April 9, 2025

BY ELECTRONIC SUBMISSION

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

> Re: **Comments on the SEC Crypto Task Force's Questions Concerning the Custody of Crypto Assets**

Dear Commissioner Peirce:

        Andreessen Horowitz ("a16z" or "we") appreciates the opportunity to respond to the request for information that the Securities and Exchange Commission's Crypto Task Force (the "**Crypto Task Force**") provided to the public on February 21, 2025 (the "**Statement**").[1] The Task Force's thoughtful approach, seeking detailed and comprehensive information about a wide range of crypto issues, is commendable. While we recognize that the questions are not a roadmap to actions the Commission will take, we nonetheless applaud the Commission for its commitment to soliciting information from the public through a transparent process and its willingness to engage.

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

        In this submission, we respond to a number of the Crypto Task Force's questions regarding the safe, legal, and practicable custody of crypto assets by registered investment advisers ("**RIAs**") (**Questions #27-29**), as well as to several questions regarding the custody of such assets more generally (**Questions #21-23**). In addition to responding individually and specifically to the six questions identified, this submission also identifies, in **Annex A** to this letter, the broad principles that we believe should determine the regulatory structure for the custody of crypto assets (the "**Crypto Custody Principles**").

---

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

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

We also reference these Crypto Custody Principles in our response to the specific questions posed in the Statement.

I.   About a16z

a16z is a venture capital firm that invests in seed, venture, and late-stage technology companies, focused on American Dynamism, bio and healthcare, AI-consumer, crypto, AI-enterprise, fintech, and games. a16z currently has more than $74 billion in regulatory assets under management across multiple funds, with more than $7.6 billion in committed capital for crypto-focused 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. As the earliest and largest investor in many crypto and web3 companies and projects, and as one of the largest investment advisers in the advanced technology space, a16z is well-positioned to respond to the Crypto Task Force's timely and important questions around the custody of crypto assets.

II.   Responses to Crypto Task Force Questions #21, 22, 23, 27, 28 and 29

Question 21: Should the Commission amend existing rules, propose new rules, or provide guidance to facilitate custody arrangements for crypto assets? If so, what rule amendments or new rules would be appropriate, and to which types of activities should they apply? Should the Commission propose any specific changes to its rules to accommodate the self-custody of crypto assets by entities registered with the Commission? If so, what conditions should apply to self-custody arrangements to mitigate any related risks? Should the requirements for crypto assets that are securities and those that are not differ?

We believe the Commission should provide new guidance to facilitate custody arrangements for crypto assets, even if only as a temporary measure until it issues new rules. The Commission has previously taken this approach, specifically in the context of crypto asset custody, through its Statement in 2020 on the "Custody of Digital Asset Securities by Special Purpose Broker-Dealers" (the "SPBD Statement").[3] While we agree with your observation that the special-purpose broker dealer designation "has not been a success,"[4] we also agree with the Commission's decision to provide a statement of guiding principles for custodying crypto assets therein.

We agree with the Commission that the provision of guidance does not have to be at the cost of adopting rules. As the Commission observes in the SPBD Statement, such guidance can "provide market participants with an opportunity to develop practices and processes that will enhance their ability to demonstrate possession or control over digital asset securities." This serves the purpose of promoting robust safeguarding standards while not suffering the time delays inherent in the rulemaking process, as

---

[3] Commission Statement, Securities Exchange Act Rel. No. 34-90788, Custody of Digital Asset Securities by Special Purpose Broker-Dealers, 86 Fed. Reg. 11627 (Feb. 26, 2021), https://www.govinfo.gov/content/pkg/FR-2021-02-26/pdf/2020-28847.pdf.
[4] Statement, Securities and Exchange Commission, Hester M. Peirce, The Journey Begins (Feb. 4, 2025), https://www.sec.gov/newsroom/speeches-statements/peirce-journey-begins-020425.

providing guidance is typically easier and quicker than adopting rules. The implementation of such guidance will meet the needs of the industry for quicker clarity and allow the Commission to maintain its historical approach of technological neutrality[5] while also providing the Commission with valuable experience in overseeing the custody of crypto asset securities to inform further action in this area, including potential rulemaking. This would allow firms to consider and implement a broad range of technologies and procedures that the Commission can examine and oversee, leading to convergence around optimal technologies and procedures over time.

As an initial matter, any guidance will need to clearly delineate between crypto asset types. We would recommend that the guidance incorporate a crypto asset taxonomy like the one we suggested in our response submitted on March 13, 2025.[6] This will enable the Commission to distinguish between security tokens (the digital representation of a security on a blockchain) from other token types, like network tokens, that may not appropriately be classified as securities. Further, the Commission should account for potential changes to the regulatory frameworks applicable to network tokens, including any jurisdiction the Commodity Futures Trading Commission ("**CFTC**") may potentially assert over secondary trading of network tokens, as proposed in the most recent market structure legislation.[7]

As we discuss further below and in our Crypto Custody Principles, we recommend that guidance from the Commission encompass:

- The conditions and protections that custodians should typically provide with respect to crypto assets under their custody (see **Annex A: Crypto Custody Principles 1 and 2**).
- The conditions under which RIAs are permitted to temporarily remove crypto asset securities from third-party custodians (see **Annex A: Crypto Custody Principles 3 and 4**).
- The conditions under which an RIA is permitted to self-custody a crypto asset (see **Annex A: Crypto Custody Principle 5**).

As we discuss in further detail, we urge the Commission to permit RIAs to self-custody security tokens (i.e., crypto assets that are securities) and clarify that the self-custody of crypto assets by RIAs would not conflict with the Custody Rule or fiduciary duties. For the avoidance of doubt, we are not advocating for the scope of the Custody Rule to expand, instead we are advocating for the appropriate treatment of crypto asset securities under this rule and in parallel, defining principles that could be made available to RIAs for crypto assets regardless of the method of custody. Importantly, the self-custody of crypto assets is not likely to lead to the fracturing or erosion of custodial or fiduciary norms. Rather, permitting self-custody should not compromise the safety and security of these crypto assets (regardless

---

[5] *See*, *e.g.*, Fact Sheet, Final Amendments to Electronic Recordkeeping Requirements (Oct. 12, 2022), https://www.sec.gov/files/34-96034-fact-sheet.pdf ("The amendments are designed to modernize the rule given technological changes over the last two decades and to make the rule **technology neutral** to be able to adapt to new technologies in electronic recordkeeping.") (emphasis added).

[6] Miles Jennings et al., *Response to Questions 1-6 of the SEC Crypto Task Force's Request for Information*, a16z (March 13, 2025), https://a16zcrypto.com/posts/papers-journals-whitepapers/control-based-decentralization-framework-securities-laws/ [hereinafter: "Response to Questions 1 through 6"].

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

of their securities status) precisely because RIAs are fiduciaries and because the Commission exerts significant powers of supervision, examination, and control over RIAs. As we discuss further under the Crypto Custody Principles, we advocate that at a minimum the Commission permit self-custody, primarily where (1) the use of a qualified custodian is not readily available; (2) self-custody would not lead to any material diminution in safety, verifiability, and transparency; or (3) where such custody is necessary or desirable to exercise attendant rights associated with idle assets (see **Annex A: Crypto Custody Principle 5**). Restricting self-custody to these circumstances will further ensure that custodial and fiduciary norms are maintained.

