unnecessary.

To preserve fairness and ensure market integrity, projects that do not eliminate control by achieving decentralization within a defined grace period—three to four years is a reasonable window—should be subject to transfer restrictions, just as new projects would be upon entry into the regulatory framework. Understandably, many existing tokens are already widely held by third parties and are not subject to transfer restrictions, however the prolonged grace period should be sufficient time for such projects to come into compliance or alternatively opt for registration under securities laws. This would ensure that the framework respects settled expectations while still aligning incentives, guarding against centralization, and promoting investor protection.

At the same time, the Committee should consider providing a lighter regulatory burden for blockchain systems that have demonstrated long-term operational integrity. Drawing from the concept of "well-known seasoned issuers" under existing securities laws, legislation could exempt or reduce obligations for blockchain projects that have been credibly decentralized and publicly operational for a sustained period—such as 10 years or more. At that point, the likelihood of material information asymmetries is greatly reduced, and the need for ongoing disclosures and oversight may no longer justify the compliance burden. This would reward long-term, credibly neutral systems like Bitcoin and Ethereum while preserving investor protection where it is still warranted. Further, special concessions could be made for such legacy projects with respect to the thresholds for decentralization. For example, in the CLARITY Act, legacy projects are only required to ensure that no person beneficially owns more than

50% of the total supply of a digital commodity, whereas new projects must comply with a lower and more stringent 20% threshold.

In short, grandfathering should not be a regulatory giveaway. It should be a structured transition, available to legacy projects that take meaningful steps toward decentralization and compliance. This preserves the integrity of the regulatory framework, rewards good-faith actors, and upholds the legislative goal of aligning risk, control, and disclosure in digital asset markets.

Key Recommendations:

1. Require all legacy projects to comply with disclosure obligations within one year.
2. Impose transfer restrictions on insiders of legacy projects if decentralization is not achieved within a specified period (3–4 year window to mature).
3. Structure grandfathering as a transition path, not a blanket exemption.

h. How should Congress address alleged violations of sections 5 or 12 of the Securities Act of 1933 arising from offers or sales of digital assets that occurred before the effective date of this Act? Should relief be provided through a conditional safe harbor or retroactive exemption, and if so, what compliance or disqualification criteria, if any, should apply?

Yes, relief should be provided through a conditional, retroactive exemption for certain past offers and sales of digital assets—provided that the project comes into compliance with the regulatory regime set forth in the legislation within the applicable transition period. This approach balances fairness to good-faith innovators with investor protection and regulatory integrity.

Both the Discussion Draft and the CLARITY Act rightly acknowledge that secondary transactions in digital commodities are not securities transactions, and the SEC has itself conceded that most digital assets are not securities in and of themselves. In light of these acknowledgments, there is a compelling policy rationale for providing retroactive relief to projects that conform to the framework established by Congress.

Congress could offer a conditional safe harbor that provides retroactive exemption from liability under Sections 5 and 12 of the Securities Act, but only if:

- The project comes into compliance with the legislation's disclosure regime within the prescribed timeline (e.g., within one year of enactment); and
- The project successfully achieves decentralization by relinquishing control prior to the expiration of a grace period (e.g., one year post-enactment).

This structure ensures that investor protection continues post-enactment, through mandatory disclosures and through the structural protection that decentralization provides. It also gives legacy projects a meaningful incentive to comply, without rewarding noncompliance or evasion. At the same time, any such exemption should contain clear limits:

- It should not apply to primary sales of digital assets, which remain subject to securities laws under the Discussion Draft.

- It should not preclude enforcement actions based on fraud, misrepresentation, or other malfeasance.
- It should be limited to technical violations of the registration provisions—not blanket amnesty for past misconduct.

Importantly, any safe harbor or retroactive exemption should not create an inference of liability prior to the effective date of the legislation. Further, legislation should clarify that the regulations adopted thereunder shall not undermine or reverse any adjudicated matters that have resulted in transactions of digital assets being determined to not be subject to securities laws. Unless such adjudicated matters are overturned, they should remain in effect.

In sum, retroactive relief should be conditioned on future compliance. It should incentivize decentralization, provide clarity for past participants, and preserve accountability where needed. That balance is consistent with the goals of the legislation and with longstanding principles of investor protection.

Key Recommendations:

1. Offer conditional safe harbor to projects that comply within a set timeline.
2. Exclude relief for primary sales, fraud, or misrepresentation.
3. Do not create an inference of liability or undermine adjudicated matters.

Question 2: The proposed legislation modernizes securities regulations for digital asset activities (i.e., proposed Section 109 of the discussion draft) while preserving the SEC's exemptive authority (i.e., proposed Section 106 of the discussion draft). Should the legislation provide more specific relief in any particular area, such as Regulation Crowdfunding, Regulation A, Regulation D, Rule 144, or frameworks for simple agreements for future tokens (SAFTs), or any other topic referenced in proposed discussion draft Section 109(a)(1) through (a)(5)?

Unlocking the benefits of blockchain technology requires modernizing aspects of U.S. securities laws to account for the unique features and structures of tokenized systems. But any such modernization must be implemented with care. The transformation underway holds significant promise, but it also touches critical infrastructure that supports investor confidence and market integrity. Any regulatory shift should be calibrated to preserve those foundations while allowing innovation to proceed responsibly.

Section 109 of the Discussion Draft takes a constructive approach by signaling a willingness to tailor existing frameworks to the realities of digital asset markets. Coupled with Section 106, which preserves the SEC's exemptive authority, these provisions strike the right general balance. In our recent submissions in response to the SEC RFI on modernizing securities laws—including our response to questions regarding tokenized securities[39] and broker-dealer capital and recordkeeping requirements[40]—

[39] Miles Jennings et al., *Comments on the SEC Crypto Task Force's Questions Concerning Tokenized Securities,* a16z crypto (July 21, 2025), https://api.a16zcrypto.com/wp-content/uploads/2025/07/comments-sec-crypto-task-forces-Tokenized-Securities.pdf.

[40] Scott Walker et al., *Comments on the SEC Crypto Task Force's Questions Concerning Broker-Dealer Capital and Recordkeeping Requirements for Crypto Assets,* a16z crypto (July 21, 2025), https://api.a16zcrypto.com/wp-content/uploads/2025/07/sec-rfi-SEC-rfi-broker-dealer-capital-recordkeeping-requirements.pdf.

we outlined how the SEC can responsibly adapt securities laws to support tokenization without compromising investor protections.

With respect to the specific exemptions referenced above, we do not believe Regulation D requires special treatment or modification for digital asset projects. This exemption functions effectively and appropriately for traditional securities, including investment contracts, and is a powerful tool for startup capital formation. There is no clear justification for creating carve-outs or special treatment for tokenized offerings, and any deviation could invite abuse and undermine the parity that securities laws are designed to ensure. We also believe Rule 144 does not need revision at this time, though we would have recommendations on this matter if Congress does not pass legislation providing a regulatory framework for digital assets.[41]

However, we do support tailoring Regulation Crowdfunding (Reg CF) for digital commodities. As noted in our response to the SEC RFI, we have recommended that Congress and the SEC develop a framework under Reg CF that would align incentives, protect retail investors, and enable token projects to grow responsibly under the oversight of the existing securities regime. In particular, our recommendations include changes that would bring Reg CF in line with the CLARITY Act and the Discussion Draft:

- Apply a disclosure regime calibrated to whether a project retains control;
- Permit limited pre-maturity fundraising (e.g., $25 million per year or $75 million lifetime), but only for projects that commit to a decentralization roadmap;
- Provide a pathway for tokens to exit the securities regime as they achieve network maturity/ decentralization;
- Impose safeguards to prevent large incumbents or centralized entities from misusing Reg CF as a substitute for public offerings; and
- Maintain investor protection and does not permit exemptions from liability for fraud.

Key Recommendations:

1. Continue to take a measured and careful approach to modernizing securities laws.
2. Do not modify Regulation D or Rule 144 for token-based projects.
3. Tailor Reg CF to allow limited pre-decentralization fundraising, contingent on a decentralization roadmap and enhanced disclosures.

Question 3: Should legislation consider a mechanism that allows market participants to seek a final determination from the SEC regarding whether a digital asset is a security? If so, how?

No. We do not believe that legislation should create a mechanism for market participants to seek a final determination from the SEC as to whether a particular digital asset is a security. Such a determination is unnecessary under existing securities laws as well as the frameworks proposed by both the Discussion Draft and the CLARITY Act.[42] In particular, both frameworks are designed to have

[41] For a discussion of potential modifications to Rule 144 in the event legislation is not adopted by Congress, see SEC RFI: 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/.

[42] Under existing securities laws, the SEC already has authority to provide case by case exemptive relief in specific circumstances when merited.

primary transactions in digital assets remain subject to securities laws and secondary transactions in digital commodities (under CLARITY) or ancillary assets (under the Discussion Draft) be excluded from securities laws. This approach cleanly delineates the jurisdictions of the SEC and CFTC without requiring a static legal classification of the asset itself. While regulatory certainty in this classification can be bolstered, it is neither necessary nor appropriate to declare whether an asset is or is not a security.[43]

However, as discussed above, the different treatment of primary transactions and secondary transactions under securities laws as proposed under CLARITY and the Discussion Draft creates a risk that bad actors could design schemes to circumvent the protections that apply to primary transactions. For example, if an issuer can route sales through underwriters, insiders, or employees, the distinction between primary and secondary transactions is easily bypassed. Both the Discussion Draft and CLARITY Act address this risk by applying transfer restrictions to insiders, such as employees, investors, and underwriters. These restrictions help prevent projects from labeling a token a "commodity" or "ancillary asset" while retaining centralized control and profiting from retail sales by taking advantage of lingering information asymmetries.

Based on these frameworks, a determination mechanism is appropriate to certify whether a project has achieved decentralization (or "maturity" under CLARITY). That milestone has real regulatory consequences: it governs when transfer restrictions fall away and when disclosure obligations may be reduced or eliminated. It is therefore appropriate for a regulatory agency to administer such a certification, provided it is bound by clear statutory criteria. At the same time, any certification mechanism must account for the fact that the risks associated with digital assets can evolve; a blockchain system that has decentralized can later become re-intermediated, reintroducing information asymmetries that securities laws were designed to mitigate. Therefore, any regulatory framework that reduces burdens such as disclosures or resale restrictions must not be a one-way door.

The Discussion Draft does not currently account for this risk. By contrast, the CLARITY Act addresses it directly through the concept of "Control Persons" in Section 411. Under that provision, if an individual or entity reasserts control over a previously decentralized/mature network, they become subject to transfer restrictions. This protects the public market from exploitation by actors who could otherwise use re-centralization to their advantage.

