DISCUSSION DRAFT

Custody Rule Modernization:
A Model Framework for Crypto Asset Safeguarding[1]

Date: December 19, 2025

By: Sarah Helena Brennan[2] & Jay Stolkin[3]

On September 4, 2025, the U.S. Securities and Exchange Commission (the "***SEC***" or the "***Commission***") announced potential topics for upcoming rulemaking.[4] The Agency Rule List includes, among other things, improving and modernizing regulations governing how registered investment advisers ("***RIAs***" or "***Advisers***") custody and safeguard client assets, including crypto assets.[5]

In connection with this announcement, this Whitepaper is being submitted to help lay the groundwork for modernizing Rule 206(4)-2 (the "***Custody Rule***")[6] under the Investment Advisers Act of 1940, as amended (the "***Act***"). More specifically, this paper (i) discusses the challenges and impracticalities associated with applying certain requirements of the Custody Rule to crypto assets; (ii) advocates for a risk-aligned approach that utilizes a reasonableness standard to provide Advisers, among other things, the *option* to manage client crypto assets outside of "qualified custodians" ("***QCs***"),[7] utilizing secure non-QC safeguarding solutions; and (iii) details, in the first column of Exhibit A, a framework non-QC safeguarding program (the "***Framework***") that is informed by prevailing market practices and which, in our view, satisfies the policy objectives underpinning the Custody Rule at least as effectively as mandated third-party qualified custody.

- Section I of this Whitepaper provides a brief introduction to the Framework.
- Section II discusses the Custody Rule and its underlying policy objectives and core tenets.

---

[1] The authors would like to thank all of those who reviewed and contributed to this Whitepaper, including Daniel Leonardo, Larry Florio, Greg Xethalis and Drew Henderson.

[2] Sarah Helena Brennan is the General Counsel of Delphi Ventures, a thesis-driven, high-conviction investment firm that allocates across core themes it believes will dramatically shape the world.

[3] Jay Stolkin is the Deputy General Counsel of Multicoin Capital Management, LLC. Multicoin Capital Management, LLC is an SEC-registered investment adviser to private funds that make long-term, high-conviction investments in category-defining crypto companies and protocols across public and private markets, on behalf of sophisticated and institutional investors.

[4] Statement on the Spring 2025 Regulatory Agenda, Paul S. Atkins (Sept. 4, 2025), *available at* https://www.sec.gov/newsroom/speeches-statements/atkins-2025-regulatory-agenda-090425.

[5] To the extent a crypto asset is not a security and does not constitute "funds", the Custody Rule is inapplicable. However, until the parameters of the SEC's jurisdiction over crypto assets are more clearly defined, RIAs need clarity with respect to their safeguarding obligations. Additionally, non-QC safeguarding solutions such as those described in the Framework constitute sound practices for crypto asset management regardless of whether the Custody Rule applies. This Whitepaper does not address certain obligations under the Act applicable to Advisers to registered investment companies.

[6] 17 CFR § 275.206(4)-2 - Custody of Funds or Securities of Clients by Investment Advisers, *available at* https://www.law.cornell.edu/cfr/text/17/275.206(4)-2.

[7] As defined in the Custody Rule, "qualified custodian" means (i) a bank or savings association that has deposits insured by the Federal Deposit Insurance Corporation, (ii) a broker-dealer, (iii) a futures commission merchant, and (iv) a foreign financial institution that customarily holds financial assets for its customers, in each case subject to additional qualification. See also FN 24, discussing the treatment of state trust crypto custodians as "banks" for the purposes of QC status. In this Whitepaper, references to "QCs" include references to the types of state trust custodians permitted to serve as QCs under the Crypto Custody NAL (as defined and discussed in Section II.B below).

- Section III addresses challenges arising from applying the Custody Rule to client crypto assets and how rulemaking that enables optionality in safeguarding practices can resolve or mitigate such challenges.
- Exhibit A contains the Framework, including analysis and explanations as to how it addresses the Custody Rule's core tenets and policy objectives.

I. Introduction to Framework

Safeguarding client assets without relying on QCs is a practical necessity for Advisers operating in the crypto space. QCs are not available for all assets, cannot permit all uses of assets, and do not easily integrate with all aspects of crypto market structure. As a result, this Whitepaper proposes amending the Custody Rule to grant Advisers the *option* to safeguard client crypto assets under a reasonableness standard, using non-QC safeguarding solutions, such as those described in the Framework. The Commission could provide this optionality in the upcoming rulemaking by amending Section (a) of the Custody Rule to permit Advisers to maintain client funds and securities with a QC *and/or* utilizing non-QC safeguarding solutions with parameters tailored to ensure client crypto assets subject to the Custody Rule are (i) maintained and managed in a manner that adheres to the Adviser's fiduciary duties; and (ii) reasonably safe from loss, theft, destruction, misappropriation, and the financial reverses of the Adviser. Contemporaneously with any such amendment, the Commission could also issue guidance outlining indicative measures Advisers may take to meet this reasonability requirement, such as those described in the Framework.[8]

The Framework draws on prevailing best practices deployed by sophisticated Advisers in the market to safeguard client crypto assets that are not secured with a QC. In sum, the Framework outlines a non-QC safeguarding program that utilizes multi-signature or multi-party computation technology (together "***MS/MPC***")[9] and model operating procedures to securely manage client crypto assets without granting any single party control, thereby mitigating the risk of fraud and mismanagement. In this structure:

1. **MS/MPC Key Management**: Client crypto assets are secured using third-party MS/MPC solutions that distribute control over one or more private keys (or key shards) among multiple

[8] The Framework is merely one representative example of non-QC crypto asset safeguarding practices that could satisfy such a reasonableness standard. This paper does not suggest that an Adviser could not satisfy the reasonableness standard through means other than the measures and protections outlined in the Framework. Advisers would be responsible for designing their own safeguarding practices in consideration of their duties to clients and SEC guidance.