We also submit that custodial requirements should clearly distinguish between different categories of crypto assets while still ensuring that non-security crypto assets are custodied in a manner that is substantially as secure as crypto asset securities. Specifically, the requirements should differentiate crypto assets that are securities (e.g., security tokens) and crypto assets that are not (e.g., network tokens, arcade tokens, and certain asset-backed tokens like liquid staking tokens and stablecoins, etc.).[8] The Commission has itself noted that in the advisory context, the fiduciary duty extends to the entire relationship between the adviser and client regardless of whether a specific holding in a client account meets the definition of funds or a security.[9] Determining the dividing line between securities and non-securities in the crypto asset context has thus far been a major compliance burden for most RIAs, in significant part because of the unclear dividing line provided by earlier Commission enforcement actions. In our experience, many RIAs have resorted to complying with custodial norms, where possible, for all crypto assets out of an abundance of caution. As we discuss further below, our proposed Crypto Custody Principles apply to security tokens, while also requiring that RIAs self-custody or use other third party custodians meeting substantially similar requirements for other crypto asset types that are likely not securities (network tokens, company-backed tokens, arcade tokens, asset-backed tokens, etc.) (see **Annex A: Crypto Custody Principles 1 and 2**).

Question 22: Public, permissionless blockchains are being used to tokenize permissioned assets. To the extent the custody rules for broker-dealers, investment advisers, and investment companies are implicated, how should the Commission differentiate between native crypto assets of permissionless blockchains and tokenized permissioned assets? Does either type of crypto asset present greater risks of theft or loss?

We submit that there is no reason to believe that private, permissioned blockchains are universally safer or superior to public blockchains or *vice versa*. Private blockchains play an important and necessary role in the crypto universe, as do public blockchains. Private blockchains can be highly efficient and effective in certain contexts, while the trustless, dispersed character of public blockchains is equally valuable in others. There neither is, nor can be a universal rule—the security of each blockchain depends upon its specific technological and economic facts.

---

[8] *See* Jennings, *supra* note 6.
[9] Safeguarding Advisory Client Assets, Release No. IA-6240, 88 Fed. Reg. 14672, 14679 (Mar. 9, 2023), https://www.govinfo.gov/content/pkg/FR-2023-03-09/pdf/2023-03681.pdf.

Public blockchains such as Bitcoin and Ethereum are "trust machines" built to operate in the world wide web. "Public blockchains can be accessed by anyone and users have little reason to believe in each others' goodwill and often cannot rely on 'off-chain' mechanisms (such as legal contracts) to protect themselves against fraud and abuse."[10] By contrast, permissioned assets on a public blockchain restrict access to a select circle of persons and institutions. These tend to already maintain business relationships and operate within a framework of existing contracts, laws, and connected technical systems. For permissioned assets, making trustlessness the overarching design principle is neither necessary nor useful.[11]

For example, in the context of bitcoin, the widely distributed, decentralized nature of the Bitcoin blockchain is a significant safeguard because it makes disruptive or manipulative activity by a single player or a group of players extremely unlikely to execute. For a different type of asset—for instance, a privately offered tokenized security—a private, permissioned blockchain may offer a more secure environment for personal information.

In response to the other aspect of the Commission's question, we do not think the Commission should differentiate between native crypto assets of permissionless blockchains and tokenized permissioned assets. These two types of crypto assets do not present greater risks of theft or loss, relative to each other. In custodial terms, crypto assets present two principal risks:

1) the risk arising from custody of the token; and
2) in the case of an asset-backed token, the risk arising from custody of the underlying asset.

In terms of the custodial risks presented by the token itself, there appears to be no material basis for a distinction between native crypto assets and tokenized permissioned assets, unless the permissioned asset has features that allow for a third-party to control distribution, reproduction, and revocation of the asset. Each type of token is subject to substantially the same types of risks of theft, loss, or misappropriation; however, to the extent the token is a permissioned asset that includes the above-mentioned features it can be potentially recovered, and in the case of an asset-based token, the underlying offchain assets will likely need to be custodied with a qualified custodian. The custodial norms for that underlying asset will likely depend on the nature of the underlying asset; custodial norms for most classes of other assets (e.g., traditional securities, cash, or commodities) are already well-established.

To summarize our response to this Question 22:

1) Expressing a regulatory preference for one type of blockchain over another would appear to violate the technological neutrality to which the Commission seeks to adhere.
2) In terms of the custodial risks, there appears to be no material basis for a distinction between native crypto assets and tokenized permissioned assets.

---

[10] Elias Strehle, *Public Versus Private Blockchains* (Blockchain Research LabWorking Paper Series No. 14), https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/BRL-Working-Paper-No-14-Public-vs-Private-Blockchains.pdf.
[11] *Id.* at 1-2.

Instead of seeking to distinguish broadly based on the public or permissioned character of the blockchain or the nature of the tokenized asset, the appropriate regulatory measures may likely involve requiring RIAs and custodians to:

1) take steps to assess, document and reasonably guard against the specific risks and vulnerabilities associated with the individual blockchains or networks on which specific crypto assets are based (including, for example, around the speed, scalability, resiliency, extensibility, and consensus mechanisms of such blockchains);[12] and

2) provide timely and appropriate disclosures and updates to their clients regarding such risks, vulnerabilities and any untoward events.[13]

We discuss these requirements further in **Annex A** (see **Crypto Custody Principle 2**, under "Disclosure.")

---

[12] Note that this approach is already one that the Commission adopted in the SPBD Statement. *See* SPBD Statement, 86 Fed. Reg. at 11629-30 ("A third step the broker-dealer could take is to establish, maintain, and enforce reasonably designed written policies and procedures to conduct and document an assessment of the characteristics of a digital asset security's distributed ledger technology and associated network prior to undertaking to maintain custody of the digital asset security and at reasonable intervals thereafter. The assessment could examine at least the following aspects of the distributed ledger technology and its associated network, among others: (1) Performance (*i.e.,* does it work and will it continue to work as intended); (2) transaction speed and throughput (*i.e.,* can it process transactions quickly enough for the intended application(s)); (3) scalability (*i.e.,* can it handle a potential increase in network activity); (4) resiliency (*i.e.,* can it absorb the impact of a problem in one or more parts of its system and continue processing transactions without data loss or corruption); (5) security and the relevant consensus mechanism (*i.e.,* can it detect and defend against malicious attacks, such as 51% attacks or Denial-of-Service attacks, without data loss or corruption); (6) complexity (*i.e.,* can it be understood, maintained, and improved); (7) extensibility (*i.e.,* can it have new functionality added, and continue processing transactions without data loss or corruption); and (8) visibility (*i.e.,* are its associated code, standards, applications, and data publicly available and well documented). The assessment also could examine the governance of the distributed ledger technology and associated network and how protocol updates and changes are agreed to and implemented. This would include an assessment of impacts to the digital asset security of events such as protocol upgrades, hard forks, airdrops, exchanges of one digital asset for another, or staking. Such assessments would allow a broker-dealer to be able to identify significant weaknesses or other operational issues with the distributed ledger technology and associated network utilized by the digital asset security, or other risks posed to the broker-dealer's business by the digital asset security, which would allow a broker-dealer to take appropriate action to identify and reduce its exposure to such risks. Accordingly, if there are significant weaknesses or other operational issues with the distributed ledger technology and associated network, the broker-dealer would be able to determine whether it could or could not maintain custody of the digital asset security.").

[13] In this regard, the recent $1.5 billion fund loss of ByBit demonstrates the importance of secure design and testing for qualified custodians. Had ByBit been required to conduct proposed testing and design analysis, it is likely they would have been aware of the mechanisms used to steal funds from them and could have successfully reduced or eliminated the impact prior to the full loss of funds. *See* Dikla Barda, Roman Ziakin & Oded Vanunu, *The ByBit Incident: When Research Meets Reality*, Check Point Research (Feb. 23, 2025), https://research.checkpoint.com/2025/the-bybit-incident-when-research-meets-reality/.

Question 23: Are there commonly accepted practices and standards for auditing and accounting for crypto asset investments and transactions, including those related to valuation? How about with respect to verifying the existence and valuation of crypto assets, both among auditors and attestation providers (including non-accountant providers)? Should the Commission propose additional or specific requirements to address the unique nature of crypto assets?