In short, a static certification that a digital asset is not a security is both unnecessary and potentially harmful. What is needed is a dynamic, criteria-based certification process focused on decentralization milestones—with the flexibility to reimpose safeguards if centralized control re-emerges. The CLARITY Act provides a strong foundation for such a framework.

Key Recommendations:

1. Do not create a mechanism for final SEC determinations on whether a digital asset is a security.

[43] Further, any framework that did create a need for a final determination as to the security status of a digital asset would likely be deeply flawed. The risks associated with a given digital asset can change, potentially dramatically, over time, most notably where a project consolidates power in the hands of a centralized actor over time. In such cases, a framework providing a one-way door to non-security status would leave investors exposed to such recentralization risk.

2. Instead, authorize a process for certifying decentralization based on objective, control-based criteria.
3. Ensure the certification framework is dynamic and allows reclassification if centralized control reemerges, using CLARITY's "Control Person" construct as a model.

Question 4: Should legislation allow market participants the freedom to choose between being subject to SEC jurisdiction or CFTC jurisdiction? If so, how?

No. Legislation should not permit market participants to unilaterally choose between SEC and CFTC jurisdiction. The allocation of regulatory oversight should be determined based on the economic characteristics and risk profile of the asset, not the preferences of the issuer or platform. Allowing such parties to elect their preferred regulator would create incentives for regulatory arbitrage and trigger a race to the bottom—undermining the core objectives of U.S. securities laws: protecting investors, facilitating capital formation, and maintaining fair and efficient markets. Further, it would potentially distort competition, favoring projects that elect one regulatory regime over another despite nearly identical characteristics.

Under existing law, the SEC and CFTC divide jurisdiction based on the underlying nature of the financial instrument—securities are regulated by the SEC, commodities and derivatives by the CFTC. That fundamental principle should remain intact. Where an asset retains trust dependencies and presents risks similar to traditional securities—such as reliance on managerial control and information asymmetries—it should fall under SEC jurisdiction. Where a digital asset is sufficiently decentralized and lacks such dependencies, it should be treated as a commodity and regulated by the CFTC.

Both the CLARITY Act and, to a lesser extent, the Discussion Draft preserve this approach by grounding regulatory classification in the structure and function of the underlying system. Importantly, neither bill requires that issuers avail themselves of the commodity-focused framework. Issuers can still subject their tokens to securities laws and pursue registration with the SEC, particularly if they intend to retain control over the system indefinitely. In those cases, the project's risk profile aligns more closely with securities markets, and SEC oversight is appropriate.

This approach provides sufficient flexibility. Market participants can influence the applicable regulatory regime not by electing a regulator, but by determining the design and governance structure of their project. If they wish to pursue a pathway under CFTC jurisdiction, they must build and operate systems that eliminate the trust dependencies that give rise to securities regulation. If they intend to maintain centralization, they should remain under the SEC's purview.

Additionally, trading platforms may end up listing both digital commodities and digital securities. In such cases, legislation should clearly articulate criteria to determine which agency serves as the platform's primary regulator. Factors could include the relative trading volume of securities versus commodities, the platform's custodial practices, and whether the platform facilitates primary offerings or merely secondary trading. Clear statutory criteria would avoid duplicative or conflicting regulatory burdens while ensuring that platforms are subject to meaningful oversight based on their activities. Without such clarity, dual-registration requirements could stifle innovation or drive legitimate platforms offshore.

In short, legislation should not grant market participants unrestricted freedom to choose their regulator. Instead, it should flow from the structure, function, and risk profile of the asset or activity—not market participant preference. Moreover, where trading platforms facilitate both digital commodities and digital securities, the law should provide clear criteria to determine the primary regulator. Without such guidance, overlapping regulatory mandates could chill innovation, raise barriers to entry, and fragment U.S. digital asset markets.

Key Recommendations:

1. Do not allow issuers or platforms to elect SEC or CFTC jurisdiction.
2. Allocate jurisdiction based on the asset's structure, function, and risk profile—consistent with existing law.
3. Ensure projects that wish to remain centralized have a pathway under securities laws and that projects that wish to decentralize by elimination control have a pathway under commodities laws.
4. Create clear statutory criteria to determine primary regulator for platforms listing both digital commodities and securities.

Question 5: What type of information should issuers be required to disclose in connection with digital asset offerings?

a. To what extent is the information specified in proposed Section 4B of the Securities Act overinclusive or underinclusive of what information should be disclosed?

We commend the Committee for proposing robust disclosure requirements for certain transactions involving ancillary assets. Unless the exclusions provided by Sec. 4B.(c)(1)(B)(i), Sec. 4B.(c)(1)(B)(ii), or Sec. 4B.(d)(3)(B) apply, then the Discussion Draft requires that ancillary asset originators provide both basic corporate information regarding their relevant activities and economic information pertaining to the ancillary asset. While the Discussion Draft directs the SEC to determine by rule what specific information must be disclosed, the Committee's list of potential disclosures provides a solid starting point.

Nonetheless, we believe that the information specified in proposed Section 4B is underinclusive. Here too we direct the Committee's attention to the CLARITY Act. Broadly, CLARITY requires that issuers provide disclosures that are similar to what is required under securities laws, but that are adapted to ensure that users have access to the most useful information, accounting for the different characteristics of digital commodities relative to shares of stock. Under CLARITY, prior to a project becoming decentralized (or "mature"), digital commodity issuers must provide extensive disclosures about how the blockchain system to which a digital commodity relates works. We believe that these tailored disclosure obligations, coupled with the insider transfer restrictions imposed by CLARITY, would enable market participants to achieve a level of protection commensurate with that provided by securities laws.

As a general matter, we support the Committee's decision to defer rulemaking authority regarding the content of disclosures to the Commission. This is a prudent decision that enables the Commission to engage in a more fulsome process to determine what disclosures are most appropriate. However, it is critically important that the Discussion Draft guidance with respect to disclosure be bolstered with requirements relating to the issuer's level of control and ongoing activity, as proposed in CLARITY. Projects that retain control should be subject to full disclosures, while those that are decentralized should

face a tailored set of ongoing obligations (see our response to **Question #1g**). In addition, while there is otherwise substantial overlap between the disclosures required by the Discussion Draft and CLARITY, there are important gaps in the former that we believe it is imperative for the Committee to close. These concern token economics, development plans, and ownership disclosures. In particular:

- **Token Economics**: Under CLARITY, digital commodity issuers are required to provide key details concerning information explaining the technical requirements for holding, accessing, and transferring a digital commodity. The act also mandates that they provide information on any method of generating or mining digital commodities, and any process for burning or destroying units of the digital commodity on the blockchain system, as well as any mechanisms for driving value to the digital commodity of such a blockchain system.[44] Each of these disclosures is essential to providing users with a clear understanding of how a given token accrues value and whether that process is controlled by a person or group of persons under common control, and therefore crucial for assessing an asset's risk profile. Yet the Discussion Draft lacks these disclosure requirements, leaving users without access to information that is critical to assessing an asset's risks.
- **Development Plans**: CLARITY likewise provides for robust disclosure requirements pertaining to an issuer's plan of development, mandating that they disclose the current state and timeline of the development of the blockchain system to which the digital commodity relates. Importantly, this disclosure must also address any mechanisms of control and critical operation dependencies present in relation to the blockchain system or its token.[45] While the Discussion Draft does require that the ancillary asset originator disclose their plans to support the asset's use or development, their obligation to do so is limited to a twelve month period, and they are not required to disclose the same control-related information as required by CLARITY. This gap likewise ultimately creates risk for users.
- **Ownership & Insider Disclosures**: CLARITY and the Discussion Draft both include a requirement that the issuer disclose information related to an asset's ownership, but the latter is substantially more narrow in this respect. Specifically, the Discussion Draft only requires the disclosure of information relating to the holdings of the ancillary asset by persons owning more than 10% of any class of equity security of the ancillary asset originator, and that of the senior management of the ancillary asset originator. Whereas CLARITY mandates that issuers disclose a list of *all* digital commodity related persons or digital commodity affiliated persons who have been issued a unit of the digital commodity by the digital commodity issuer or have a right to a unit of the digital commodity from its issuer.[46]

As we elaborated in a recent response to the SEC RFI,[47] each of these categories of information is designed to surface risks related to control and ongoing managerial efforts. We view the risks arising from control to be the most significant, even more so than ongoing managerial efforts, because while a dependence on the ongoing managerial efforts of a small number of actors to maintain and develop the

[44] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress § 504 (2025).
[45] *Id.*
[46] *Id.*
[47] Miles Jennings et al., *SEC RFI: Comments on the SEC Crypto Task Force's Questions Concerning Public Offerings and Safe Harbor from Registration* (May 1, 2025), https://api.a16zcrypto.com/wp-content/uploads/2025/05/a16z-Crypto-SEC-RFI-Comments-on-Public-Offerings-and-Safe-Harbor-from-Registration.pdf.

system can give rise to information asymmetries, such risk is greatly reduced when the centralized control of the system is eliminated. As such, we urge the Committee to harmonize the Discussion Draft with the disclosure requirements and decentralization milestones of CLARITY in the manner described above.

b. What type of ongoing information, such as that under proposed Section 4B, should legislation mandate?

As noted in our response to **Question #5a**, we appreciate that proposed Section 4B of the Discussion Draft includes detailed disclosure obligations intended to protect investors and support responsible innovation. Unless an exclusion under Sec. 4B(c)(1)(B)(i), (c)(1)(B)(ii), or (d)(3)(B) applies, ancillary asset originators must comply with a set of periodic reporting requirements. While this is a valuable step forward, we believe the current framework should be further refined to align with a control-based decentralization model and the evolving risk profile of digital commodities.

Specifically, legislation should adopt a tiered ongoing disclosure regime calibrated to two key variables:

1. Whether the project has eliminated mechanisms of operational, economic, and governance control (i.e., control-based decentralization); and
2. Whether the issuer or related parties continue to engage in material ongoing managerial efforts.

As explained in our submission to the SEC RFI,[48] control is the most salient risk indicator in blockchain-based systems. When a token is issued by a centralized entity that retains control, such as over the ability to alter system parameters or extract value, the risks are similar to those of traditional securities—warranting robust disclosures. This is because whoever controls a system controls the risks associated with that system and can unilaterally affect or structure its risk. Conversely, where blockchain systems eliminate mechanisms of control and no party retains unilateral control, the digital commodities of such systems are not subject to the trust dependencies that intermediary-based arrangements give rise to and, therefore, reduced disclosure requirements are merited. Nevertheless, even blockchain systems that have eliminated control may still depend upon material ongoing efforts, which could give rise to information asymmetries, and therefore engender risks. Thus, certain issuer-based disclosure obligations should still apply to blockchain systems that have eliminated control whenever they remain dependent on ongoing efforts.