[9] A traditional crypto asset key management solution relies on a single public-private cryptographic key pair, whereby a single private key may sign transactions relating to, and authorize movements of, assets associated with a public key address. In a typical *multi-signature* structure, a public key address is designed (either through native blockchain script or a smart contract) to be associated with a defined number of private keys, with a threshold sub-set of such defined number (*i.e.*, M of N, as described in FN 11 below), required to sign transactions to authorize moving assets associated with the multi-signature vault. In a *multi-party computation* solution, private key material associated with a public key address is divided and shared among multiple parties such that a threshold sub-set of those parties may collectively construct and sign a transaction to authorize movements of assets associated with the public key address. Our Framework solution is intended to be inclusive of institutional grade multi-signature, multi-party computation and other similar or future key management solutions that similarly divide control of transaction authorization and operate consistent with best practices in the custody and management of private keys and/or crypto assets. It also represents an example implementation that should be updated as technology and best practices evolve. This approach preserves optionality as new technologies come to market. It should also be noted that not all MS/MPC technology is created equal. Advisers would be responsible for exercising diligence in selecting the software providers they engage.

trusted parties (*e.g.*, Adviser personnel or other agents of a client)[10], with defined thresholds[11] of such parties being required to "sign" transactions to authorize asset movements. Under this construct, no single party can unilaterally access or transfer client assets, ensuring that no individual can unilaterally misappropriate the same.

2. **MPA Contract Wrap or Policy Set**:[12] The Adviser and/or client (in this context, the "***MPA Sponsor***")[13] would institute internal policies and/or enter into a written legal contract (an "***MPA***") with the designated MS/MPC signers (each, a "***Signer***"), who are appointed by the MPA Sponsor in a fiduciary capacity with the client as beneficiary. Key aspects of the MPA are as follows:
    a. The MPA provides that Signers act at the direction of the MPA Sponsor in safeguarding client assets and in accordance with the operational and security standards established in the MPA. The role of a Signer is administrative, not discretionary. Signers execute in accordance with authorized instructions, absent manifest evidence of fraud or misappropriation, and bear contractual and legal liability only for willful misconduct, collusion, or gross negligence, as defined and limited by the standards of conduct set forth in the applicable MPA. The MPA provides that a Signer may rely on the authenticity of MPA Sponsor instructions absent manifest evidence of fraud or misappropriation, and that a Signer should be indemnified by the Adviser with standard exceptions for fraud, willful misconduct, gross negligence, etc.
    b. The MPA contractually confirms, consistent with the Custody Rule, that client assets and Adviser assets should not be commingled, and that title to the assets in the MS/MPC solution remains with the client, thereby reducing uncertainty of asset ownership in insolvency proceedings. The MPA Sponsor can direct the Signers to act on behalf of the client but neither the Adviser nor the Signers can claim legal ownership of the assets.
    c. The MPA outlines procedures for changing Signers and MS/MPC keys to ensure orderly transition, including in the event of a change or termination of a Signer or the Adviser.
    d. The proposed solution, as governed by the MPA, eliminates single points of failure by imposing operating procedures to validate instructions from Adviser personnel to the Signers and builds upon the multisignature design (M of N), which itself operationally limits the ability of any individual Signer to exert control or defect.
3. **Operational Security Standards**: Advisers and Signers are required to adhere to operating procedures and internal controls designed to ensure security and safety of client assets. These include access governance and authorization controls for Signers (who can initiate or approve transactions, with appropriate checks and balances); key lifecycle management and backup

[10] To be clear, the solution proposed herein does not necessarily require that the key holders are exclusively Adviser personnel. MPA Sponsors (as defined herein) should retain optionality that Signers (as defined herein) and/or other holders of role-based access control could be third-party service providers under contractual obligation. Additionally, under the approach proposed herein, the Custody Rule's internal controls report requirement should not apply, because the program does not involve utilizing an affiliated QC, but involves leveraging third-party software solutions.

[11] Often referred to as "M of N" where N represents the total number of Signers, and M represents the minimum number of Signers needed to execute a transaction. M of N solutions can be flexibly designed for policies on the number or identities of required Signers for specified transactions.

[12] The authors discussed at length with various commenters whether a contractual wrap or an internal policy set (or a combination of the two) is best suited to accomplish the objectives of the MPA, as outlined herein. Based on those conversations, the authors believe either approach, or a combination of the two (*e.g.*, a contract that refers to and/or incorporates certain internal policies) could achieve the goals of the MPA, as described in this section, and that Advisers should be responsible for determining the approach best suited to their specific needs. Note that, to the extent an Adviser utilizes a third-party Signer, a binding contractual MPA would be necessary.

[13] The MPA Sponsor is responsible for administering the non-QC safeguarding solution.

procedures; transaction verification thresholds (*e.g.*, M of N); and processes and procedures for change in management, incident response, business continuity, data security, hardware isolation (*i.e.,* airgapping and/or the use of hardware security modules), and review for updates against threat vectors.

4. **Independent Verification Bolstered by Enhanced Transparency**: Advisers remain subject to independent verification or audit requirements, consistent with the Custody Rule.[14] The approach proposed in the Framework enhances these verification protections by (i) enabling transparent, continuous tracking and monitoring of asset holdings and real-time detection of problematic activity, rather than relying on independent examinations or audits that reveal issues months later when transactions are reviewed in arrears; and (ii) distributing the authority to move assets across multiple Signers.