There is a swiftly emerging body of best practices and standards for (1) the auditing and accounting of crypto assets and crypto asset transactions, as well as (2) the existence and valuation of crypto assets. We are not accountants or auditors, but we engage with accountants and auditors regularly in a variety of contexts, including crypto asset-related transactions, and it is our experience that practices and standards in these areas have rapidly converged in many respects.

In support of these observations, we would note the following developments, among several others:

- The Financial Accounting Standards Board ("**FASB**") issued Accounting Standards Update 2023-08 in December 2023, which is effective for fiscal years beginning after December 15, 2024. That update requires an entity to present:
  - crypto assets measured at fair value separately from other intangible assets in the balance sheet, and
  - changes from the remeasurement of crypto assets separately from changes in the carrying amounts of other intangible assets in the income statement (or statement of activities for not-for-profit entities).[14]
- The Public Company Accounting Oversight Board ("**PCAOB**") published a report entitled "Inspection Observations Related to Public Company Audits Involving Crypto Assets."[15] That report, among other things, provides a list of recommended actions for auditors of public companies and broker-dealers transacting in, or holding crypto assets.[16] It also notes that PCAOB has observed a series of "good practices" that "enhance audit quality," such as the use of technology-based tools to support audits of crypto assets.[17]
- The development and increased adoption of the Cryptocurrency Security Standard ("**CCSS**"), an open standard that focuses on the storage and usage of crypto assets within an organization.[18] CCSS is designed to augment standard information security practices and to complement existing standards, such as ISO 27001 (which enables organizations to establish an information security management system and apply a risk management process).
- Auditors have increasingly adopted new techniques and tools, such as:
  - Use of blockchain analysis tools to trace transactions and verify balances.

---

[14] Fin. Accounting Standards Bd., Accounting Standards Update 2023-08—Intangibles—Goodwill And Other—Crypto Assets (Subtopic 350-60): Accounting For And Disclosure Of Crypto Assets (Dec. 2023), https://www.fasb.org/page/PageContent?pageId=/projects/recentlycompleted/accounting-for-and-disclosure-of-crypto-assets.html.

[15] Pub. Co. Accounting Oversight Bd., Spotlight: Inspection Observations Related to Public Company Audits Involving Crypto Assets (June 2023), https://pcaobus.org/documents/crypto-assets-spotlight.pdf.

[16] *Id*. at 5,7, and 9.

[17] *Id.* at 11-12.

[18] *See What is the CCSS*, Cryptocurrency Certification Consortium (C4), https://cryptoconsortium.org/standards-2/.

o   Procedures to verify ownership/control of crypto assets, such as requesting signed messages from wallet addresses.

o   Approaches to auditing crypto valuations, including assessing the appropriateness of pricing sources.

o   Testing completeness of crypto transaction records by reconciling onchain and offchain data.

We strongly support requiring crypto custodians to undergo an annual surprise audit by a PCAOB-registered auditor. As we discuss further in **Annex A**, we believe that SOC 1 and SOC 2 audits, penetration tests (including ISO 27001 tests), and tests of disaster recovery procedures and business continuity planning, should all form part of such audits. We discuss these requirements further in **Annex A**: **Crypto Custody Principle 2** (under "Audit").

Question 27: What challenges do [RIAs] face in complying with the Investment Advisers Act of 1940 ("Advisers Act") as it relates to investments in crypto assets that are securities? What common practices, if any, have developed to address these challenges?

>   a.   **Could best execution or recordkeeping obligations, or compliance with Form ADV or Form PF disclosure requirements, be clearer in the crypto asset context?**
>   b.   **Do any crypto asset characteristics or market structures place advisory client crypto assets at a greater or different risk of theft, loss, or misappropriation? If so, how can those risks be addressed?**

An important challenge that RIAs face in complying with the Advisers Act is balancing their primary fiduciary duty of profitably investing client assets against their secondary obligation to safeguard those assets. As we discuss below, safeguarding crypto assets gives rise to certain unique challenges, which has ramifications on how an RIA can invest those assets and, therefore, potentially on an RIA's ability to generate investment returns. While those challenges are not necessarily greater than those faced in regard to traditional assets, their potential effect on an RIA's fiduciary duties makes them different in-kind and deserving of nuanced and thoughtful regulatory treatment, especially considering that the relative importance of an RIA's duties means that safeguarding client assets cannot come at the expense of maximizing investment returns. Below, we discuss the most significant regulatory challenges that RIAs face and common practices that have developed with respect to: (1) the "Thin" Crypto Custodial Market, (2) the unique features of crypto assets, (3) best execution requirements, (4) recordkeeping obligations, and (5) Form PF and Form ADV Disclosure Requirements.

Regulatory Challenges and the "Thin" Crypto Custodial Market: The Advisers Act's Custody Rule applies to an RIA's customers' funds and securities.[19] With respect to traditional assets, the application of this rule is generally straightforward, but in the crypto context, there is considerable uncertainty about which crypto asset transactions are securities transactions, and consequently, about whether rules that apply to the custody of securities should apply to these transactions.

As a threshold matter, many crypto assets are not securities, as we discussed in our Response to Questions 1 through 6, and therefore, an RIA must determine whether their crypto assets constitute

---

[19] Rule 206(4)-2 under the Investment Advisers Act of 1940, 17 CFR 275.206(4)-2.

"funds" under the Custody Rule. Nonetheless, determining whether crypto assets constitute "funds" may introduce an additional level of complexity into an RIA's compliance procedures when it is already struggling with the non-uniform approaches that exist with respect to token classification. While some RIAs have made good faith attempts to determine whether the crypto assets they hold are securities or funds, other advisers have made the prudential decision to treat crypto assets as covered assets (i.e., securities or funds) for purposes of the Rule, in the absence of any specific regulatory guidance to the contrary.[20] Accordingly, and as we discuss earlier, our **Crypto Custody Principles** currently apply only to crypto asset securities, but they also require that non-security crypto assets held by RIAs be custodied in a manner that is substantially as secure as crypto asset securities.

In addition, the lack of meaningful guidance on custodying crypto assets has made it difficult for crypto asset intermediaries to discern which existing custodial options are secure, and it has disincentivized businesses from entering the crypto custody market. Specifically, the Custody Rule includes four categories of qualified custodians, of which the most common are typically broker-dealers and banks. However, although these custodians are eligible to custody a wide range of crypto assets, they typically face regulatory obstacles that make it impossible or economically infeasible to do so. For example, as we discussed in our response to Question 21, SPBDs that are permitted to self-custody crypto asset securities cannot take custody of crypto assets that are not securities.[21] In addition only two entities have, over a four-year period, managed to attain SPBD status,[22] which suggests acquiring SPBD status is a commercially questionable decision, at best, for most entities.

The regulatory situation for banks is hardly better. The Office of the Comptroller of Currency ("OCC") has affirmatively stated that banks may take custody of crypto assets,[23] but has granted national trust bank charters to only a few entities that are seeking to custody crypto assets.[24] Moreover, the OCC previously required national banks and federal savings associations to receive prior written supervisory

---

[20] Scott Walker & Neel Maitra, *Crypto Asset Custody by Investment Advisers After the SEC's Proposed Safeguarding Rule*, 56 Review of Securities & Commodities Regulation 75 (Mar. 2023).

[21] SPBD Statement, 86 Fed. Reg. at 11631.

[22] Press Release, tZERO, *tZERO Receives Landmark Approval To Custody Digital Securities and Support End-to-End Digital Securities Lifecycle in the United States* (Sept. 10, 2024), https://www.prnewswire.com/news-releases/tzero-receives-landmark-approval-to-custody-digital-securities-and-support-end-to-end-digital-securities-lifecycle-in-the-united-states-302242412.html; Press Release, Prometheum Inc. Prometheum Receives First of Its Kind Approval From FINRA to Clear and Settle Digital Asset Securities (Jan. 10, 2024), https://www.businesswire.com/news/home/20240110419249/en/Prometheum-Receives-First-of-Its-Kind-Approval-From-FINRA-to-Clear-and-Settle-Digital-Asset-Securities.