Once a decentralized system has eliminated control and is no longer subject to material ongoing efforts, publicly available information should suffice to ensure that market participants are equally situated with respect to the risks associated with a given digital asset. As such, when it comes to ongoing information reporting, market structure legislation should pair a control-based decentralization approach with issuer-centric disclosure requirements where material ongoing efforts persist.

[48] Miles Jennings et al., *SEC RFI: Comments on the SEC Crypto Task Force's Questions Concerning Public Offerings and Safe Harbor from Registration* (May 1, 2025), https://api.a16zcrypto.com/wp-content/uploads/2025/05/a16z-Crypto-SEC-RFI-Comments-on-Public-Offerings-and-Safe-Harbor-from-Registration.pdf.

The Discussion Draft reflects elements of this logic. For example, Sec. 4B.(d)(3)(B) provides that ancillary asset originators that have successfully certified to the Commission that they have not engaged in material ongoing efforts for a period of time do not need to comply with the Discussion Draft's disclosure requirements. This provision recognizes that once ongoing efforts cease, the risk of information asymmetries with respect to that digital asset is reduced. However, the Discussion Draft lacks a structured, tiered approach that also considers decentralization (elimination of control) as a precondition for reducing obligations. This omission risks leaving investors exposed to information gaps in situations where control remains.

We recommend that the Committee adopt CLARITY's phased approach and explicitly condition reductions in disclosure on both decentralization and the cessation of managerial efforts. This pairing ensures that investors are protected when it matters most and reduces compliance burdens only once structural protections—like trustless system design—are in place.

This tiered framework recognizes the dynamic nature of blockchain projects and ensures that disclosures match the actual risks investors face at each stage of development and decentralization.

c. How often should ongoing disclosure be required? For example, proposed Section 4B would require semi-annual disclosures.

Here too we advise the Committee to follow the approach taken by CLARITY. We appreciate that the Discussion Draft's requirement for semiannual disclosure requirements already aligns with CLARITY's approach to controlled blockchain systems, however we recommend that the Discussion Draft also incorporate ongoing disclosures that are simply conditioned upon the occurrence of any material change.[49] For example, CLARITY mandates that issuers must file current reports as soon any material change has occurred with respect to the network. This combination of semiannual and material change reporting requirements can help ensure that market participants are well-situated with respect to a digital asset's evolving risk profile.

d. When should ongoing disclosure obligations discontinue? For example, proposed Section 4B of the Securities Act sets forth a mechanism by which disclosure obligations could cease. Does that subsection set forth the appropriate test, or should another test or mechanism be considered?

With respect to the termination of disclosure obligations, we believe that the Discussion Draft should be harmonized with CLARITY. As described in our respect on **Question #5b**, CLARITY provides that, once a blockchain system is decentralized (has eliminated control) and the system is no longer dependent on the material ongoing efforts of any centralized party, ongoing disclosure obligations lapse. This is warranted because, at this stage, all relevant information about the blockchain system and token are publicly available via onchain information, and therefore, further disclosures are not required.

[49] Specifically, CLARITY provides that issuers of a digital commodity related to a blockchain system that is still controlled must provide semiannual reports containing an updated description of the current state and timeline for the development of the blockchain system, a description of the issuer and related persons in relation to the system's development, and financial information, including the amount of money raised and spent to date.

e. How should the information required be tailored to the size and type of the issuer or offering?

We appreciate the inclusion of Sections 4B(c)(1)(B)(i) and (ii), which provide disclosure exemptions for smaller offerings—specifically, those totaling under $5 million in a 12-month period or for tokens with an average daily aggregate trading value under $5 million. These exclusions are important. America's technological leadership depends on the growth of startups and early-stage projects, and these provisions help ensure that "Little Tech" has a viable path to market.[50]

However, we are concerned that, as written, the Discussion Draft's disclosure requirements risk undermining innovation and forestalling private fundraising by sweeping in offerings that would otherwise be exempt under securities laws—undermining key private fundraising channels for emerging companies, such as those available under Regulation D. As this outcome would be at cross purposes with the exclusions provided by 4B.(c)(1)(B), we strongly suggest rectifying this problem.

Specifically, the Discussion Draft does not appear to preserve exemptions like Rule 701, which provides a long-established carveout for compensatory equity issuances to employees, consultants, and advisors. That exemption is regularly used for compensating employees with digital assets. Nor is it clear that the Discussion Draft's disclosure framework respects the scope of Regulation D, which facilitates private fundraising under Rule 506. In fact, the bill's reference to 17 C.F.R. § 230.506(d) in Section 102(b)(1), but not in Section 4B, suggests that these private placements may be swept into the new disclosure regime unintentionally.

These rules—Rule 701, Reg D, and others—are foundational to early-stage capital formation. If digital asset projects are subject to new disclosure burdens while traditional securities remain exempt under longstanding rules, the regulatory imbalance will harm innovation and drive projects offshore. The Committee should therefore ensure that the Discussion Draft does not inadvertently override or undercut these exemptions.

We strongly recommend that Section 4B be revised to clarify that its disclosure obligations do not apply to digital asset transactions that qualify for an existing federal securities law exemption, including those under Rule 701, Rule 506, or other comparable SEC rules.

f. Should legislation require a new form for digital asset offerings? If not, what updates should be made to existing forms that are used in connection with traditional securities offerings?

We do not believe that legislation should require a new form for digital asset offerings. Please see our response to **Question #2** above for elaboration.

[50] Marc Andreessen & Ben Horowitz, *The Little Tech Agenda*, a16z (July 5, 2024), https://a16z.com/the-little-tech-agenda/.

Key Recommendations:

1. Adopt CLARITY's control-based, phased disclosures approach and explicitly condition reductions in disclosure on both decentralization and the cessation of managerial efforts.
2. Incorporate additional requirements pertaining to token economics, development plans, and ownership and insider disclosures.
3. Harmonize the Discussion Draft's approach to ongoing disclosure and discontinuance with CLARITY.
4. Revise Section 4B to clarify that its disclosure requirements do not apply to token transactions that qualify for an existing federal securities law exemption.

Question 6: Proposed Section 4B(h) of the Securities Act would provide the SEC with authority to establish "limitations on the disposition of certain ancillary assets . . ." What, if any, restrictions on the disposition of ancillary assets by related persons or in affiliate transactions should Congress consider? To what extent are conflicts disclosures sufficient?

Yes. Transfer restrictions on ancillary assets held by insiders and affiliates are essential. Disclosure obligations are not sufficient to address the risks of potential information asymmetries arising from digital commodities that relate to blockchain systems. Rather they must be paired with disclosure obligations—and remain in place until credible decentralization is achieved—to safeguard investors against risks that mirror traditional securities.

(1) Why transfer restrictions are essential

Even sophisticated disclosure regimes—like those in CLARITY and the Discussion Draft—are weaker than traditional securities-law safeguards. Neither framework requires audited financial statements, detailed management discussion and analysis or executive compensation disclosure. This is for good reason—blockchain systems can function autonomously, not controlled by any company or person. A lighter touch disclosure regime that places less emphasis on an issuer is therefore not only appropriate but necessary to ensure that compliance with the regime does not entrench centralization.

However, this approach potentially creates a shortfall when it comes to protecting investors from potential information asymmetries relating to digital commodities. This is particularly true where a blockchain system remains centralized and subject to insider control, in which case the risks associated with its native digital commodity mirror those of traditional securities. A controlled blockchain is functionally analogous to proprietary software. In both cases, the controller can abruptly alter functionality, shut down the system, or extract value—creating severe downside risk for holders. If Apple securitized ownership in the App Store, securities laws would clearly apply because of Apple's unilateral control—instilling information asymmetry and concentration risk.

What distinguishes decentralized blockchains from proprietary software is autonomous operation without human intervention. Once a network is credibly decentralized, no individual or entity can censor transactions, alter consensus, or alter token rules. At that point, the trust dependencies that justify securities regulation evaporate. Until then, tokens issued by controlled systems pose the same risks as unregistered securities—and therefore, require analogous safeguards: disclosure plus transfer restrictions.

Without pairing these tailored disclosures with transfer restrictions, investors could be exposed to significant harm due to lingering asymmetries. As a result, market structure legislation should make a deliberate tradeoff: replace the burdensome and often ill-fitting disclosure obligations of securities law with a more proportional framework for digital commodities—while restricting insider participation in secondary markets to preserve equivalent investor protection. Once decentralization is achieved and control is relinquished, and with the added benefit of onchain transparency, both disclosure obligations and transfer restrictions appropriately taper off. This structure ensures that protections remain robust across the project lifecycle without over-regulating at any stage.

(2) How transfer restrictions protect investors

Transfer restrictions are a vital investor protection function in digital commodities markets. They are not novel: similar restrictions exist under securities laws, including under Rule 144, to prevent unregistered distributions by insiders and affiliates. In the context of digital commodities, their role is arguably more critical, as they operate as a counterbalance to the lighter-touch disclosure framework and help ensure that investor harm is not created through regulatory arbitrage.

Specifically, transfer restrictions protect investors in several distinct but complementary ways:

- **Preventing circumvention of securities laws through two-step schemes.** Transfer restrictions reduce the risk that early investors, employees, or underwriters act as conduits in a scheme to distribute tokens to the public. Without such restrictions, an issuer could sell tokens in a private placement (e.g., under Rule 506), have insiders or affiliates acquire those tokens, and then have those parties immediately sell them to the public—functionally replicating a public offering without registration or robust disclosures. Transfer restrictions prevent this by limiting the ability of insiders to resell into public markets while the project remains centralized and high-risk. Both the Discussion Draft and CLARITY seek to apply securities laws to primary transactions of digital commodities, so without transfer restrictions, both regimes would be exposed to a two-step loophole.

- **Phasing in secondary market access as risk declines.** Allowing broader participation in secondary markets only once a project has decentralized by eliminating control—and thereby mitigated information asymmetries—ensures that digital commodities markets operate more like commodities markets than securities markets. In doing so, transfer restrictions help preserve the integrity of the regulatory distinction: until decentralization is achieved, the token may behave like a security and should be subject to similar constraints; once decentralization eliminates control and managerial dependence, the asset becomes more commodity-like and can be freely traded.

- **Creating incentives for investor-protective behavior.** Transfer restrictions provide a powerful structural incentive for projects to achieve decentralization and eliminate control. If insiders want access to secondary market liquidity, they must relinquish control and minimize ongoing managerial efforts. This framework aligns the incentives of issuers with those of investors and the public—encouraging structural reforms that reduce risk rather than simply relying on ex ante representations.