II. The Custody Rule - Policy Justifications, Core Tenets & Need for Modernization

A. Policy Objectives & Core Tenets.

The Custody Rule was initially adopted in 1962, after Congress amended the Act to grant the SEC rulemaking and inspection authority under the Act's anti-fraud provisions – a response to reports of rampant fraud and embezzlement of client assets by investment advisers.

The policy goals underlying the Custody Rule are laudable, generally unobjectionable and have remained largely static since the rule's initial adoption more than 60 years ago. In short, the rule aims to protect client assets from being lost, misused, misappropriated and/or subject to an Adviser's financial reverses, such as insolvency.[15]

The Custody Rule aims to achieve this policy objective through a number of core tenets (the "***Custody Core Tenets***"):[16]

1. *Safeguarding*. Client funds and securities must be kept safe from theft, loss misappropriation and Adviser financial reverses;
2. *Segregation*. Client funds and securities must be segregated from Adviser assets;
3. *Client Notifications*. Clients must be informed and notified of custodial relationships and modifications thereto;
4. *Account Statements*. Clients must receive (or, in certain instances, the Adviser must have a reasonable basis for believing clients receive) account statements and/or audited financials; and,
5. *Independent Verification*. Client funds and securities maintained by an Adviser must be subject to verification by an independent public accountant.

---

[14] Within the Custody Rule, particularly for private funds, the audit serves as the primary safeguard against malfeasance, and this paper does not suggest changing that framework. If an Adviser misappropriates client assets—which is always a risk—the audit is generally the mechanism by which such misconduct is ultimately identified. Utilizing QCs does not, in and of itself, prevent Advisers from misappropriating funds, as QCs take direction from Advisers when it comes to moving assets.

[15] *See e.g.*, 17 CFR Parts 275 and 279, Release No. IA-2176; File No. S7-28-02, RIN 3235-AH 26, *Custody of Funds or Securities of Clients by Investment Advisers*, U.S. Securities and Exchange Commission, *available at* https://www.sec.gov/files/rules/final/ia-2176.htm.

[16] *See,* Custody Rule, Sections (a)(2) (Notice), (a)(3) (Statements), and (a)(4) (Independent Verification).

Note that, with respect to private fund clients, under Section (b)(4) of the Custody Rule, Advisers may satisfy the Custody Core Tenets outlined in items 3-5 above by undergoing annual (and liquidation) audits by Public Company Accounting Oversight Board ("***PCAOB***") registered and inspected independent public accountants and subsequent distribution to limited partners of audited financials (the "***Audit Exception***"). The Audit Exception would remain applicable under the revised Custody Rule and in the context of non-QC safeguarding solutions, such as the Framework.[17] As noted below, non-QC safeguarding solutions improve upon the risk mitigating effects of independent verifications and audits by enabling real-time transparency into wallet balances, continuous auditability and reconciliation, and automatic transaction notifications.

While the Custody Rule has been amended several times to modify the manners in which the Custody Core Tenets are implemented and enforced, the tenets themselves have been largely steadfast since 1962. The model outlined by this paper remains true to the Custody Core Tenets (and the Custody Rule's policy objectives), but provides a new approach to their implementation. Thus, Exhibit A maps the Framework's components to their corresponding Custody Core Tenets.

B. Short Procedural History.

Historically, the Custody Rule has been rooted in a reasonableness standard and the SEC has been measured in amending the rule, typically modernizing to reflect market developments and conform to best practices already pervasive among Advisers in the market.

For instance, from 1962 until 2003, the Custody Rule required that Advisers custody client funds and securities "in some place *reasonably* free from risk of destruction or other loss".[18] In 2003, the SEC amended the rule to require that client funds and securities be kept with QCs (rather than merely safekept).[19]

In proposing this amendment, the SEC indicated the QC requirement was meant simply to memorialize existing market best practices. In other words, the SEC was not straying from the Custody Core Tenet of ensuring client assets are safeguarded. Rather, it was modifying the implementation of that tenet to match then prevailing practices. The proposed rule underpinning the 2003 amendments stated:

> "*Almost all advisers that have custody of client securities maintain them in accounts with a broker or a bank, but on occasion our examiners discover an adviser keeping [stock] certificates in office files or a safety deposit box. Such custodial practices do not provide adequate protection for client securities, because these certificates may be too easily lost, stolen or destroyed*."[20]

This statement suggests that, in implementing the QC requirement, the Commission drew on Advisers' best practices to establish measured regulations that eliminated undesirable edge cases, without disrupting

---

[17] *See,* Custody Rule, Section (b)(4).
[18] U.S. Securities and Exchange Commission, *Custody of Funds or Securities of Clients by Investment Advisers; Final Rule*, Release No. IA-2176 (Sept. 25, 2003), *available at* (emphasis added).
[19] Final Rule: Custody of Funds or Securities of Clients by Investment Advisers; Release No. IA-2176 (Nov. 5, 2003), available at https://www.sec.gov/files/rules/final/ia-2176.htm.
[20] Securities and Exchange Commission, Release No. IA–2176; File No. S7–28–02, *Custody of Funds or Securities of Clients by Investment Advisers* (Oct. 1, 2003), at 48582, *available at* https://www.govinfo.gov/content/pkg/FR-2003-10-01/pdf/03-24813.pdf.

good and pervasive market standards. Thus, in introducing the QC requirement, the Commission was not necessarily establishing intermediation as a core tenet or implying that intermediated custody is the only manner by which Advisers can safeguard client funds and securities in perpetuity. Rather, it was modifying the implementation of an existing Custody Core Tenet - safeguarding - to match market best practices for custodying the forms of funds and securities then typically managed.