[23] *Re: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers*, OCC Interpretive Letter 1170 (July 22, 2020).

[24] Anchorage Digital is the only federally chartered crypto bank. The OCC granted conditional approvals to Paxos National Trust and Protego Trust Company, but both of those approvals expired. *See* Max Bonici, Stephen T. Gannon & Kristal Rovira, National Trust Banks – Revisited for Crypto and Payments, Davis Wright Tremaine LLP (Nov. 24, 2022), https://www.dwt.com/blogs/financial-services-law-advisor/2024/11/why-fintechs-should-consider-national-trust-banks; *see also* OCC Conditional Approval of Application by Anchorage Trust Company, Sioux Falls, South Dakota to Convert to a National Trust Bank (Jan. 13, 2021); OCC Conditional Approval of Application to Charter Paxos National Trust (Apr. 23, 2021); OCC Conditional Approval of Application by Protego Trust Company, Seattle, Washington, to Convert to a National Trust Bank (Feb. 4, 2021).

non-objection before engaging in certain legally permissible crypto-asset-related activities, which had a chilling effect on their ability to engage with crypto.[25] As a result, the total number of crypto qualified custodial entities is quite low. As the Commission observed in 2023, the entirety of the crypto custodial landscape in the U.S. amounted to: "one OCC-regulated national bank, four OCC-regulated trusts, approximately 20 state-chartered trust companies, and other state-chartered, limited purpose banking entities, and at least one [futures commission merchant]."[26] This very small group of custodians is not sufficient to serve a multi-trillion dollar growing industry, and it raises significant concerns regarding concentration risk.

Certain Unique Features of Crypto Assets: Complicating the picture further is that even the custodians willing to custody crypto assets may not be able or willing to custody a broad range of crypto assets with their distinct features and associated rights. The Custody Rule long predates crypto assets and did not anticipate their emergence. Crypto assets are unlike traditional physical assets that have been historically custodied in many ways, but perhaps most notably in that a holder's control over a crypto asset is not proof of the absence of any other person's control over that same crypto asset. More than one entity may have access to the private keys related to a set of crypto assets, and consequently, more than one person may be able to effectuate a transfer or disposition of those crypto assets regardless of the contractual rights authorizing such conduct.[27]

Importantly, crypto assets may have multiple inherent economic or governance rights associated with the asset, which sometimes may only be exercised if the crypto asset holder temporarily deploys those assets out of custody.[28] For example, and perhaps most prominently, certain crypto assets can earn income from staking or yield farming, or include voting rights.[29] In contrast to traditional debt or equity securities, which do not require that holders transfer the assets or take any further action after acquiring them in order to earn income (such as dividends or interest) "passively," the process of staking or voting in regard to crypto assets may require shifting control of the asset from the custodian to an unaffiliated third-party program. Exercising the rights associated with crypto assets, therefore, creates unprecedented challenges for custody arrangements. Without a solution, holders of crypto assets, including RIAs, are faced with the difficult choice: either leave their assets in custody at all times and forego all associated income or governance participation, or exercise the rights associated with the crypto assets and risk potential losses that arise from having to remove their assets from custody.[30]

Faced with these complexities, many compliance-minded RIAs have resorted to self-custody as a potential balance between the need for secure custody and the deployment of the full range of rights associated with the asset. In custodying crypto assets, such RIAs have sought to meet the principles underlying the Custody Rule—namely security and segregation of the assets, independent audit or verification of the assets, and timely disclosures regarding the assets to RIA clients. Pursuant to these

---

[25] OCC Interpretive Letter No. 1183 (Mar. 7, 2025), https://occ.gov/topics/charters-and-licensing/interpretations-and-actions/2025/int1183.pdf.

[26] "Safeguarding Advisory Client Assets," 88 Fed. Reg. at 14739-40.

[27] Walker & Maitra, *supra* note 20.

[28] *Id.*

[29] *Id.*

[30] *Id.*

principles, compliance-minded RIAs that custody crypto assets will typically use some or all of the following protective measures:[31]

- operational controls for multi-step transfer instructions, and multi-person or multi-system approval mechanisms (e.g., the requirement that two or more unaffiliated persons authorize any transfer of crypto assets);
- relatedly, strong authentication requirements to access private key materials (whether complete or shards), which require authorization from multiple key holders, or multi-party computation (a method for joint computation of a crypto asset transaction while each component input is maintained privately from one another);
- the use of hardware security modules, which are tamper-resistant devices aimed at securing cryptographic keys;
- "air-gapping," that is, ensuring that the device that holds private key material is isolated from any connected network;
- insurance arrangements against breaches of the custodian's cybersecurity (insurance arrangements for specific crypto assets are evolving but are still nascent);
- System and Organization Controls ("SOC") reports around the custodian's security, availability, processing integrity, and privacy controls, as well as annual audits of the crypto assets under custody; and
- transparency to investors (through instant access through an application programming interface ("API") or website) regarding crypto assets held by the custodial entity.

Notably, many RIAs have successfully and consistently used these protective measures for some years now. We would also note that despite the absence of specific regulatory guidance around the custody of crypto assets, many RIAs who custody their crypto assets on the basis of these protections have been subject to multiple examinations by the Commission's Division of Examinations, FINRA, and state authorities, without attracting adverse enforcement action.

In addition to these protective measures, we also suggest several principles that the Commission should consider to make custody easier for RIAs dealing in crypto assets, which we also describe in our **Crypto Custody Principles** in **Annex A**.

Below, we also provide brief responses to the Commission's more specific queries under Section 27(a) and (b).

Best Execution Requirements: On December 14, 2022, the Commission proposed a new regulation which would establish a best execution standard for broker-dealers ("Regulation BestEx").[32] The Commission also proposed that Regulation BestEx would extend to crypto assets and broker-dealers dealing in crypto asset securities. We have strongly opposed the Commission's Regulation BestEx proposal, particularly as applied to RIAs dealing in crypto assets, and we take this opportunity to reiterate

---

[31] *Id.* at 85. We have based part of our response to Question 29 on these and other related practices.
[32] Regulation Best Execution, 88 Fed. Reg. 5440 (proposed Jan. 27, 2023), https://www.govinfo.gov/content/pkg/FR-2023-01-27/pdf/2022-27644.pdf.

our opposition and ask that the Commission recognize an appropriately tailored duty of best execution for RIAs dealing in crypto assets.[33]

As proposed, Regulation BestEx would require that, in any securities transaction for a customer or a customer of another broker-dealer, a broker-dealer must:

1) Use reasonable diligence to ascertain the best market for the security; and
2) Buy or sell in such market so that the price to the customer is as favorable as possible under prevailing market conditions.[34]

As a preliminary matter, we agree that RIAs have a fiduciary duty to seek best execution of their clients' transactions, which forms part of their broader duty of care. An investment adviser's duty to seek best execution of its client's transactions applies only where the adviser has the responsibility to select broker-dealers to execute client trades (usually in the case of discretionary accounts).[35] That duty of best execution requires that an adviser seek to obtain the execution of transactions for each of its clients, such that the client's total cost or proceeds in each transaction are the most favorable under the circumstances.[36] An adviser fulfills this duty by seeking to obtain the execution of securities transactions on behalf of a client with the goal of maximizing value for the client under the particular circumstances occurring at the time of the transaction.[37] The duty of best execution is therefore deeply contextual and can vary significantly according to the circumstances.