- **Facilitating progressive decentralization and network growth.** Non-insider access to secondary markets is often essential to bootstrapping network participation and protocol adoption. By allowing public trading while restricting insider participation, transfer restrictions permit projects to grow while maintaining guardrails against insider advantage. This structure also mirrors the phased access model in traditional capital markets—where insiders are often subject to lockups or restrictions when they possess material information, while public investors are allowed to trade freely.

In sum, transfer restrictions are a necessary investor protection tool in any regime that reduces the disclosure and registration burdens of securities laws. They are proportionate, targeted, and effective—and they work in tandem with decentralization milestones to promote a safer, fairer, and more credible digital asset ecosystem.

(3) Why criticisms of transfer restrictions are not compelling

Certain industry stakeholders, including crypto hedge funds, have raised concerns about the effect of transfer restrictions on U.S. digital commodity markets that are worth addressing.

First, some argue that transfer restrictions may push developers offshore or chill innovation. This is a misplaced concern. U.S. securities laws are globally respected for facilitating transparency, market efficiency, and investor confidence. Far from undermining innovation, disciplined regulation supports it and fosters capital formation. Markets in foreign jurisdictions without such standards are plagued by toxic assets, which causes capital to flee. Moreover, the transfer restrictions framework proposed in both CLARITY and the Discussion Draft are designed to reflect blockchain's unique technical properties. A structure that limits restriction to the period before decentralization aligns with the very innovation blockchain enables, rather than contradicting it. Further, control-based rules mesh naturally with existing U.S. regimes—such as money-transmission law (focused on control) and tax law (focused on dominion). These are not regulatory burdens—they are standards rooted in technology's reality. No industry proponent argues that "decentralization" should not factor into the regulation of decentralized finance, so why would it not factor into the regulation of blockchain systems and their digital commodities?

Second, some argue that restrictions may impede liquidity or distort price discovery. While this is a valid concern, and low liquidity assets have led to distorted market prices that have left to investor harm, both CLARITY and the Discussion Draft already effectively address this risk. In practice, the proposed regimes unlock more liquidity than the current state of digital commodity markets. They establish compliant distribution mechanisms like airdrops and incentive-based rewards, improve transparency via enhanced disclosures and market-making disclosure requirements, and provide for a crowdfunding regime that will enable price discovery. Insider-trading rules in equities markets do not impede liquidity or distort price discovery, they will similarly not do so in emerging digital commodity markets.

Key Recommendations:

1. Bolster the transfer restriction framework proposed in the Discussion Draft by eliminating or reducing the flat 5% related person threshold. A cap that allows investors to acquire up to 5% of a token supply creates room for schemes that fall just beneath the limit (4.99%) and exposes

consumers to significant harm. We recommend harmonizing with CLARITY and using a lower threshold of 1%, while carving out less significant persons.
2. Eliminate the allowance for insiders to sell 60% per year pre-decentralization. This carveout undermines the entire transfer restrictions framework to the point of rendering it meaningless. It enables early extraction of value by the insiders that are most likely to have asymmetric information about a project, before decentralization is realized and when they may control the underlying blockchain system.
3. Streamline post-sale reporting obligations. Imposing ongoing disclosure obligations to all related persons is unnecessarily burdensome. Instead, we recommend applying reporting to only those holders whose holdings exceed 5% of the token supply.

a. Are the factors in proposed Section 103 for determining whether an ancillary asset "is not under common control by related persons" appropriate? If not, how should they be modified?

We commend the Committee for adopting a control-based decentralization framework in the Discussion Draft. By centering the regulatory framework on "control," the Discussion Draft aligns with the core foundational premise included in CLARITY: the application of securities laws should turn not on labels or forms, but on whether a project retains trust dependencies that expose public market participants to information asymmetries and risks of managerial discretion.

Control-based decentralization offers a principled, technology-neutral path forward. As discussed in our SEC RFI submission,[51] it is not sufficient to rely on proxies such as ownership dispersion or the volume of transactions. Rather, the relevant inquiry must focus on whether a person or group retains the *ability to alter the risk profile* of the system—operationally, economically, or in governance. In this respect, Section 103 of the Discussion Draft is a meaningful step in the right direction.

That said, the principles-based language included in Section 103 alone is insufficient. To ensure legal clarity and limit future regulatory overreach, legislation should pair the Discussion Draft's standards with an objective, rules-based safe harbor—modeled on the framework set forth in the CLARITY Act. As explained in our response to the SEC's RFI, the absence of objective criteria introduces regulatory uncertainty and opens the door for shifting interpretations over time. Projects need clear, verifiable milestones to guide development, assess compliance, and secure the confidence of ecosystem participants. Without such certainty, innovation will slow and legal risk will increase.

The decentralization safe harbor in the CLARITY Act was built to address these concerns. Developed with input from across the crypto industry—including founders, protocol builders, governance experts, and legal practitioners—it establishes a practical and reliable standard for determining when control has been eliminated. The framework focuses on the elimination of *mechanisms* of control, not just the diffusion of ownership. It requires the absence of:

[51] 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/.

- Operational Control: No party should be able to unilaterally pause, censor, or override network operations.

- Economic Control: No party should retain the power to extract value from the system through privileged monetary rights, such as unvested token allocations or privileged minting authorities.

- Governance Control: No party or coordinated group should be able to pass protocol governance proposals unilaterally or through offchain influence.

Crucially, the CLARITY framework applies these criteria not only to issuers and founders, but to any related person or group acting in concert. It includes thresholds for token holdings and governance participation that can be objectively measured. These criteria were designed to work across blockchain systems of all types—including Layer 1s, Layer 2s, bridges, smart contract protocols, and appchains—and reflect the largest consensus from the crypto industry ever assembled in support of a legal standard for decentralization.[52] Defining such criteria is also consistent with the recent report of the President's Working Group on Digital Asset Markets, which called for decentralization criteria to be "...clear and objective to ensure fairness and provide market participants with certainty."[53]

In short, while the principles outlined in Section 103 are directionally sound, Congress should codify an objective safe harbor for decentralization consistent with CLARITY's approach. Doing so would provide legal certainty to developers and teams, prevent arbitrary or politicized enforcement, support compliance with the transfer restriction and disclosure frameworks embedded elsewhere in the legislation.

III. Responses to Committee Questions #15 - #17

Question 15: What challenges do market participants face relating to the custody of digital assets, and how could legislation address those challenges?

For our positions on the matters addressed by **Questions #15a-f**, please see our recent submission to the SEC RFI.[54]

g. What, if any, changes should Congress consider to preserve the right to self-custody digital assets?

We are grateful for the Committee's inclusion of protections for self-custody in the Discussion Draft. As the President's Working Group on Digital Assets affirms, protecting self-custody is essential to

[52] Decentralization Research Center, *Joint letter to Speaker Johnson, Representative Jeffries, Leader John Thune, and Senator Schumer* (July 14, 2025), https://x.com/TheDRC_/status/1944787470903603272.
[53] Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto/.
[54] Scott Walker et al., *SEC RFI: Comments on the SEC Crypto Task Force's Questions Concerning the Custody of Crypto Assets* (Apr. 9, 2025), https://api.a16zcrypto.com/wp-content/uploads/2025/04/Andreessen-Horowitz-a16z-response-to-Crypto-Task-Force-re-Custody-of-Crypto-Assets-04.09.2025.docx.pdf.

ensure that digital assets remain usable by individuals and communities.[55] The protections for self-custody in the CLARITY Act also received broad industry support. The protections in the Discussion Draft could be bolstered by expanding them to include all "U.S. persons" as well as with preemption of state attempts to impose registration, licensing, or surveillance mandates on self-custody activity.

Question 16: What laws, requirements, and practices relating to illicit finance and anti-money laundering do digital asset market participants already follow?

a. To what extent are distributed ledger technology and digital assets useful in promoting compliance with anti-money laundering and sanctions laws?

Public blockchains and digital assets are useful in promoting compliance with anti-money laundering and sanctions laws because, as a general matter, their transparency features have made it easier for law enforcement and intelligence agencies to follow funds flows and collect valuable data and evidence. Specifically, in contrast to opaque traditional markets, all transactions on public blockchains are transparently available for anyone with access to a block explorer to view.[56] Although it is true that the transactions are identified with pseudonymous wallet addresses, rather than real names or identities, it is not difficult to establish a connection between a user and a wallet. Once a user uses digital assets to buy anything or transfer digital assets to someone else, the receiving person or company generally knows the identity behind the sending wallet address. Tracing techniques have developed over the years to take advantage of this blockchain feature, and data analytics have become increasingly good at surmounting pseudonymity. It is these techniques that allow law enforcement to track the movement of illicit funds on public blockchains to "off-ramps" (i.e., cash-out points for cryptocurrencies, such as exchanges), and blockchain wallet addresses associated with bad actors.[57] Law enforcement can then work with the "off-ramp" to gather information about the account holder, freeze or seize funds, or take other enforcement action, and OFAC can sanction wallet addresses, as well as foreign persons identified as controlling those addresses. Notably, blockchain tracing techniques played an important role in the takedowns of illicit marketplaces, including the Silk Road, Alpha Bay, and BTC-e.[58]

Given the traceability of funds flows, public blockchains are typically less attractive for money laundering, terrorist financing, and proliferation financing, at least when compared to more traditional methods used for illicit finance. Indeed, government reports, particularly those from the Biden Administration's Treasury Department—including its 2024 National Risk Assessments,[59] Illicit Finance

[55] Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto/.
[56] *See, e.g.*, Blockchain.com, http://blockchain.com/explorer (block explorer for viewing the Bitcoin blockchain network); Etherscan, https://etherscan.io/ (block explorer for viewing the Ethereum blockchain network).
[57] See U.S. Dep't of the Treasury, Action Plan to Address Illicit Financing Risks of Digital Assets, at Pg. 6 (Sept. 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf ("regulators and law enforcement can in some cases take viewable pseudonymous user and transaction information and pair it with other pieces of information to identify transactions participants.").
[58] Nicole Perlroth, Katie Benner & Erin Griffith, *Colonial Pipeline investigation upends idea that Bitcoin is untraceable*, Seattle Times (June 9, 2021), https://www.seattletimes.com/business/colonial-pipeline-investigation-upends-idea-that-bitcoin-is-untraceable/.
[59] U.S. Department of the Treasury, Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing (Feb. 2024), https://home.treasury.gov/news/press-releases/jy2080.