The Custody Rule is again in need of modernization.[21] Technological developments have spurred the creation of all types of digitally produced and stored assets and altered how securities are typically issued and how their ownership is typically recorded, custodial practices have changed, and new asset classes that necessitate rethinking custody paradigms, such as crypto assets, have emerged. All the while, SEC guidance has not kept pace.

To the contrary, the previous administration doubled down on the legacy custody paradigm. By failing to modernize the rule to track technological developments, proposing an overbroad asset-agnostic expansion of the Custody Rule and QC mandate with its 2023 proposed rule on Safeguarding Advisory Client Assets (the "***Safeguarding Proposal***"),[22] and in instituting the *Galois* action,[23] the Commission, under prior leadership, signaled it believed custody requirements designed for physical stock certificates and fiat currencies remain fit for all purposes in 2025. This is not the case, and this approach ignores the intrinsic properties of new asset classes that make alternative safeguarding solutions not only viable, but cheaper and safer.

Fortunately, under current leadership, the Commission has signaled openness to exploring asset-specific safeguarding models and modernizing the Custody Rule.

For instance, the SEC withdrew the Safeguarding Proposal from consideration.[24] Further, in September of 2025, the SEC provided no action relief permitting Advisers to utilize state trust companies to safeguard client crypto assets, provided Advisers ensure these state trust custodians satisfy certain operational conditions (the "***Crypto Custody NAL***").[25] Though the market generally welcomed this relief, the Crypto Custody NAL still adheres to the third-party custody paradigm, which presumes intermediary

---

[21] Though amended in 2009, the 2009 amendments did not address the frictions created by digitally native assets. While this paper focuses on application of the Custody Rule to crypto assets, the proliferation of other forms of digital assets, including, without limitation, electronic stock certificates, tokenized securities, etc., also contribute to the need for Custody Rule modernization.

[22] Securities and Exchange Commission, 17 CFR Parts 275 and 279, Release No. IA-6240; File No. S7-04-23, *Safeguarding Advisory Client Assets* (Feb. 15, 2023), *available at* https://www.sec.gov/files/rules/proposed/2023/ia-6240.pdf

[23] In re: Galois Capital Management, LLC, Advisers Act, Release No. 6670 (Sept. 3, 2024), available at https://www.sec.gov/files/litigation/admin/2024/ia-6670.pdf. In citing the Galois action, this paper does not express an opinion on the specific practices of that particular Adviser, but highlights that the enforcement action, together with the contemporaneous sweep of Adviser crypto asset custody practices, expressed to the market the Commission's (prior) view that the Custody Rule's QC requirement was fit for crypto asset safeguarding.

[24] *See,* Securities and Exchange Commission, *Notice of Withdrawal of Proposed Regulatory Actions (June 12, 2025), available at https://www.sec.gov/files/rules/final/2025/33-11377.pdf*.

[25] Securities and Exchange Commission, *Response of the Office of Chief Counsel of Division of Investment Management*, (Sept. 30, 2025), *available at* https://www.sec.gov/rules-regulations/no-action-interpretive-exemptive-letters/division-investment-management-staff-no-action-interpretive-letters/simpsonthacherbartlett093025
(allowing state trust companies providing crypto asset custody services to be treated as a 'bank' for purposes of the custody rule contingent on meeting certain requirements for custody).

control is required to protect client assets against unauthorized access and loss – a presumption that does not hold true in practice.[26]

C. Updating the Custody Rule for the Digital Paradigm.

The proliferation of digital and crypto assets necessitates new options for safeguarding. It must be acknowledged that best safeguarding practices necessarily *should* vary across asset classes, and that one-size-fits-all regulation will not suffice. Crypto assets (whether or not they constitute securities) are digital, not physical and they are, by design, secured and controlled by public-private key cryptography.[27] Their core value proposition lies in enabling decentralized, peer-to-peer transactions. Regulation that forces Advisers to safeguard crypto assets *exclusively* through operationally constrained and expensive intermediaries introduces unnecessary concentration risk, fails to acknowledge the realities of 24/7 crypto markets, and undermines the technology's core purpose. Additionally, the Custody Rule does not impose affirmative standards of care on crypto QCs. While the Crypto Custody NAL requires that Advisers ensure state trust custodians meet certain operational standards and restrictions, the current Custody Rule is silent on the methodologies QCs must deploy to safeguard assets, which does not ensure uniformity or predictability in crypto asset safeguarding practices, or remove the need for substantive diligence by Advisers in selecting QCs.

Properly designed non-QC safeguarding solutions can, in many cases, enhance rather than diminish security, and they provide Advisers and clients with transparency and control in their safeguarding programs. Moreover, allowing optionality in safeguarding models would compel QCs to compete on product quality and innovation rather than rely on a regulatory monopoly, thereby encouraging a healthier market for consumers and continued advancement in security infrastructure.

The Commission itself has begun to acknowledge this reality. Commissioner Peirce's February 2025 Request for Input (the "***RFI***")[28] posed a series of thoughtful questions to solicit feedback from Advisers regarding best practices for safekeeping client crypto assets, including non-QC safeguarding models. This is a meaningful shift in regulatory posture. It represents recognition by the Commission that the unique characteristics of crypto assets require a reassessment of legacy custody assumptions and a willingness to consider alternative, technology-native models.

---

[26] It should also be acknowledged that the Crypto Custody NAL is intended to provide partial and interim relief while the Commission considers more robust modifications to the Custody Rule.