However, in contrast to the duty of best execution, Regulation BestEx provides bright line rules and would require brokers to evaluate markets using factors such as best displayed prices, opportunities for price improvement, the trading characteristics of the security, the size of the order, the likelihood of execution, and the accessibility of the market. While these factors may be relevant to a determination of best execution, in an evolving market such as the one for crypto assets, the Commission should not seek to provide bright line rules regarding best execution. Instead, we believe that the Commission's examination authority, RIA disclosures to clients regarding transactions, and competition among investment advisers should be sufficient to police best execution by RIAs.

As a general principle, rather than defining best execution narrowly in the crypto asset context, the Commission should recognize the conditions that enable RIAs to make that determination in their particular contexts and circumstances. This more flexible approach would also allow the Commission to keep open more avenues that might allow an RIA to achieve best execution for its client transactions. For example, and as we discuss in **Crypto Custody Principle 4** in **Annex A**, the Commission should expressly recognize that RIAs may transfer an asset out of custody to a crypto trading venue to secure best execution for that asset—and this should be seen as an act in furtherance of the RIA's fiduciary duty,

---

[33] *See* Jai Ramaswamy, Scott Walker & Miles Jennings, a16z Comment Letter on Reg. BestEx, a16z (Mar. 28, 2023), https://www.sec.gov/comments/s7-32-22/s73222-20161914-330741.pdf

[34] Proposed Rule § 242.1100 (The best execution standard).

[35] Commission Interpretation Regarding Standard of Conduct for Investment Advisers, 84 Fed. Reg. 33669 at 33674, (July 12, 2019), https://www.govinfo.gov/content/pkg/FR-2019-07-12/pdf/2019-12208.pdf.

[36] *Id.*

[37] *Id.* at 33675.

not in breach of its obligation to custody client assets securely. We agree that there should be limitations on this principle, namely that: (1) the RIA must reasonably assure itself as to the resilience and security of the trading venue; and (2) must return the asset to custody if the trade cannot be duly executed at the venue. Likewise, our other proposed Crypto Custody Principles embody this flexible approach.

Recordkeeping Obligations: The Commission should permit RIAs to rely on information that is publicly available on blockchains to meet the recordkeeping requirements under Rules 204-2(a) and (b) of the Advisers Act. Blockchains are true, trusted, and current records that provide most, if not all of the items that Rules 204-2(a) and (b) require, and unlike in the case of best execution, these recordkeeping requirements are clear and defined for RIAs custodying both traditional and crypto assets.

For example, Rule 204-2(b) under the Advisers Act requires RIAs requires RIAs who maintain custody of client securities and assets to maintain certain specified records for each client, including:

1) journals showing securities transactions,
2) separate client ledgers,
3) copies of trade confirmations, and
4) records for each security held by the client showing amount and location.[38]

In addition, Rule 204-2(e) specifies that most required records, particularly those relating to client trades, must be maintained by an RIA for five years (in the RIA's principal office for at least the first two years; they may be kept in an easily accessible place for the balance of the five years). The blockchain meets these requirements—as a record, it is effectively eternal, accessible, and transparent, and we urge the Commission to recognize the use of blockchain in this manner.

Form PF and Form ADV Disclosure Requirements: Form PF requires the reporting of information relating to digital asset strategies[39] and digital asset exposures,[40] but does not define the term "digital asset." As discussed in further detail in our Response to Questions 1 through 6,[41] we urge the Commission to create and adopt a taxonomy for crypto assets and then decide which of those categories of crypto assets should constitute "digital assets" for the purposes of Form PF reporting.

In the context of Form PF, we would also urge the Commission to re-visit its instruction in Form PF's Glossary to "not include any digital assets in *cash* and *cash equivalents*." We think this is far too sweeping a prohibition. We recognize that stablecoins come in a number of different varieties and should not be subject to the same regulatory treatment, but at the same time, there may be circumstances under which a U.S. dollar-backed stablecoin or other similar crypto asset could be considered to be cash or a cash equivalent. This is, we respectfully submit, a determination best left to the RIA, subject to any further guidance around stablecoins that the Commission or Congress may provide.

---

[38] 17 CFR 275.204-2(a) and (b).
[39] Form PF Section 1c, Item B.25, https://www.sec.gov/files/formpf.pdf.
[40] *Id.*, Section 2, Item B.25.
[41] *See* Jennings, *supra* note 6.

Turning to Form ADV, we note that Item 8 of Part 2A of Form ADV, entitled "Methods of Analysis, Investment Strategies and Risk of Loss," requires an RIA, among other things, to explain the material risks: (1) associated with each "significant investment strategy or method of analysis" it uses—**in detail** if the investment strategy or method of analysis involves "significant or unusual risks"; and (2) involved if the adviser recommends "primarily a particular type of security"—**in detail** if the type of security involves "significant or unusual risks."[42] We offer no comment on these requirements, and we acknowledge that there may be crypto asset investment strategies that involve significant or unusual risks—as indeed there are for practically any class of asset. However, we would request the Commission to expressly clarify that the use of blockchain or crypto assets should not, by itself and in isolation, be considered a "significant or unusual risk" that merits detailed reporting for any investment strategy or asset.

Question 28: Can RIAs trade, stake, vote, or otherwise participate without moving crypto assets outside a qualified custodian? Should the Commission amend the existing RIA custody rule to provide an exception to allow RIAs to move client crypto assets temporarily out of qualified custodial arrangements to engage in staking, voting, or other novel participatory features of crypto assets? If so, should that exception be subject to time limits or other limitations or requirements?

Permitting RIAs to temporarily move crypto assets out of third-party custodial arrangements to exercise rights associated with those assets will allow RIAs to better honor their fiduciary duties to clients. Specifically, as mentioned above, RIAs have fiduciary duties to optimize client portfolios and make informed governance decisions for their investments. To quote the Commission, an investment adviser must consider "an investment product's or strategy's investment objectives, characteristics (including any special or unusual features), liquidity, risks and potential benefits, volatility, likely performance in a variety of market and economic conditions, time horizon, and cost of exit—to consider when determining whether a security or investment strategy involving a security or securities is in the best interest of the client."[43] The exercise of that fiduciary duty requires RIAs to serve the best interest of their clients and not to subordinate their clients' interest to their own. In the context of crypto assets, those considerations for an RIA must extend to the technological characteristics of these assets, and their associated rights, which may require temporary movement out of third-party custodial arrangements.

For that reason, in certain circumstances and for certain assets, the Commission should clarify the Custody Rule[44] to permit RIAs to temporarily move client crypto assets out of a qualified custodial arrangement in order to engage in trading, staking, voting, or other more novel participatory features of crypto assets. **Crypto Custody Principle 3** in **Annex A** adopts this position as a default rule. To be clear, this rule should permit—but not require—RIAs to stake, vote, or mandatorily exercise any right in connection with any crypto asset, and only in circumstances when the RIA deems these actions advisable and consistent with their client-contractual arrangements. As an alternative, RIAs should be allowed to

---

[42] Form ADV, Item 8 of Part 2A, https://www.sec.gov/about/forms/formadv-part2.pdf (emphasis added).
[43] *Id.* at 33674. *See also* Walker & Maitra, *supra* note 20.
[44] 17 CFR 275.206(4)-2.

contract with crypto custodians to permit such custodians to take any such commercially reasonable actions as may be required to exercise any right associated with an asset onchain.[45]

However, given that the Custody Rule is a vital safeguard for RIA clients, the Commission should place reasonable limitations on an RIA's ability to remove crypto asset securities out of third-party custodial arrangements, which we discuss below and in our **Crypto Custody Principle 3**. For example, the Commission should require that RIAs bear and make good on losses of assets that occur due to the negligence of the RIA when assets are out of third-party custody, when those losses could have been avoided had the assets remained in custody. We also support other reasonable limitations on RIAs and third party custodians, as applicable, including a duty to return any asset taken out of custody back to custody as soon and as securely as practicable.