Risk Assessment on Decentralized Finance,[60] and Illicit Finance Risk Assessment of Non-Fungible Tokens[61]—have all recognized that most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs in fiat currency or via more traditional methods. Data analytics companies have also issued reports showing consistently that illicit activities are a small portion of the total activity that occurs on blockchains,[62] and the percentage of total transaction volume on blockchains attributable to illicit activities has steadily decreased since Satoshi Nakamoto first launched the Bitcoin network in 2009. As effective tools for combating illicit finance continue to improve, and blockchains and digital assets continue to enter the traditional financial world, these numbers will likely continue to fall even further.

b. What existing supervisory frameworks at the international, federal or state levels address the potential illicit finance risks of digital assets?

Federal supervisory frameworks

At the federal level, the Bank Secrecy Act (BSA) provides a supervisory framework that addresses potential illicit finance risks of digital assets.[63] The Act was first passed in 1970 to "promote financial transparency" and then subsequently amended to criminalize money laundering, require financial institutions to file "suspicious activity reports" and implement procedures "reasonably designed" to maintain "minimum standards" for an anti-money laundering (AML) program, and other requirements.[64] In 2020, Congress passed the Anti-Money Laundering Act, which expanded the statutory scope of the BSA to include businesses that provide covered financial services involving "value that substitutes for currency," which includes certain digital assets and convertible virtual currencies (CVC).

Importantly, the BSA regulates "financial institutions," which includes a broad set of financial intermediaries, such as banks, SEC-registered brokers or dealers, money services businesses, and others.

---

[60] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf ("[T]his risk assessment recognizes that most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs in fiat currency or otherwise outside the virtual asset ecosystem via more traditional methods.")

[61] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Non-Fungible Tokens (May 2024), https://home.treasury.gov/system/files/136/Illicit-Finance-Risk-Assessment-of-Non-Fungible-Tokens.pdf ("The assessment identifies that NFTs and NFT platforms are, to date, rarely being used for proliferation financing or terrorist financing.").

[62] TRM Labs, *2025 Crypto Crime Report: Key trends that shaped the illicit crypto market in 2024* (2025), http://www.trmlabs.com/files/report-2025-crypto-crime-report (finding that illicit volume accounted for approximately 0.4% of total crypto volume in 2024 and 0.9% in 2023 based on the USD value of funds stolen in crypto hacks, as well as the USD value of transfers to blockchain addresses that have been linked to entities in illicit categories); Chainalysis Team, *2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth* (2024), https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (finding that transactions associated with illicit activity made up 0.34% of all onchain cryptocurrency activity in 2023); Elliptic, *Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders* (2020), https://www.elliptic.co/resources/typologies-concise-guide-crypto-leaders ("illicit activity today still accounts for less than 1% of all transactions").

[63] 12 U.S.C. 1829b, 12 U.S.C. 1951-1960, 31 U.S.C. 5311-5314, 5316-5336.

[64] *See* Rebecca Rettig, Michael Mosier & Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*, at Pgs. 5-7 (2024), https://dcfintechweek.org/wp-content/uploads/2024/09/Paper-Genuine-DeFi-as-Critical-Infrastructure.pdf.

Regulations promulgated under the BSA further define the term "money services businesses" to include "money transmitters," which include persons who provide money transmission services, i.e., the "*acceptance* of currency, funds, or other value that substitutes for currency from one person and the *transmission* of currency, funds, or other value that substitutes for currency to another location or person by any means," or other persons "engaged in the transfer of funds."[65] Whether a business qualifies as a "money transmitter" depends on its business model, but as a general matter, FinCEN has long taken the position that certain digital asset businesses fall within scope of the term, including centralized exchanges, issuers of CVC (e.g. stablecoins), hosted wallet providers, crypto kiosks (ATMs), and others. All digital asset businesses that are "money transmitters" must comply with BSA obligations.

Although not technically a supervisory framework, it also bears mentioning that all U.S. persons—U.S. citizens and all lawful residents (wherever located), all individuals and entities within the United States; and all entities organized under the laws of the United States or any jurisdiction within the United States—are required to comply with OFAC's sanctions programs.[66] All persons who are subject to OFAC regulations are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade- or investment-related transactions. OFAC's sanctions programs can target foreign countries, geographic regions, entities, individuals, and property. Notably, OFAC regularly identifies digital asset wallet addresses as blocked property and publishes those wallet addresses on the Specially Designated Nationals and Blocked Persons list (SDN List). While OFAC does not require digital asset businesses to use any particular in-house or third-party software, many businesses have done so, and such software providers have improved with time. Compliance with OFAC's sanctions programs, therefore, is also helpful in mitigating the risk of illicit finance transactions.

State supervisory frameworks

At the state level, the existing frameworks for addressing the potential illicit finance risks of digital assets include state licensing regimes, which include digital asset business activity-specific licenses and state money transmitter licenses, as well as legislation regulating crypto ATMs.

State licensing regimes include several protections relating to illicit finance.[67] For example, digital asset business activity-specific licenses require registrants to set up anti-money laundering programs, programs to prevent the funding of terrorist activities, or both.[68] Where digital asset business

[65] 31 CFR § 1010.100(ff)(5)(i)(A) (emphasis added).

[66] In certain circumstances, additional persons could also be subject to OFAC regulations. *See* Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry, at Pg. 1 (Oct. 2021), https://ofac.treasury.gov/media/913571/download?inline.

[67] Although we are providing an overview of the state frameworks that address digital assets and mitigating illicit finance, we do not take a position on the effectiveness of these frameworks or their necessity. We note that, in certain cases, state-level requirements are, in fact, overly burdensome and duplicative of the requirements at the federal level, as well as other state-level requirements that apply to state money transmitters. If all of the states were to pass individual digital asset licensing frameworks that are both duplicative of other state licensing regimes, as well as existing federal frameworks like the BSA, significant impediments to innovation could arise. A better approach would be to instead enact a strong federal regulatory regime with appropriate safeguards to protect against illicit finance, which would also preempt individual state regimes.

[68] 23 NYCRR § 200.15 (Anti-money laundering program); La. R.S. § 1391.2 (Compliance policies and procedures); Cal. Fin. Code § 3701 (Policies and Procedures Section); SB 1797 / HB 0742 § 10-10 (Required policies and

activity-specific licenses are not required, states require that certain digital asset businesses obtain state money transmitter licenses.[69] Businesses licensed as state money transmitters must also develop programs to mitigate illicit finance. Lastly, although crypto kiosks, or ATMs, tend to be money transmitters, and therefore subject to the BSA and state money transmission laws, many states have also passed crypto ATM-specific legislative frameworks that require operators to receive state-specific licenses and set daily transaction limits, or include such limits in already existing state money transmission laws.[70] Municipalities and localities have also passed ordinances regulating crypto ATMs.

International supervisory frameworks

At the international level, the Financial Action Task Force (FATF)—an intergovernmental body that sets international standards relating to global money laundering, terrorist financing, and proliferation financing—has issued standards for countries relating to "virtual asset service providers."[71] Because of their similarities to traditional financial intermediaries, the FATF requires that "virtual asset service providers" carry out the same preventive measures as financial institutions, such as customer due diligence, record keeping, and suspicious transaction reporting. Notably, the FATF also identifies jurisdictions with weak measures to combat money laundering and terrorist financing in two FATF public documents that are issued three times a year. The FATF's "black-list" identifies high-risk countries or jurisdictions with "serious strategic deficiencies" in countering money laundering, terrorist financing, and proliferation financing, while the "grey-list" identifies countries that are actively working with the FATF to address strategic deficiencies in their regimes for combatting illicit finance.[72] Countries on these lists typically suffer negative consequences to their economies as a result. The FATF provides targeted updates on the implementation of its standards,[73] with the goal of achieving consistency of laws, supervision, and enforcement across jurisdictions.

procedures). At this time, New York and Louisiana have legislation in place that requires certain digital asset businesses, which generally act as financial intermediaries, to obtain state-specific licenses. California has passed legislation that would require digital asset businesses to obtain licenses, but it does not broadly go into effect until the summer of 2026. Both houses of the Illinois legislature also passed a licensing bill.

[69] All states except Montana require money transmitters to obtain a license.

[70] *See, e.g.*, AZ HB2387 (Arizona), Cal. A.B. 39 (California), CO SB079 (Colorado).

[71] Financial Action Task Force, Virtual Assets, https://www.fatf-gafi.org/en/topics/virtual-assets.html.

[72] Financial Action Task Force, "Black and grey" lists, https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html.

[73] International jurisdictions, such as the EU and the UK, also have frameworks that address the potential illicit finance risks of digital assets. For example, the EU's Markets in Crypto-Assets Regulation requires "crypto-asset service providers" (CASPs), as defined in the regulation, to submit to its national competent authority an application that includes "a description of the applicant [CASP's] internal control mechanisms, policies and procedures to identify, assess and manage risks, including money laundering and terrorist financing risks, and business continuity plan robust internal controls, policies, and procedures to identify, assess and manage risks, including money laundering and terrorism financing risks," among other things. Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114), Article 62. The EU's Anti-Money Laundering Regulation (Regulation (EU) 2024/1624) also scopes in CASPs.

Question 17: How should legislation address illicit finance and anti-money laundering issues as they relate to digital assets?

a. What additional authorities, if any, should Congress provide the Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC) to effectively prevent illicit activities relating to digital assets without restricting responsible innovation?

Congress should consider amendments to the International Emergency Economic Powers Act (IEEPA) that would give the Executive branch expanded and clear extraterritorial jurisdiction for sanctions relating to certain foreign digital asset property or interests in property. Such amendments should also include clear language excluding immutable smart contracts from the definition of property.

Congress could create additional authorities similar to FinCEN's authority granted in section 9714(a) of the Combating Russian Money Laundering Act,[74] discussed below, to include other jurisdictions and activities involved in money laundering and sanctions evasion. Under 9714, upon determining that one or more financial institutions operating outside of the United States, or one or more classes of transactions within, or involving, a jurisdiction outside of the United States, or one or more types of accounts within, or involving, a jurisdiction outside of the United States is of primary money laundering concern in connection with Russian illicit finance, the Secretary of the Treasury is authorized to impose one or more of the following special measures: (1) one or more of the special measures described in 31 U.S.C. § 5318A(b), commonly known as section 311 of the USA PATRIOT Act (section 311); or (2) special measures prohibiting or imposing conditions upon certain transmittals of funds, as defined by the Secretary of the Treasury, by any domestic financial institution or domestic financial agency.

In its first use-case of this authority, FinCEN issued an order prohibiting certain transmittals of funds involving Bitzlato, a crypto exchange located in Russia, by any covered financial institution.[75] Creating a similar authority to address North Korean cybercrime or Southeast Asian transnational crime syndicates running pig butchering operations, for example, could be a highly effective legal tool.[76]

---

[74] Public Law 116-283, as amended by section 6106(b) of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81).