[27] For a basic explanation of public-private key cryptography, *see, e.g.*, *What are Public and Private Keys?*, Emily Ekshian (Aug. 26, 2022), Crypto Council for Innovation, *available at* https://cryptoforinnovation.org/what-are-public-and-private-keys/. It is important to note that crypto assets consist of digital entries or allocations to a public address on a distributed ledger. As a result, the concept of, "custody of crypto assets" differs fundamentally from custody of traditional, tangible assets. Custodians of crypto assets do not hold the crypto assets themselves, nor is the custodian required to participate in the operation or maintenance of the underlying distributed ledger. Rather, a custodian of crypto assets safeguards the private key material used to authorize transactions and authenticate control over the assets allocated to a public address. In this sense, crypto asset custody entails the safeguarding of cryptographic credentials as opposed to physically possessing or storing the crypto assets themselves. For a more thorough explanation of this distinction and its implications, *see, Comment to File No. S7-04-23* (May 8, 2023), Gregory E. Xethalis and Daniel A. Leonardo, Multicoin Capital, *available at https://www.sec.gov/comments/s7-04-23/s70423-188279-343502.pdf*.

[28] Commissioner Hester Peirce, *There Must Be Some Way Out of Here* (Feb. 21, 2025), *available at* https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125.

As the Commission progresses toward rulemaking, any SEC framework addressing crypto assets that are subject to the Custody Rule should be grounded in best practices for cryptographic asset security. This includes robust standards for operational security and fostering innovation and growth in the market for secure storage solutions.

III. The Custody Rule's Application to Crypto Assets & Need for Optionality/Flexibility

A. Mitigating Challenges Through Rulemaking.

Drafted for a world of intermediated financial instruments, the Custody Rule presumes that third-party custody best ensures client protection. Yet crypto assets—natively digital, cryptographically secured, and designed for direct control on distributed networks—do not fit neatly within that paradigm.[29]

Given the SEC's prior statements and enforcement posture, Advisers have been compelled to structure their safeguarding programs for crypto assets as though the Custody Rule applies, even when practical or legal uncertainties persist. This has created significant operational friction for market participants. In some cases, this has produced an impossible standard, as QCs may not support a given asset, and even where they do, they may not support features and functions integral to that asset's core value proposition. For example, Advisers may, by utilizing a QC for the sake of Custody Rule compliance, forgo opportunities to participate in network governance, stake assets, and engage in other activities that produce additional returns or otherwise optimize the value of client investments.

These challenges can be addressed through targeted rulemaking that embeds flexibility into the Custody Rule.

Specifically, rulemaking that is rooted in a reasonableness-based standard[30] and permits well-defined non-QC safeguarding solutions would resolve many of the persistent regulatory and structural market challenges of the current custody regime. Such flexibility would not supplant the QC model, but rather complement it. Flexibility provides Advisers the ability to select, on a position-by-position basis, the safeguarding method that is best aligned with its fiduciary duties, portfolio characteristics, operational security, client interests and contractual obligations. It also forms the best basis for regulatory harmonization across securities and commodities designations in this asset class.

A more flexible framework could facilitate regulatory harmonization across the federal regulatory frameworks by allowing each agency to evaluate custody outcomes empirically. Over time, data from parallel models, QC/third-party, MS/MPC/non-QC, or hybrid, could inform a unified, principles-based standard for safeguarding crypto (and other digital) assets. Thus, instituting a reasonableness standard that enables optionality converts the Custody Rule from a binary compliance chokepoint into an adaptable framework that replaces check-the-box compliance with dynamic standards for assessing and implementing substantively measured safekeeping protocols.

The discussion below provides a non-exhaustive list of issues arising from the Custody Rule's application to crypto assets and explains how granting optionality via rulemaking can mitigate or eliminate some of

[29] *See*, FN 27 for discussion of the custody paradigm as it applies to crypto assets.

[30] A "reasonableness standard" is a known concept under the Act, so adopting it here is not a departure from historical and/or existing SEC regulations. Reasonableness standards exist throughout the Act, SEC rules, and guidance — including in fiduciary duty guidance, compliance rules, the Custody Rule (e.g., Section (a)(3)), the advertising rule, the books-and-records rule, and beyond.

these risks, which arise largely from market structure and competition issues. Next, this paper addresses certain custodial risks rulemaking may not resolve, discusses the need for flexibility and the potential benefits of allowing the non-QC safeguarding technology market to evolve with a significant total addressable market.

i. *The Need for Optionality*.

The QC market for crypto assets remains in its early stages. Only a small number of providers offer custody across a limited set of assets,[31] and most do so at high cost with constrained functionality. These conditions stem from regulatory deterrents (*e.g.*, SAB 121), the novelty of the asset class, and high engineering costs associated with onboarding new protocols. Many of the issues described below are fully recognizable from a pure economics perspective given the stage of the market. As a result, mandating the use of QCs in this market environment—even conditionally, such as "only where available"—effectively entrenches a handful of incumbents, suppressing competition and innovation.

Alternatively, by granting Advisers and their clients optionality in safeguarding models, as proposed herein, the Commission can expand market capacity, and cultivate increased innovation and growth in the custody and safeguarding services market. This in turn will result in better, more robust, more affordable and more operationally secure product offerings, from QCs, MS/MPC software providers and, perhaps, other providers of safeguarding or safeguarding-related services or products, while still imposing effective regulatory guardrails.

The table below summarizes key structural frictions in the current custody market and outlines how an adaptive, technology-neutral rulemaking approach could mitigate each.