These are the broad principles that underpin our approach to custody. However, it is equally important to acknowledge that the technology currently permits RIAs, in many circumstances, to trade, stake, vote, or otherwise participate without moving crypto assets outside a qualified custodian. In these cases, we support requiring RIAs or custodians to first reasonably determine whether such rights could be exercised without taking the asset out of custody (see **Annex A**: **Crypto Custody Principle 3**).

It may be helpful to illustrate the technological developments that allow crypto asset rights to be exercised without moving the asset out of custody with an example. One such prominent and relatively recent example is that of "User Interface Embedded Staking," which is sometimes also commonly called "point-and-click staking." In point-and-click staking, when the crypto asset is staked, an address called a "withdrawal address" is specified. This withdrawal address accesses and receives all the fees and rewards associated with the act of staking, and these actions are intermediated by a smart contract. When the staker seeks to exit from staking, withdrawal is triggered by a "validator key," which is distinct from the private key that possesses the assets. At no point does the staker "move" or relinquish control over the staked ether to any other entity. What the staker does share is its validator key—a key which can initiate or exit staking, but which cannot be used to otherwise move or dispose of the ether staked. In other words, at no point does the staker give up possession of the staked asset, or control over the staked asset to the withdrawal address. All that is shared, through the validator key, is the very limited right to withdraw from staking. And even where the validator key is used to withdraw from staking, the rewards received from staking accrue to the original staker.

Notably, there are already significant efforts underway to make greater use of point-and-click staking at an institutional level. Two SEC-registered national securities exchanges have filed proposals with the Commission to stake ether held by exchange-traded products, and have noted that point-and-click

---

[45] Commission Interpretation Regarding Standard of Conduct for Investment Advisers, Investment Advisers Act Release No. 5248, 84 Fed. Reg. 33669, 33671 (July 12, 2019), https://www.govinfo.gov/content/pkg/FR-2019-07-12/pdf/2019-12208.pdf.

staking does not involve moving the staked ether out of custody.[46] We acknowledge that it may not be universally possible to exercise crypto asset rights in every circumstance without moving the assets out of custody, but the technological trends in this direction demand that RIAs reasonably determine the extent to which movement out of custody is necessary for the exercise of any right. Our **Crypto Custody Principle 3** in **Annex A** incorporates this approach.

The Commission has proceeded against delegated staking services, and has not permitted exchange-traded products to stake their crypto assets. That unduly restrictive approach deprives crypto asset holders, including RIA clients, of significant value and interferes with their full enjoyment of the asset. That restrictive approach may potentially also harm those that are not allowed to stake if the network's mechanism for rewarding stakers includes new tokens entering the supply, so that as a result, holders that do not participate may have their assets diluted over time. As we discussed in our response to Question 4 of the Task Force's request for information, there are many reasons why delegated staking services should not implicate federal securities laws.[47] Further, even where they do implicate federal securities laws, prohibiting RIAs from utilizing such services is utterly at odds with the Commission's approach to other assets. The Commission does not prevent holders of common stock from collecting dividends, engaging in securities lending arrangements and repurchase agreements, or bondholders from receiving coupon payments. There is no good reason to treat crypto assets differently—if investors can validly hold an asset, they should also be permitted to exercise the full range of rights associated with that asset.

---

[46] Cboe BZX Exchange, Inc.; Notice of Filing of a Proposed Rule Change To Amend the 21Shares Core Ethereum ETF, Shares of Which Have Been Approved by the Commission To List and Trade on the Exchange Pursuant to BZX Rule 14.11(e)(4), 90 Fed. Reg. 10645, https://www.govinfo.gov/content/pkg/FR-2025-02-25/pdf/2025-03030.pdf; NYSE Arca, Inc.; Notice of Filing of Proposed Rule Change To Amend the Grayscale Ethereum Trust ETF and Grayscale Ethereum Mini Trust ETF To Permit Staking of the Ether Held by the Trusts, 90 Fed. Reg. 11081, https://www.govinfo.gov/content/pkg/FR-2025-03-03/pdf/2025-03336.pdf. As the Cboe filing notes, "Point-and-click staking involves an interface through which an entity can simply initiate staking by pointing and clicking on the ether assets to be staked. This process does not involve the staked ether leaving the wallet at which it is held, and accordingly reduces the risk of loss of ether through theft at the node while the asset is staked (although this process will not reduce the risk of loss of the ether through slashing)."

[47] *See* Jennings, *supra* note 6.

Question 29: What clarifications, if any, are needed in the Advisers Act regulations to address the cold or hot storage of crypto assets held in custody on behalf of a client?

        a. **What requirements, if any, should the Commission consider for the custody of crypto assets held in each type of wallet on behalf of a client? Should the requirements be the same for both types of wallets?**

        b. **How would a requirement to maintain custody of some or all crypto assets in either cold or hot storage affect an adviser's ability to transact in those crypto assets or otherwise implement its investment strategy?**

        c. **What means are available to mitigate the risks related to maintaining crypto assets in hot storage?**

General Requirements for Crypto Custody in Hot and Cold Wallets

    a) Wallet-Level Custody Requirements

The terms "hot storage" (online wallets) and "cold storage" (offline wallets) are commonly used by some to assess levels of security; however, we respectfully submit to the Commission that this distinction does not constitute a true dichotomy and these two concepts, in isolation, do not provide a complete framework for regulatory classification. These distinctions are imprecise because security in custody arrangements is dependent on much more than the online or offline state of a key management system. It is possible to design an online system that is meaningfully more secure than a poorly implemented offline system. Furthermore, the ability of an RIA to access investment strategies or opportunities may be hampered by requirements to keep a key management system offline. With sufficiently well-designed and well-managed risk mitigation systems, an online system can be as secure—or even more secure—than a less rigorously managed offline system. The core principle guiding custody should be risk-centric.

The three main categories of risks that the Commission should seek to mitigate are (1) the loss of keys and inability to recover funds, (2) the loss of funds due to insider risk or user error, and (3) the loss of funds to an external attacker. The first category of risks can be mitigated through proper disaster recovery controls at the organizational level. The second and third classes of risks can be mitigated through advanced security measures such as Multi-Party Computation (MPC), Hardware Security Modules (HSMs), multi-signature transaction controls, and other systems of cryptographic and programmatic checks and limits. We have suggested these risk mitigation measures in our description of safeguards in **Crypto Custody Principle 2** in **Annex A**. The key regulatory clarification should therefore focus on requiring custodians of crypto assets to establish a robust security architecture that adequately addresses each of these three primary categories of risk in specific detail.

Accordingly, we would strongly support the development of general principles requiring custodians (including RIAs who self-custody crypto assets) to establish specific safeguards at each major step of the "key management" process. In general, key management—the foundation of wallet security—can be divided into three areas, each of which has unique opportunities for exposure: (1) key

generation (creating cryptographic keys), (2) key storage (securing keys at rest), and (3) key usage (putting keys to work).[48]

b) Custody Requirements and Transaction Practices

In general, custody requirements should not impair transactional practices, provided RIAs have the ability to choose from multiple different custodial models and providers for their needs.

i) The solution for allowing a broad range of transacting parties to use and maintain crypto assets is to permit RIAs to choose from multiple custodial arrangements that do not compromise on the core custodial safeguards and principles that we outline here and in our **Crypto Custody Principles** in **Annex A**. For example:

    (1) Well-resourced private equity or venture capital ("PE/VC") RIAs may be best placed to undertake self-custody of crypto assets as long as such self-custody is materially as secure as the use of a third-party custodian and adheres to the **Crypto Custody Principles** we discuss in **Annex A**.

    (2) RIAs with greater resource constraints may find it useful to license or use technology providers as a substitute for certain processes instead of creating their own self-custody solutions from the ground-up.

    (3) RIAs for trading firms are likely to be able to rely on robust custodial solutions offered by centralized crypto exchanges.

ii) Custodial needs and transactional practices are likely to vary across RIAs depending on their business model, and the specific types of vehicles the RIAs advise.