[75] *See* Frequently Asked Questions, Fin. Crimes Enf't Network, Subject: Section 9714 Order Prohibits Certain Transmittals of Funds Involving Bitzlato (Jan. 18, 2023), https://www.fincen.gov/sites/default/files/shared/FAQs_Bitzlato%20FINAL%20508.pdf.

[76] There is a strong argument that targeted financial measures, such as section 9714(a) and section 311, are even more effective than traditional sanctions programs. Former Undersecretary for Terrorism and Financial Intelligence Stuart Levey testified in 2008 that:

> In the case of broad, country-wide sanctions that are often perceived as political statements, it can be difficult to persuade other governments and private businesses to join us in taking action. Even when other governments agree with us politically, they generally tend to be unwilling to force their businesses to forgo opportunities that remain open to others. When the private sector views such broad sanctions as unwelcome barriers to business, companies are unmotivated to do more than what is minimally necessary to comply. Indeed, history is replete with examples of participants in the global economy working to evade such sanctions while their governments turn a blind eye.

b. Do digital asset mixers and tumblers warrant special legislative, regulatory or supervisory attention? What are potential ways to combat illicit activities using these technologies while safeguarding privacy rights and free speech?

Digital asset "mixers" and "tumblers" do not warrant special legislative attention because sufficient regulatory and criminal authorities already exist for combating the use of mixers and tumblers for unlawful activities. Those authorities include: (1) civil and monetary penalties under the BSA and regulations issued pursuant to that Act,[77] (2) criminal penalties under Title 18 of the U.S. Code, including money laundering, fraud, drug trafficking, and computer hacking,[78] (3) the sanctions programs that the Office of Foreign Assets Control enforces and administers,[79] and (4) FinCEN "of primary laundering concern" designations that target money laundering and terrorist financing risks.[80]

> The dynamic is different when we instead impose financial measures specifically targeted against individuals or entities engaging in illicit conduct. When we use reliable financial intelligence to build conduct-based cases, it is much easier to achieve a multilateral alignment of interests. It is difficult for another government, even one that is not a close political ally, to oppose isolating actors who are demonstrably engaged in conduct that threatens global security or humanitarian interests. Also, whatever their political views, all countries want their financial sectors to prosper and to have good reputations. They therefore share a common interest with us in keeping their financial sectors untainted by illicit conduct.

See Testimony before the Senate Committee on Finance, Under Secretary for Terrorism and Financial Intelligence Stuart Levey, at 2-3 (Apr. 1, 2008), https://www.finance.senate.gov/imo/media/doc/040108sltest.pdf.

[77] FinCEN has authority to investigate and impose civil monetary penalties on money services businesses that violate the Bank Secrecy Act. *See* 31 U.S.C. § 5321(a); *see also* Fin. Crimes Enf't Network, *First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws* (Oct. 19, 2020), https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf (assessing a civil monetary penalty against the primary operator of digital asset mixer Helix).

[78] Two common charges that the DOJ brings include money laundering or operating an unlicensed money transmission business (or conspiracy charges relating to the same). *See* Dep't of Justice, Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million (Aug. 18, 2021), https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million (convicting the operator of Helix on a money laundering conspiracy charge); Dep't of Justice, Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions (Mar. 15, 2023), https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3 (charging the operator of ChipMixer with money laundering and operating an unlicensed money transmitting business).

[79] OFAC has authority to authorize sanctions against foreign countries, geographic regions, entities, individuals, and property. *See* Exec. Order No. 13694, 80 Fed. Reg. 18,077 (Apr. 2, 2015), https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities. U.S. Dep't of Treasury, *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK* Cyber Threats (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768 (sanctioning digital asset mixer Blender.io); U.S. Dep't of Treasury, *Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency* (Nov. 29, 2023), https://home.treasury.gov/news/press-releases/jy0768 (sanctioning digital asset mixer Sinbad.io).

[80] Section 311 of the USA Patriot Act authorizes the Treasury to designate a foreign jurisdiction, financial institution, class of transactions, or type of account as being of "primary money laundering concern" and to impose one or more of five "special measures" that U.S. financial institutions must institute with respect to the designated

We note that the terms "mixer" and "tumbler" are not defined. While we do not purport to offer definitions for these terms in this submission, we caution against an overly broad interpretation approach to them. Under the Biden Administration, FinCEN issued a notice of proposed rulemaking proposing a special measure under section 311 of the Patriot Act that would have broadly categorized transactions involving "convertible virtual currency (CVC) mixing" as "of primary laundering concern."[81] FinCEN's proposal was its first-ever use of section 311 authority to designate an entire class of transactions within, or outside of, the United States as "of primary laundering concern." In the past, FinCEN had exercised its authority in relation to specific entities, like banks, or foreign jurisdictions, like the Democratic People's Republic of Korea. In our response to the special measure, we explained why FinCEN's proposal was not sufficiently targeted and how it could undermine the use of privacy technologies for legitimate and lawful transactions.[82] To the extent that any legislation expands FinCEN's authority to issue "of primary laundering concern" designations, it should also circumscribe FinCEN's discretion to issue overly broad designations.

While the authorities described above are effective tools for mitigating illicit finance concerns relating to digital asset mixers and tumblers, like the Senate Banking Committee, we strongly support privacy rights and free speech. Importantly, there are many legitimate privacy reasons for using mixers and tumblers. On public blockchains, transactions are transparently recorded on an open, shared digital recordbook. Although digital wallet addresses provide users with a layer of pseudonymity, the pseudonymity is rarely sufficient to preserve a user's privacy and prevent a network observer from connecting a public address to a real-life identity. A wallet address can function like a username, email address, phone number, or bank account number. Once a user interacts with another person or entity, the counterparty can link the pseudonymous wallet address with a particular user, exposing the user's entire onchain transaction history and potentially revealing their personal identity. For example, if a shop accepts payment in cryptocurrencies from its customers, the store's cashiers could see where else those customers had shopped before and the customer's crypto holdings (at least for the wallet on the blockchain network used for that particular transaction). It is no surprise that users of digital assets would,

---

entities or transactions. 31 U.S.C. § 5318A(1). FinCEN has already used the authority against financial institutions that have laundered the crypto proceeds of cyber heists and romance scams (commonly referred to as "pig butchering"). Proposal of Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern, 90 Fed. Reg. 18,934 (May 5, 2025), https://www.federalregister.gov/documents/2025/05/05/2025-07837/special-measure-regarding-huione-group-as-a-foreign-financial-institution-of-primary-money. Section 9714(a) of the Combating Russian Money Laundering Act also allows FinCEN to designate financial institutions as "of primary money laundering concern" in connection with Russian illicit finance. *See* Frequently Asked Questions, Fin. Crimes Enf't Network, *Subject: Section 9714 Order Prohibits Certain Transmittals of Funds Involving Bitzlato* (Jan. 18, 2023), https://www.fincen.gov/sites/default/files/shared/FAQs_Bitzlato%20FINAL%20508.pdf ("A section 9714 action is similar to a section 311 action. However, section 9714 actions are expressly intended to address, and can only be invoked for, primary money laundering concerns in connection with Russian illicit finance, can be implemented via order (without accompanying rulemaking), and can prohibit or place conditions on certain transmittals of funds.").

[81] Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72701 (Oct. 23, 2023), www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions.

[82] *See* Jai Ramaswamy et al., *a16z Letter to the Financial Crimes Enforcement Network: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern* (Jan. 22, 2024), https://www.regulations.gov/comment/FINCEN-2023-0016-2106.

therefore, demand greater privacy protections for their transactions. Accordingly, to the extent that the Senate Banking Committee chooses to bolster or expand the authorities listed above, we recommend a cautious approach that ensures the preservation of both privacy and free speech rights.

c. Which digital asset market participants should be considered financial institutions pursuant to the Bank Secrecy Act?

Digital asset market participants who engage in businesses that resemble traditional financial intermediaries—custodial businesses that can exert independent control over assets, have account and customer relationships with users, and "accept" and "transmit" funds on behalf of users—are and should be considered "financial institutions" pursuant to the BSA. These attributes are consistent with longstanding FinCEN regulations and guidance.

Under FinCEN regulations, the term "financial institution" includes a broad set of financial intermediaries, such as banks, SEC-registered brokers or dealers, money services businesses, and others. When digital asset businesses fall within the scope of the term "financial institution," in general, it is because the business constitutes a sub-category of money services businesses known as "money transmitters." FinCEN's regulations define a "money transmitter" as "a person that provides money transmission services," and further define "money transmission services" as the "acceptance" and "transmission" of currency or the "transfer of funds."[83] The terms "accept," "transmit," and "transfer," have long been interpreted to require control over the underlying value.

FinCEN's guidance on the application of the BSA to different types of digital asset businesses also focuses on control. Specifically, the FinCEN 2019 guidance states that, "[t]he regulatory interpretation of the BSA obligations of persons that act as intermediaries between the owner of the value and the value itself is not technology-dependent. The regulatory treatment of such intermediaries depends on four criteria: (a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the CVC runs; and, (d) whether the person acting as intermediary has ***total independent control*** over the value."[84] Importantly, "total independent control" only exists when an entity or individual has the ability to independently direct the movement of the underlying assets.[85] In addition, FinCEN regulations exempt businesses from the definition of money transmitter that only "provide[] the delivery, communication, or network access services used by a money transmitter to support money transmission services."[86]

Digital asset businesses that are not, from a technical perspective, able to exert total independent control over a user's digital assets should not be considered covered financial institutions. Indeed, FinCEN's 2019 guidance takes the position that digital asset trading platforms and decentralized exchanges are not money transmitters if they provide only a forum where buyers and sellers of digital

[83] 31 C.F.R. § 1010.100(ff)(i)(A).
[84] FinCEN Guidance, FIN-2019-G001, 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 (emphasis added) [hereinafter: FinCEN 2019 Guidance].
[85] Control is also present in traditional forms of money transmission (e.g., physical receipt of a check that a money transmitter exchanges for cash).
[86] 31 CFR § 1010.100(ff)(5)(ii)(A).

assets post their offers and bids, and the parties themselves settle any matched transactions through "an outside venue (either through individual wallets or other wallets not hosted by the trading platform)."[87] However, in circumstances when transactions are matched, and the trading platform purchases the digital assets from the seller and sells it to the buyer, then the platform is acting as a money transmitter. The essential factor is whether a business operator or other person could exercise "independent control" over the underlying asset.

d. To what extent should the President's authority under International Emergency Economic Powers Act apply to digital assets?