Market Pain Point	**Mitigation by Proposed Rulemaking with Optionality**
Limited Market Depth & Asset Coverage.	
Even among the few QCs[32] dedicated to providing crypto asset safeguarding solutions, support for assets is limited and onboarding new networks is slow and costly.	Dual pathways will increase aggregate market capacity. The number of assets supported by existing MS/MPC software solutions is more robust[36] than the list of assets supported by existing QCs.

[31] Further, it is unclear whether certain of the largest, most reputable and utilized crypto asset custodians constitute QCs under the Custody Rule, as these providers are typically structured as state trusts. By giving Advisers relief to use these state trust custodians, provided they meet certain criteria, the Crypto Custody NAL could be interpreted to suggest that such entities explicitly do not satisfy the current QC definition.

[32] *See*, FN 7 regarding the scope of the term "QC", as used in this Whitepaper.

[36] While formal studies with aggregated empirical data are sparse, this is generally supported by our experience and by market disclosures and developer documentation indicating that institutional facing multiparty computation (MPC wallet) providers support a broader range of digital assets than existing custodians. *See, e.g.*, Fireblocks Developer Portal, *List Supported Assets* (https://developers.fireblocks.com/docs/list-supported-assets-1) (visited Nov. 10, 2025) (reporting support for "thousands of assets across dozens of blockchains"); Squads https://squads.xyz/multisig; (Gnosis) Safe https://help.safe.global/en/articles/40795-supported-networks, Foredefi https://docs.fordefi.com/user-guide/manage-chains/supported-blockchains. By contrast, leading QCs publish more curated, limited lists reflecting regulatory and operational constraints. *See,* Coinbase Prime and Custody, *Supported Cryptocurrencies and Trading Pairs* (https://help.coinbase.com/en/prime/trading-and-funding/supported-cryptocurrencies-and-trading-pairs) (visited Nov. 10, 2025) (≈ 440 assets across 38 chains); BitGo Blog, *BitGo Reaches New Milestone: 80 of the Top 100 Digital Assets Now Supported* (https://www.bitgo.com/resources/blog/bitgo-reaches-new-milestone-80-of-the-top-100-digital-assets-now-supported/) (Feb. 25, 2025); Anchorage Digital Bank, *Supported Digital Assets*

Particularly in the months immediately following their launch, many crypto assets are not supported by any QC in the market. In other words, it may be the case that crypto assets acquired for client accounts *cannot* be held with a QC. This issue is not easily rectified, even with rulemaking. For a QC, adding support for a crypto asset requires robust technical and governance diligence, engineering work, and upfront expenditure. Thus, QCs are often reluctant to add support for new assets unless there exists market demand sufficient to rationalize the associated costs. For certain assets, there may never be enough demand to justify the expenditures necessary for a QC to add support. Additionally, once QC support for a new asset is established, the available solution may limit an Adviser's capacity to leverage key features of the asset in question, such as staking and/or governance participation.

This puts RIAs in the untenable position of deciding to (i) not invest in/hold crypto assets for which there is client demand and which may produce favorable returns or (ii) invest in/hold such assets pursuant to their investment mandates, while running the risk of technical Custody Rule violations – which can result and have resulted in deficiencies and enforcement actions. Many venture-style investments in the crypto space afford investors, in addition to equity or equity rights, rights to future tokens that may or may not ultimately be created and issued. If and when a project determines to create and issue a token, the token is unlikely to be supported by a QC at launch. Thus, investors must then decide whether to exercise their token rights and receive the tokens, potentially in violation of the Custody Rule,[33] or forgo their rights, and cede potential risk (which could, in and of itself, give rise to claims of fiduciary duty violations).[34] Thus, as noted by Commissioner Peirce, SEC custody regulation has been used as a chokepoint to prevent investment in crypto.[35]

This structural reality means Advisers will need accommodation through a regulatory option for non-QC safeguarding solutions when no third-party custodian is available. Absent such optionality, Advisers are forced to either forgo client opportunities altogether or risk technical noncompliance with the Custody Rule. Neither outcome serves investors, market efficiency, nor the policy goals underlying the rule.

MS/MPC software providers tend to be more asset-agnostic, which often enables faster and more cost-efficient support for new crypto and tokenized assets. Indeed, many leading MPC platforms claim support for dozens of blockchains and thousands of tokens. By contrast, many traditional QCs — especially non-crypto-native banks/trust companies — continue to face operational, regulatory and infrastructure constraints that can slow the addition of new assets and limit breadth of support.

Thus, optionality to utilize MS/MPC solutions to satisfy the Custody Rule will immediately reduce the number of crypto assets Advisers are unable to maintain.

Further, permitting non-QC safeguarding solutions such as the Framework will likely propel QCs to increase asset support or otherwise risk losing market share to other viable solutions. Providing optionality via rulemaking will generally lead to a healthier market for crypto asset custody.
Optionality in custody solutions will also reduce tensions between Custody Rule compliance and Adviser fiduciary duties, as Advisers will have guidance for compliantly safeguarding client crypto assets that are not QC-supported, meaning the lack of QC support for an asset will be less of a factor for investment decisions.

From a market structure perspective, the better policy approach is to foster competition—encouraging QCs to compete based on the quality and cost of their services, rather than regulatory capture.

Optionality will also yield a positive feedback cycle where broader investments are made in the R&D of the underlying security technology that is used across QCs and non-QC safeguarding solutions. Rulemaking that incorporates optionality levels the playing field between QC and non-QC custody models, creating incentives for all market participants to improve security, efficiency, and client outcomes.

(https://www.anchorage.com/who-we-serve/venture-capital-firms) (visited Nov. 10, 2025) (referencing 500+ assets for custody).