    (1) RIAs to PE/VC funds typically advise pooled investment vehicles that have an investment model that can span several years. For this same reason (i.e., their long-term investment model), RIAs to PE/VC funds may invest even in crypto assets that appear to lack a ready or liquid secondary market. As a result, such RIAs may not find custodians who are willing or able to custody the specific crypto assets that such RIAs seek to hold for their clients. For this reason, and as we discuss in our **Crypto Custody Principles** in **Annex A**, self-custody under limited circumstances is likely to be necessary for many RIAs.

    (2) By contrast, "hedge fund" or RIAs that advise high-turnover portfolio trading strategies will likely need a custodial model that is swift and flexible, and permits crypto assets to be moved in and out of custody with minimum obstruction.

        (a) Such trading firms will likely need to keep their assets with the custodian associated with a crypto exchange, so that assets can be traded when required.

---

[48] Nassim Eddequiouaq & Riyaz Faizullabhoy, *Wallet Security: The Non-Custodial Fallacy*, a16z crypto (Oct. 14, 2022), https://a16zcrypto.com/posts/article/wallet-security-non-custodial-fallacy/.

iii) The Commission should therefore consider identifying a broad set of custodial principles, along the lines identified in **Annex A**, and then permit market forces to generate a range of custodial solutions. RIAs will find their favored solution at various points on the continuum.

c) **Mitigating the Risks of "Hot" Storage**

Although, all other things being equal, there are greater risks in an online ("hot") system, there are mitigations that can together make such a system more secure than some airgapped or offline ("cold") systems. In the context of blockchains, these mitigations can be "onchain" or "offchain"—that is, risk mitigation logic could be enforced by a smart contract (onchain) or by a separate custodian-controlled system (offchain). Not all of these measures are needed for an online system to be secure, nor is this list intended to be exhaustive of all possible mitigations. These are simply illustrative of modern techniques that may be useful in mitigating the risks of an online system.

i) **Key Isolation and Distribution**: even when keys are online, they can be geographically and logically isolated in order to decrease the likelihood that any vulnerability leads to the exploitation of the entire system.

ii) **Hardware Security Modules (HSMs)**: storing keys in secure, tamper-resistant hardware isolates them from threats. These devices can be configured to recognize and enforce transaction authorization policies, preventing the approval of malicious transactions, and ensuring that approvers of transactions can correctly scrutinize exactly what is being authorized.

iii) **Multi-signature wallets**: require the cryptographic coordination of multiple independent keys in the construction of a complete transaction. This can be achieved using offchain advanced cryptographic methods (e.g., secure multiparty computation or threshold signature schemes) or onchain enforced by smart contract logic (e.g., "multisig wallets"). This approach means no single stored key can be compromised to create malicious transactions.

iv) **Role-based transaction authorization policies**: define explicit, auditable administrative rules about who can initiate, authorize, or approve various categories of transactions—including conditions under which transactions may occur (e.g., rate limits, whitelists).

v) **Rate limiting and thresholds**: limit withdrawals (either through offchain or onchain systems) per day in order to reduce loss and allow custodians to regain control of compromised systems.

vi) **Whitelisting and address verification**: restrict transfers to addresses approved through separate processes, or addresses verified as being under the control of known counterparties.

vii)   **Multifactor authentication**: require multiple independent verification methods (e.g., passwords, TOTP codes, hardware authentication devices, or biometrics) to authenticate users initiating or approving transactions.

Safeguards like these can enable an online system to be as secure—or even more secure—than a less rigorously managed offline system.

III.   <u>Conclusion</u>

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

Respectfully submitted on behalf of A.H. Capital Management, L.L.C.,

Scott Walker, Chief Compliance Officer
a16z

Jai Ramaswamy, Chief Legal Officer
a16z

Miles Jennings, Head of Policy & General Counsel
a16z crypto

Michele R. Korver, Head of Regulatory
a16z crypto

ANNEX A

CRYPTO CUSTODY PRINCIPLES

Our approach in this Annex A is to identify the broad principles that should govern custody of crypto assets by RIAs. We agree with the fundamental aims underlying the Investment Advisers Act's (the "Advisers Act") Custody Rule, namely security, periodic disclosure and independent verification.

In this Annex A, we focus on how these aims can be operationalized in the context of crypto assets. More specifically, we discuss:

- The legal status of third-party crypto custodians (hereinafter "**Crypto Custodians**").
- The internal controls of Crypto Custodians.
- The circumstances and conditions under which self-custody should be permitted.

A note on scope: Our aim is not to expand the Custody Rule to include crypto assets that are not securities. These principles apply to crypto assets that are securities and set forth standards by which fiduciary duties are satisfied for other crypto asset types. We urge the Commission to require RIAs to ensure that crypto assets that are not securities are maintained under conditions that are substantially similar, and substantially as secure as the conditions for custody of crypto assets that we outline below. RIAs should document custodial practices for both crypto asset securities and crypto assets that are not securities, and should explain in writing any reason for any material discrepancy between custodial practices for different types of assets.

Principle 1: Legal Status Should Not Determine a Crypto Custodian's Eligibility.

- Legal status, and the protections associated with a specific legal status are important for a custodian's customers. For example, banks and broker-dealers are subject to custodial regulations that provide significant protections to their customers.
- However, registration under a particular category should not be the sole determinant of whether an entity is eligible to custody crypto assets. The Custody Rule's "qualified custodian" category should be expanded in the crypto context to also include at least:
    o State-chartered trust companies which effectively meet the definition of a "bank" under the Advisers Act.
    o Any entity registered pursuant to any rules and regulations promulgated under federal market structure legislation relating to crypto assets (hereinafter "**Crypto Market Structure**").
    o Any other entity, regardless of state or federal registration status, that can show, by means of a legal opinion or otherwise, that:
        ▪ the custodial contract offers the same protective terms and mechanisms as a bank, broker-dealer, or other similar entities under Crypto Market Structure;

- crypto assets in its custody would receive substantially similar treatment in the event of its bankruptcy as crypto assets custodied by a bank, broker-dealer, or other similar entities under Crypto Market Structure;
- it has the capability to provide account statements that satisfy reporting and audit standards; and
- that the entity is subject to regulatory supervision and examination of a competent regulatory body.

Principle 2: Crypto Custodians Should Establish Appropriate Protections.

- Irrespective of the specific technological tools adopted, Crypto Custodians should adopt certain optimal protections around the custody of crypto assets, including:
  - **Division of Powers**: No Crypto Custodian should be able to transfer a crypto asset out of custody without the cooperation of the RIA (e.g., by signing a transaction, device-based authentication, or instruction). No RIA should be able to transfer a crypto asset out of third-party custody without the cooperation of the Crypto Custodian.
  - **Segregation**: No Crypto Custodian other than a registered broker-dealer should commingle any asset held for an RIA with any assets held for any other entity. A registered broker-dealer may, however, hold assets for more than one RIA in a single omnibus wallet, provided it maintains a current record of ownership of such assets at all times, and promptly discloses the fact of such commingling to the relevant RIAs.
  - **Provenance of Custodial Hardware**: Every Crypto Custodian should have reasonable procedures to ensure it does not make use of any custodial hardware or other tools whose provenance raises security risks, or any concerns regarding risk of compromise. Crypto Custodians must confirm such provenance on an annual basis, and such provenance must also be the subject of an annual SOC2 Type 2 audit.
  - **Audit**: Each Crypto Custodian should undergo financial controls and technical audits no less than annually. Such audits should include:
    - Financial Controls Audits by a PCAOB-registered auditor:
      - a SOC 1 audit;
      - a SOC 2 audit;
      - the recognition, measurement, and presentation of crypto assets from a holder perspective;
    - Technical Audits:
      - ISO certifications (specifically ISO 27001);
      - a penetration test ("pen test"); and
      - tests of disaster recovery procedures and business continuity planning.
  - **Insurance**: Each Crypto Custodian should obtain and maintain adequate insurance coverage from an established insurer (including, for the clarification of doubt, through "umbrella" coverage), or, if insurance is unavailable, should establish an adequate insurance reserve, or optionally, reserves in combination with insurance.
  - **Disclosure**: Every Crypto Custodian must provide the RIA, at least on an annual basis, with a list of the principal risks associated with its custody of crypto assets and its

relevant written supervisory procedures and internal controls that mitigate such risks. Every Crypto Custodian must assess, at least on a quarterly basis, the risks associated with its custody of crypto assets, and determine whether updates to the disclosure are warranted.

o **Location of Custody**: No Crypto Custodian should custody any crypto asset in any location where the Crypto Custodian is aware that the law of that locale includes an insolvency/bankruptcy regime that considers custodied assets to be part of the bankruptcy estate in the event of the custodian's bankruptcy.