Under IEEPA, the President has broad authority to regulate a variety of economic transactions following a declaration of national emergency.[88] Specifically, IEEPA provides the authority to prohibit transactions involving certain "property" in which a foreign "national" or sanctioned "person" has an "interest."[89] OFAC regularly identifies digital asset wallet addresses as blocked property and publishes those wallet addresses on the SDN list.

e. How could legislation promote the use of digital assets and distributed ledger technology to improve regulatory compliance, either within the digital asset ecosystem or more broadly, including by facilitating compliance with the Bank Secrecy Act and Know Your Customer requirements?

One way that legislation could promote the use of digital assets and distributed ledger technology to improve regulatory compliance would be if it directed Treasury and FinCEN to issue rules or guidance allowing emerging technologies to be used for compliance. Considering new methods for addressing illicit finance would also broadly be consistent with provisions mandating research and studies in both the Guiding and Establishing National Innovation for U.S. Stablecoins Act[90] and the Digital Asset Market Clarity Act.[91]

---

[87] *See* FinCEN 2019 Guidance, at § 5.1.

[88] IEEPA authorizes the President to "block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States." 50 U.S.C. §§ 1701-1708 (2018).

[89] The President's authority to authorize sanctions under IEEPA does not extend to immutable smart contracts. In *Van Loon v. Department of the Treasury*, the 5th Circuit held that OFAC had exceeded its statutory authority by designating the immutable smart contracts underlying Tornado Cash — an open-source, decentralized, and ownerless software protocol — on the SDN List. No. 23-50669 (5th Cir. 2024). The immutable smart contracts, in contrast to mutable smart contracts that also made up the Tornado Cash protocol, could not be altered or deleted by anyone. The 5th Circuit found that the Tornado Cash immutable smart contracts did not constitute "property" because property must be "capable of being owned." *Id.*, at 22. OFAC later dropped its designation of the Tornado Cash smart contracts. Treasury Dept., *Tornado Cash Delisting* (Mar. 21, 2025), https://home.treasury.gov/news/press-releases/sb0057.

[90] *See* Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025, S. 1582, 119th Cong. § 9 (2025).

[91] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress § 504 (2025).

A key emerging technology that could be useful for compliance is decentralized identification ("DID"). DID harnesses the unique advantages of the blockchain and sophisticated forms of encryption (for example, zero-knowledge proofs) to allow customers to confirm that they are who they claim to be, at times without even having to disclose their actual personal information. DID works by having a trusted entity, such as a financial institution, verify certain information about an individual (such as a birthdate, social security number, or the fact that they have undergone full KYC as of a certain date) and then issue them an attestation token confirming the fact at issue. The token holder can then use it when interacting with other entities that need to confirm the same fact—for example, that she is a U.S. citizen—without necessarily having to disclose anything additional about herself. The use of such technology should be an acceptable means of meeting CIP requirements and furthers cybersecurity objectives by reducing centralized honeypots of PII that attract hackers.

Because several rules in the BSA may currently limit covered providers' ability to utilize DID, the rules or guidance should take the position that BSA-covered digital asset service providers may adopt decentralized identity tools to improve the effectiveness and efficiency of AML compliance. FinCEN could also work collaboratively with financial institutions to increase adoption of new technology and analytics and encourage the use of decentralized identity.

f. What challenges currently exist in identifying, tracking, and addressing instances of pig butchering?

Law enforcement agencies that have access to and knowledge working with blockchain analytic tools are very effective in investigating romance and investment scams involving cryptocurrency. The challenge with these scams is two-fold. First, the sheer number of victims in the United States means that much of the work falls on state and local law enforcement who may not have the same training and investigative resources as their federal counterparts. Second, these scams are primarily run by extremely sophisticated, hierarchical business operations located almost entirely outside of the United States. As the *New York Times* has reported,[92] individuals throughout China and Southeast Asia have been kidnapped, trafficked, and forced to work in labor camps housed within large compounds, carrying out pig butchering scams. And, politically unstable cities like Myawaddy in Myanmar have allowed pig butchering gangs to operate with impunity.[93] Law enforcement can identify these compounds, interrelated websites and domains, as well as commingled wallets and overseas exchanges used for laundering proceeds, but investigating this type of large-scale transnational crime is complex and requires dedicated resources and coordination with foreign governments.

g. What can the U.S. government do with its existing tools and authorities to more aggressively combat pig butchering?

The U.S. government should provide additional available technical resources to law enforcement investigators and prosecutors, particularly state and local agencies, and pursue these transnational

[92] Isabelle Qian, *7 Months Inside an Online Scam Labor* Camp, N.Y. Times (Dec. 17, 2023), https://www.nytimes.com/interactive/2023/12/17/world/asia/myanmar-cyber-scam.html.
[93] Chainalysis Team, *The On-chain Footprint of Southeast Asia's 'Pig Butchering' Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed* (Feb. 24. 2024), https://www.chainalysis.com/blog/pig-butchering-human-trafficking/.

criminal organizations in a more centralized and coordinated manner. Congress should consider establishing a dedicated national intelligence unit tasked with coordinating and consolidating evidence in individual cases across the country, identifying scam typologies, rapid information sharing with financial institutions, expedited asset recovery, and establishing close communications and agreements with foreign law enforcement and government authorities.

h. What new tools and authorities would help the U.S. government combat pig Butchering?

As mentioned above, Congress could establish additional authority similar to section 9714(a) of the Combating Russian Money Laundering Act, to include financial institutions in Southeast Asia and other jurisdictions which support laundering of scam victim funds and the funding and payment of operating expenses for these criminal organizations.

Key Recommendations:

- Consider amendments to IEEPA that would give the Executive branch expanded and clear extraterritorial jurisdiction for sanctions relating to certain foreign digital asset property or interests in property.
- Create additional authorities similar to FinCEN's authority granted in section 9714(a) of the Combating Russian Money Laundering Act, to include other jurisdictions and activities involved in money laundering.
- Direct Treasury and FinCEN to issue rules or guidance allowing emerging technologies to be used for compliance.
- Establish a national, multi-agency coordination and intelligence center to combat romance and investment scams involving cryptocurrency.

IV. Responses to Committee Questions #22, 26, 27, 29, 30, 31, 33, and 35

Question 22: How should legislation address digital assets that are issued outside of the United States but traded and purchased by United States consumers?

The regulatory framework should apply to offers and sales of digital assets to U.S. persons, consistent with longstanding securities law principles. This includes applying the legislation's disclosure obligations to issuers offering tokens to U.S. persons and ensuring that U.S. persons are subject to the transfer restrictions outlined in the bill. Listing standards for regulated intermediaries can further promote compliance by incentivizing foreign projects seeking access to U.S. users and capital to meet those standards in order to be listed by compliant intermediaries.

Offshoring has become a major challenge due to ongoing regulatory uncertainty. A well-calibrated framework must not only protect U.S. consumers but also onshore entrepreneurs through regulatory clarity and incentives. For example, the crowdfunding regime proposed in the Discussion Draft should be limited to U.S.-based issuers to align with existing crowdfunding regimes and the CLARITY Act.

Combined with new domestic entity structures like the decentralized unincorporated nonprofit association[94] and stablecoin legislation, the regulatory clarity and control-based decentralization framework created by the Committee's legislation will help establish the U.S. as the global center for responsible blockchain innovation.

Question 26: What action should market structure legislation take with respect to decentralized finance?

a. How should an exemption for decentralized finance be structured?
b. What changes, if any, should Congress make to prior legislative attempts to structure an exemption for decentralized finance?

Decentralized finance ("DeFi") delivers substantial public benefits by reducing barriers to entry, increasing user choice, and enhancing transparency.[95] Because DeFi systems are capable of functioning in a genuinely non-intermediated manner—where no party can exert unilateral control or access user funds—they mitigate the risks that traditional financial regulation is designed to address. For this reason, market structure legislation should include a narrowly tailored exemption for truly decentralized systems that do not, in form or substance, function as intermediaries.

Here too we believe that CLARITY, with appropriate modifications, represents an effective model. CLARITY primarily addresses DeFi through a three-pronged approach: in Section 309, the act provides an exclusion for DeFi activities from intermediary registration at the SEC; in Section 409, it offers a parallel carve out for DeFi activities from intermediary registration at the CFTC; and both of these exclusions explicitly exempt persons engaged in activities including the development and administration of "decentralized finance messaging systems" and "decentralized finance trading protocols," terms defined in Title I.[96]

CLARITY's approach to DeFi is effective because it is narrowly tailored to *only* exclude DeFi systems that are genuinely non-intermediated and therefore do not require the application of rules designed to mitigate intermediary risk. For example, the act provides a carve out for persons engaged in activities including the development and administration of "decentralized finance messaging system[s]," which it defines as "[...] a software application[s] that [provide] a user with the ability to create or submit an instruction, communication, or message to a decentralized finance trading protocol for the purpose of executing a transaction by the user."[97] However, it goes on to specify that any system that provides a person other than the user with control of user funds or the ability to execute user transactions cannot avail itself of this carve out.

CLARITY thus makes a critical distinction between systems that simply enable users to engage with DeFi systems, and those that exercise control over user funds or transactions. Importantly, this aligns with the recommendations of the President's Working Group on Digital Assets, which highlights the

[94] Miles Jennings & David Kerr, *The DUNA: An Oasis For DAOs*, a16z crypto (Mar. 8, 2024), https://a16zcrypto.com/posts/article/duna-for-daos/.
[95] Marvin Ammori, *Decentralized Finance: What It Is, Why It Matters*, a16z crypto (June 15, 2021), https://a16zcrypto.com/posts/article/what-is-decentralized-finance/.
[96] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress § 504 (2025).
[97] *Id.*

extent to which an application exercises control over user assets as a key criteria for determining the appropriate regulatory treatment of DeFi.[98] And in this way, the "decentralized finance messaging system" exemption in CLARITY is narrowly-crafted to disapply to systems that function as intermediaries, and therefore pose precisely the risks that intermediary-oriented rules are designed to address.

The same is true of the exemption in CLARITY for persons engaged in activities including the development and administration of "decentralized finance trading protocols," which is conditioned on the absence of controlling persons. Specifically, blockchain systems that do not function according to transparent, predetermined rules or that empower a person or group under common control to alter their rules, cannot be considered "decentralized finance trading protocols," and therefore cannot benefit from this exclusion. Market structure legislation should provide such a carefully calibrated DeFi exemption, specifying that *only* DeFi systems that do not in practice act as intermediaries, thereby introducing the very risks that regulation is designed to mitigate, are eligible.

Nevertheless, the approach CLARITY takes to DeFi can be improved upon. Because it focuses solely on digital commodities, this act does not address other regulated digital assets like tokenized securities and derivatives that may be traded through DeFi systems. And while CLARITY exempts DeFi systems from federal intermediary rules, it does not preempt state regulation—which means the DeFi industry remains exposed to inconsistent or overreaching state-level policies. These gaps should be addressed either in the Senate or through coordinated regulatory guidance (such as SEC and CFTC rulemaking) instructed through legislation.