[33] This approach has the practical effect of making the SEC a merit regulator. Where a QC does not support a particular token, Advisers are effectively precluded from investing in it, notwithstanding the absence of any determination regarding the asset's risk profile or suitability. In this respect, the Custody Rule operates to constrain investment access in a manner not historically applied to other asset classes. As discussed further in Section III(A)(ii)(b) below, many protocol-native activities such as staking, governance participation, and other onchain activities require assets to be deployed to smart contracts such that custody in the traditional wallet-control sense ceases to be the relevant construct at all, which is why a reasonableness-based approach is necessary.

[34] Waiting for a QC to establish support before exercising a warrant or claiming tokens is generally an unfavorable option, as (i) sometimes token rights carry short exercise periods measured from the date of launch and (ii) tax treatment of token rights favors early exercise and possession to start the capital gains clock or lock in fair market value. These factors, together with the risk of non-delivery that arises from delay are strong incentives to exercising and taking possession as soon as possible.

[35] *See, e.g.,* Hester Peirce Outlines SEC Reforms to Bring Crypto Clarity, CRYPTONEWS (Dec. 6, 2024), available at https://cryptonews.com/news/hester-peirce-outlines-sec-reforms-to-bring-crypto-clarity/ (citing Commissioner Peirce as calling the ongoing regulatory crackdowns 'Operation Chokepoint 2.0,'" and urging the Commission to "cease blocking crypto's access to essential services like custody.").

Concentration Risk	
As noted above, only a handful of QCs offer meaningful crypto asset solutions. With an ever-growing number of Advisers investing in crypto assets, and a relatively stagnant number of "crypto native" QCs, concentration in crypto asset custody is an increasing concern. As assets under custody among a handful of QCs grows, the risk that these QCs and their users are targeted by hackers and bad actors grows as well. Additionally, the underlying technology used by QCs will, in many cases, be similar to that used in non-QC safeguarding solutions, but with additional concentration risk, posing a larger honey pot. High concentration creates single points of failure and introduces an increased threat of contagion in the market arising from a security breach or insolvency event. Absent additional rulemaking, RIAs have less assurance as to whether concentration risk is balanced out by heightened standards of care. With QCs, customers have little certainty over the availability of their assets in the case of bankruptcy. As an example, even though the terms of service dictated that customers retained title, the Prime Trust bankruptcy administrator claimed that because the assets were pooled, they became assets of the bankruptcy estate. *In the context of QCs that allow staking, even where the QC's terms of service provide assurances that title remains with the customer, the staking terms of service often preempt the base custody terms, leaving the Adviser's legal position uncertain in a bankruptcy.*	Permitting non-QC safeguarding solutions and increasing competition in the crypto asset custody market should reduce concentration concerns, as Advisers will have the option of spreading client assets across QC and non-QC options. By distributing assets across multiple solutions and reducing concentration, Advisers can temper the impact of a security breach or insolvency of a single third-party QC. Rulemaking can require standardization around what happens in the event of QC bankruptcy, such as mandating that title stays with the customer and asset segregation practices to bolster customer claims to their assets. It can also mandate increased transparency in terms of service around when customers are opting in/out of these protections.
Opaque Standards.	
Historically, a QC designation, absent additional guidelines, has not entailed any particular security standards for the crypto asset class. In fact, security standards and internal controls at QCs are, for one reason or another, including for operational security purposes, somewhat of a black box. While there is a patchwork of standards imposed by various regulatory bodies that may apply, the Custody Rule does not currently impose minimum standards. To date, the only operational security standards imposed by the Commission[37] with respect to crypto asset custody were established in the Crypto Custody NAL.[38] The Crypto Custody NAL established baseline requirements for certain custodians, by making the relief contingent on the following requirements: the custodian must maintain robust internal controls, including policies governing key management, access, reconciliation, and cybersecurity; it must provide independent financial audits and SOC reports, and demonstrate adequate capital and operational resilience.	Optionality in custody solutions will incentivize QCs to improve upon and increase transparency into their crypto asset custody security parameters, as they'll be forced to compete with the security and transparency offered by non-QC safeguarding solutions, which will lead to improved safety of client assets, whether maintained with a QC or not. While rulemaking can solve some of the issues related to standards of care, QCs will, by their nature, continue to be a black box from an administrative perspective. Thus, providing optionality via rulemaking improves an Adviser's capacity to truly understand, and dictate, custody security protocols.
Pricing Power & One-Sided Terms.	

[37] *E.g.*, various state licensing or banking regimes and the Office of the Comptroller of the Currency (for OCC-regulated custodians) may impose cybersecurity and/or operational security standards on their registrants.

[38] Notably, the Crypto Custody NAL does not broadly impose security standards on QCs, as such term is defined in the Custody Rule. Rather, it imposes standards on custodians organized as state trust companies that may or may not constitute QCs under the plain language of the Custody Rule. So, even in the wake of the Crypto Custody NAL, only certain custodians must draw from the security measures outlined therein.