● We would suggest that custodians ideally implement the following processes at each stage:

o **The preparatory process for custody:**
  ▪ Custodians must review and evaluate the asset to be custodied, including the key generation process and transaction signing procedures.
  ▪ If the asset is supported by an open-source wallet or open-source software, custodians must review such wallet or other software for vulnerabilities and consider any modifications required for secure custody.
  ▪ Custodians must consider the provenance of each piece of hardware and software to be used in the key management process, and discard any infrastructure whose provenance is doubtful or exposed to material risk and security analysis is not feasible (e.g., it is closed source or too complex).

o **Key generation:**
  ▪ Encryption should be used at all levels of the key generation process, and multiple encrypted keys should be required in order to generate one or more private keys.
  ▪ Key generation processes should be both "horizontal" (i.e., multiple encryption key holders at the same level), as well as "vertical" (i.e., multiple levels of encryption).
  ▪ Quorum requirements should also require the physical presence of the authenticators, and any physical location in which quorum is met must be secured and monitored against interference.

o **Key storage:**
  ▪ Keys should never be stored in plaintext, only in encrypted form.
  ▪ Key copies must be physically separated (e.g., geographic locations, different individuals with access).
  ▪ Hardware security modules or equivalent, if used to maintain key copies, must meet U.S. Federal Information Processing Standard ("FIPS") security ratings.
  ▪ Rigorous physical isolation and authorization measures should be put in place to ensure airgapping. These measures can include the use of Faraday cages (shields that block wireless signals), biometrics access (like fingerprint or iris scanners), motion sensors (to trip alarms in case of unauthorized use), and SCIFs, or

Sensitive Compartmented Information Facilities (special areas for processing classified information).
- ▪ A secure wallet should never allow keys to be exported without authentication and appropriate safeguards, and exports should be encrypted.
- ▪ Redundancy of at least two levels of encryption should be maintained by a Custodian such that they are able to maintain operations in the event of natural disasters, power outages, or the destruction of property.
  - ○ However, institutional custody providers must maintain multiple, redundant storage locations and geographically distributed backup sites for encrypted keys.
  - ○ Any unencrypted key copies must be immediately destroyed.
  - ○ Custodians should maintain at least two layers of redundancy to maintain operations in the event of natural disasters, power outages, or the destruction of property.

- o **Key usage**:
  - ▪ Wallets should require authentication. In other words, they should verify that users are who they say they are, and that only authorized parties can access the wallet's contents. The most common safeguards are PIN codes or passphrases. More advanced forms of authentication can include biometrics or public key encryption-based approvals, such as cryptographic signatures from multiple secured devices.
  - ▪ Wallets should use well-established open source cryptography libraries (a "cryptography library" is a collection of pre-built components and tools that provide developers with cryptographic algorithms and functions for secure data handling, like encryption, decryption, and digital signatures, without requiring them to implement complex algorithms from scratch).
  - ▪ Another best practice is avoiding reuse of a key for more than a single purpose. Separate keys should be kept for encryption and signing, for example. This follows the principle of "least privilege" in case of compromise, meaning that access to any asset, information, or operation should be restricted only to the parties or code that absolutely require it for the system to work.

Principle 3: Crypto Custody Rules Should Permit RIAs to Exercise Economic or Governance Rights Associated With Custodied Crypto Assets.

- ● As a default rule and absent contrary client instructions, RIAs should be able to exercise economic or governance rights associated with custodied crypto assets, absent a compelling justification to the contrary. These economic and governance rights include staking, yield farming, voting, and any other right that is inherent in the asset.
- ● Absent a contractual agreement to the contrary, a Crypto Custodian should comply, where it is technologically feasible, with an RIA's reasonable request to exercise economic or governance rights associated with custodied crypto assets.

- A Crypto Custodian's transfer of an asset in connection with the exercise of an economic or governance right shall not be considered to be a transfer out of custody if the asset is moved to self-custody by any RIA in accordance with Principle 5 below.
- A Crypto Custodian's transfer of an asset in connection with the exercise of an economic or governance right shall not be considered to be a transfer out of custody if the asset is deployed to any non-custodial protocol or smart contract.
- A Crypto Custodian shall be permitted to take any such commercially reasonable actions as may be required to exercise any right associated with an asset onchain. This includes, but is not limited, to the explicit right to delegate any crypto asset to a wallet of the RIA in order to give effect to any right associated with an asset.
- Before taking any crypto asset out of custody in order to exercise a right associated with that asset, an RIA or custodian, as applicable, must first reasonably determine, in writing, whether such rights could be exercised without taking the asset out of custody.
- Unless the asset was in the custody of the RIA during the exercise of an economic or governance right, Crypto Custodians shall remain liable for any loss of the asset in connection with the exercise of an economic or governance right when such loss is the result of the Crypto Custodian's negligence.

Principle 4: Crypto Custody Rules Should be Flexible to Permit Best Execution.

- In general, RIAs are subject to a duty of best execution with respect to crypto assets.
- Pursuant to this duty of best execution, RIAs may transfer an asset to a crypto trading platform in order to secure best execution for that asset, provided:
  - o The RIA has taken such steps as are required to reasonably assure itself as to the resilience and security of the trading venue; or
  - o The RIA has transferred the crypto asset to a Crypto Market Structure regulated entity.
- No transfer by an RIA of a crypto asset to a trading platform to secure best execution for that asset should be considered to be a withdrawal from custody, provided:
  - o The transfer of the crypto asset to such venue is advisable in order to receive best execution;
  - o The RIA has reasonably determined, in its discretion, that the venue is suitable for best execution; and
  - o If the trade cannot be duly executed at the venue, the asset is promptly returned to custody with the Crypto Custodian.

Principle 5: RIAs Should be Permitted to Self-Custody Under Specified Circumstances.

- While the use of a Crypto Custodian should remain the default option for crypto assets, it should not be the exclusive custodial approach for RIAs.
- An RIA should be permitted to self-custody crypto assets if the RIA determines in writing, after reasonable examination, that:
  - o There is no Crypto Custodian reasonably available to take custody of the crypto asset; or

- o The RIA's own custodial arrangements are at least as protective as that of the Crypto Custodians reasonably available to take custody of the crypto asset; or
- o Self-custody is commercially reasonable in order to optimally exercise any economic or governance rights associated with the crypto asset.
- Where an RIA decides to self-custody a crypto asset for one of the three reasons identified above, the RIA must on an annual basis confirm in writing that the circumstances justifying self-custody remain unaltered.
- Where an RIA decides to self-custody a crypto asset, it should endeavor, to the extent reasonably feasible, to put in place the protections that would exist if the asset had been custodied by a Crypto Custodian.
  - At a minimum, and without prejudice to the generality of the foregoing, any RIA that undertakes self-custody must ensure that any crypto asset that is self-custodied is subject to at least the audit requirement, provided such audit confirms in writing that the assets so self-custodied are duly segregated (from the assets of the RIA) and adequately secure.