Question 27: What, if any, action should market structure legislation take with respect to non-fungible tokens?

We support the CLARITY Act's approach to collectible tokens (non-fungible tokens). CLARITY mandates that the Comptroller General carry out a study to analyze the marketplace for collectible tokens, their use-cases, benefits, risks, and more. At the end of a one year period following the act's enactment, the legislation requires that the Comptroller make public the findings of this study.[99] Such an analysis would help provide policymakers and regulators with a more nuanced understanding of collectible tokens. With respect to collectible tokens, we do not believe that legislation should go beyond this at this time, because the SEC already possesses sufficient jurisdiction to provide the guidance necessary to facilitate innovation in this area while protecting consumers.

Though early in their development, collectible tokens already have a wide range of use cases. They are often issued in limited or otherwise well-defined editions and provide ownership of or specific rights to (such as intellectual property rights) works of art, musical compositions, collectible merchandise, and video game assets. Further, they are often used to represent tokenized tickets, event souvenirs, receipts for redeemable tangible items, and loyalty points. Many collectible tokens are simply digital proofs of ownership of existing goods like online imagery or digital swords that can be used in one or more video games. Their value is embedded in the asset to which the collectible token is linked—from being a record of ownership of a tangible or intangible good (or specific rights therein)—rather than being

[98] Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto/
[99] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Congress (2025).

created by or derived from the ongoing efforts of the collectible token's creator or any third party. This is not to say that collectible tokens cannot derive value from the ongoing efforts of any creator or third party, but that they have inherent *economic independence* separate and apart from such creator or third party. This means that collectible tokens generally do not have the inherent characteristics of securities and there should be a strong presumption against the application of federal securities laws to transactions of collectible tokens.[100]

Federal securities laws have limited application to collectible tokens—they do not extend to crypto assets that do not constitute securities under the Securities Act of 1933 or transactions of crypto assets that are not otherwise subject to federal securities laws. However, the analysis of when a transaction in a collectible token may be subject to securities laws can be subjective and difficult, creating uncertainty for creators and entrepreneurs and slowing the pace of innovation without providing investor protections. In a March submission to the SEC, we urged the Commission to resolve this uncertainty through two measures:[101]

- First, the Commission should create a safe harbor (either through a Commission-level policy statement, by providing Commission-level guidance, or by adopting formal rules) that provides objective conditions under which ordinary transactions of collectible tokens are excluded from securities laws. The criteria for eligibility for the safe harbor should be based on the principle that if the asset does not give rise to the risks the federal securities laws are intended to address, the application of such laws is unwarranted and inappropriate. Not all transactions of collectible tokens will be able to avail themselves of the safe harbor. On the contrary, *only* those transactions of collectible tokens which *do not* engender the risks that Section 5 and other federal securities laws were designed to address should be eligible. We elaborate upon such eligibility criteria in our submission.[102]
- Second, the Commission should establish new crowdfunding regulations for transactions of collectible tokens that are not eligible for the above safe harbor because they may engender the risks federal securities laws were intended to address, such as certain capital raising transactions of collectible tokens designed to attract investments for the funding of future creative endeavors. This crowdfunding pathway should be narrowly tailored to empower creators to create while mitigating risks to investors, collectors, and other market participants through the use of blockchain technology. We further elaborate upon this crowdfunding proposal in our submission on this topic.[103]

Through these two measures the Commission can establish clear limits with respect to the application of federal securities laws to transactions of collectible tokens, including crowdfunding transactions. By applying these measures prospectively *and* retroactively, to both existing works and future creative endeavors, the Commission can foster creative innovation and safeguard creators,

---

[100] 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/.

[101] *See* Miles Jennings et al., *Recommendations Regarding a Safe Harbor and Crowdfunding Regime for Collectible Tokens (NFTs)*, a16z crypto (Mar. 27, 2025), https://api.a16zcrypto.com/wp-content/uploads/2025/03/a16z-Safe-Harbor-Proposal-Collectible-Tokens-NFTs.pdf.

[102] *Id.*

[103] *Id.*

collectors, and other market participants from becoming subject to the retroactive application of federal securities laws by regulators in the future. If effectively crafted, these measures would help fulfill the Commission's mandate of protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation, while also promoting responsible innovation in blockchain technology. Given that the Commission already has the authority to effectuate these two recommendations, we recommend that the Committee should seek to harmonize its approach to collectible tokens with that of CLARITY, by solely requiring that the Comptroller General carry out a study to analyze the marketplace for collectible tokens, their use-cases, benefits, risks, and more.

Question 29: What, if any, action should market structure legislation take with respect to decentralized physical infrastructure networks?

No specific action is needed. Decentralized physical infrastructure networks (DePIN) should be evaluated under the same control-based decentralization and transfer restriction framework established in the CLARITY Act. These mechanisms are technology-neutral and suitable for assessing whether DePIN projects function as open, decentralized systems or rely on centralized actors—ensuring consistent treatment across network types without requiring bespoke rules. As discussed in response to **Question #6a**, the Discussion Draft should be modified to be consistent with the CLARITY Act.

Question 30: Should Congress mandate that the SEC consider whether an action would promote "innovation" when conducting rulemakings, as under Section 107 of the discussion draft?

Question 31: Should Congress create an office at the SEC to be responsible for promoting innovation or designate an existing office as encompassing such duties?

Yes on both counts. Congress should revise the SEC's mission to explicitly include fostering innovation, alongside investor protection, market integrity, and capital formation. The current absence of this directive has contributed to inconsistent, overly restrictive treatment of new technologies—including in the digital asset space—often without regard to the broader benefits those technologies may provide.

Short of a statutory mission change, Congress should require the establishment of a permanent innovation-focused office at the SEC—consistent with the Strategic Hub for Innovation and Financial Technology proposed in the CLARITY Act. Such an office should have a clear mandate to engage constructively with emerging technologies, coordinate interagency efforts, and ensure that the SEC's regulatory posture reflects both the risks and the opportunities of innovation.

Question 32: Should legislation encourage interoperability or the development of interoperability across different layer-1 blockchain networks? If so, how?

Yes. Interoperability is a core promise of blockchain technology—it enables composability, facilitates open networks, and ensures users are not locked into systems controlled by centralized actors. Just as open protocols defined the architecture of the internet, interoperable blockchain systems are foundational to realizing a truly decentralized digital infrastructure.

While legislation should not mandate specific interoperability standards, it should encourage them indirectly through incentives for open systems. As discussed in response to **Question #6a**, the

control-based decentralization and transfer restriction framework set forth in the CLARITY Act does exactly this and the Discussion Draft should be modified accordingly. By rewarding projects that relinquish unilateral control and broadly distribute ownership, CLARITY's framework favors open, composable ecosystems where interoperability and enhanced investor protections are a natural outcome.

Question 33: Would a sandbox for distributed ledger technology or other digital assets, including as under proposed Section 401 and Section 404, be useful?

We do not believe legislation should establish a statutory regulatory sandbox. Innovation in crypto is moving too quickly for such a one-size-fits-all program to be effective. Instead, Congress should encourage the SEC and CFTC to adopt discretionary sandbox programs through their existing exemptive and no-action authorities. These programs should be used to supervise novel use-cases—such as AI trading agents and decentralized derivatives protocols—that do not fit neatly into existing frameworks but may still advance core policy goals.

By inviting the agencies to create sandbox mechanisms, legislation can foster innovation without hardcoding unnecessary constraints. Any such programs should include clear entry and exit criteria, transparency requirements, and periodic public reporting. This approach aligns with the broader goals of regulatory modernization and complements the risk-based, control-oriented framework established by the CLARITY Act.

Question 35: Should federal legislation preempt certain state laws, and if so, how?

Yes. Market structure legislation must include strong federal preemption. Without it, the patchwork of inconsistent and often conflicting state laws will continue to frustrate Congressional intent, fragment the national digital asset market, and expose participants to overlapping and contradictory obligations.

As the President's Working Group on Digital Assets noted, "Congress should provide that federal law preempts state law with respect to securities and commodities laws applicable to SEC- and CFTC-registered intermediaries, including in the areas of state virtual currency business, 'blue sky,'; and commodity broker laws."[104]

But preemption must also address other areas. It should also protect core protocol participants and developers from state-level attempts to reassert control over areas explicitly addressed by federal law. That includes persons directly or indirectly engaging in any of the following activities, in relation to the operation of a blockchain system or distributed ledger service or in relation to a non-custodial blockchain-based protocol:

- Compiling network transactions or relaying, searching, sequencing, validating, or acting in a similar capacity;
- Providing computational work, operating a node, providing an oracle service, procuring, offering, or utilizing network bandwidth, or providing similar services or resources;

[104] Report, President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology (July 30, 2025), https://www.whitehouse.gov/crypto/.

- Providing a user-interface that enables a user to read and access data about a blockchain system or distributed ledger;
- Developing, publishing, constituting, administering, maintaining, or otherwise distributing a blockchain system, distributed ledger, user interface, or non-custodial blockchain-based protocol, or operating or participating in a liquidity pool;
- Developing, publishing, constituting, administering, maintaining, or otherwise distributing software or systems that create or deploy hardware or software, including wallets or other systems, facilitating a user's ability to keep, safeguard, or custody the user's digital assets or related private keys.

If federal law fails to preempt in these areas, states will continue asserting jurisdiction in ways that contradict federal policy—creating regulatory inequality across the country. Already, we've seen residents of neighboring states subject to different rights, restrictions, and enforcement outcomes. These disparities not only hurt consumers, but also undermine innovation, confuse compliance, and destabilize enforcement consistency.

Recent litigation reinforces the urgency of preemption. Even after the SEC dismissed its lawsuit against Coinbase, several states refused to follow suit—continuing actions based on identical or derivative theories. This fractured enforcement landscape shows that uniform federal rules alone are not enough. Without explicit and retroactive preemption, state regulators will likely continue pursuing legal theories that Congress has expressly rejected, undermining the very goals of federal legislation.

To be clear, preemption should not displace state anti-fraud or anti-manipulation authority. But it must preclude states from reclassifying assets or imposing additional restrictions on digital commodities and decentralized infrastructure already covered under federal law.

* * * *

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

Respectfully submitted,

Miles Jennings, Head of Policy & General Counsel
a16z crypto

Michele R. Korver, Head of Regulatory
a16z crypto

Jai Ramaswamy, Chief Legal Officer
a16z

Scott Walker, Chief Compliance Officer
a16z