Additionally, given the small market, QCs that meaningfully support crypto assets are in a very strong negotiating position when it comes to the terms by which their services are offered. As a result, Advisers are forced to onboard with QCs via contracts of adhesion, at high costs and with terms of service that are changeable at the whim of the provider. This leaves Advisers entrusting providers to custody assets with no standardization of (or deep insight into) security practices and little recourse for loss, as risk of loss is generally allocated to the customer, except in circumstances such as gross negligence or fraud.[39] Additionally, the insurance market is not keeping pace with growth in crypto asset investment. While QCs typically offer insurance coverage for certain losses, the maximum coverages are generally far below the value of assets under custody and the recognized forms of casualty are limited. As assets under custody at a small number of QCs grows, so does the risk of uninsured losses. And, given contractual terms, customers could be stuck eating losses even where a QC negligently loses customer assets.	Given the nascency of the custodial market, a portion of the high cost of third-party custody can be attributed to QCs building custodial products from the ground up. However, the ability of QCs to pass these costs onto the customer and to generally dictate pricing is predominantly a function of market power The competition produced by optionality in safeguarding solutions should prompt QCs and software providers to offer their products on terms, and at costs, more favorable for Advisers and their clients. Further, fund-level insurance policies that cover certain asset losses, including crypto assets, are available on the market, though they are not cheap. In theory, the insurance market will mature alongside the custody market. If non-QC safeguarding solutions are permitted, insurance products covering losses from non-QC safeguarding solutions should become more obtainable and affordable. This dynamic can create a positive feedback loop in the market where better insurance products for non-QC solutions may encourage QCs to offer Advisers enhanced coverage as well.
Service Availability Mismatch Against 24/7 Markets.	
Unlike traditional markets, crypto markets operate on a 24/7 basis. QCs generally do not. Maintaining crypto assets with QCs that do not operate on a 24/7 basis presents illiquidity and asset availability risks, issues that are pronounced in highly volatile markets. Most Advisers establish a variety of programmatic alerts and automatic notifications to keep investment teams informed of significant market movements, even in the middle of the night, so they can opportunistically trade, meet margin calls and take other actions in the best interests of their clients. However, these protective measures are ineffective if assets cannot be transferred and traded until their designated QC opens for business the following day. In traditional markets, QCs can align their hours of operation with market hours. To do the same in crypto, QCs would need to operate 24 hours per day, 365 days per year. This would drastically increase operational costs, thereby drastically increasing the costs of custodial services for Advisers and their clients.	For Advisers, the ability to maintain longer term positions with QCs while maintaining other assets via non-QC safeguarding solutions, creates operational flexibility to quickly make disposition decisions, react to market developments, and generally mitigate the risks associated with misalignment of 24/7 crypto markets and QC hours of operation, allowing Advisers to be more nimble and reactive to volatile market conditions. Additionally, optionality may encourage QCs to increase hours of operation to compete with non-QC safeguarding solutions, without passing massive costs onto customers.
Functional Limitations (Staking, Governance, Utility of Assets).	
Currently, QC custody solutions often constrain Advisers' ability to exercise the core functionalities of many crypto assets. For example, network tokens and application tokens are often intended to be *used* - they	Competition from other safeguarding solutions will force QCs to increase service level standards and ensure users can take full advantage of these various functionalities.

[39] Though most custody agreements are subject to confidentiality restrictions, they all contain common provider-friendly terms. For instance, common allocations of risk in digital-asset custody agreements, where custodians limit liability to gross negligence or willful misconduct and cap recoverable damages at recent fee levels. This limits remedies in the case of loss, theft and misappropriation where the custodian played a role in such loss. *See, BitGo Custodial Services Agreement*, § 14 (Limitation of Liability) (https://www.bitgo.com/legal/bitgo-custodial-services-agreement/); *Coinbase Custody Trust Company LLC*, Ex-10.3.3, Prime Broker Agreement (https://www.lawinsider.com/contracts/2Mj3Q8Wbkm5#coinbase-custody-custodial-services-agreement); *Master Custody Service Agreement*, Anchorage Digital Bank N.A. (https://contracts.justia.com/companies/ft-intermediate-inc-103940/contract/1339215/); and *Gemini Custody Agreement*, § 12 (https://www.gemini.com/legal/custody-agreement) (all visited Nov. 10 2025).

have a broad variety of functionalities and are designed to be put to work rather than passively held. For instance, staking affords Advisers the opportunity to produce additional returns for clients (or at a minimum, preserve the value of the investment in the context of an inflationary supply model), while contributing to associated protocol's network security. However, the capacity to stake assets that are held with QCs can be severely limited, and QCs may require that customers utilize affiliated staking providers with high commission rates. Thus, Advisers are often in the unfortunate position of determining to forgo staking rewards (or pay high fees) that would otherwise accrue to clients, and contributing to a protocol or network's security, solely to remain in compliance with the Custody Rule.	

In short, a more open safeguarding regime would diversify service providers, broaden asset coverage, reduce concentration thereby enhancing systemic resilience, and align incentives toward stronger security and lower costs—benefits that extend to both Advisers and their clients.

ii. *Additional Operational and Legal Considerations for Rulemaking*.

The following considerations highlight residual frictions that neither the Framework nor optionality in rulemaking alone will fully resolve. These issues illustrate where more guidance is needed, and how a reasonableness standard will provide Advisers the flexibility necessary to implement crypto asset safeguarding programs that serve their clients' best interests while the market continues to develop.

a. Establishing Baseline Standards and Protections.

1. **Developing Standards of Care**.

Rulemaking can, and absent a legislative framework for crypto, probably should, impose minimum standards of care as applied to this asset class, such as those described in the Crypto Custody NAL. QCs, operating as centralized financial institutions, often move slowly in adapting to emerging threats such as phishing attacks, deepfake authorizations, or zero-day vulnerabilities. While non-QC safeguarding solutions allow Advisers to set bespoke security standards, regularly update internal protocols, and respond swiftly to new risks, custody frameworks will inevitably need a reasonableness standard to be applied in evaluating the sufficiency of their efforts, rather than the application of a prescriptive set of requirements.

Whether using a QC or a non-QC safeguarding solution, safeguarding should not depend on uniformity of these procedures but on reasonably designed controls proportionate to the risks and technologies used. Under a reasonableness standard, Advisers using non-QC safeguarding solutions and QCs would be expected to (i) implement controls appropriate to the assets and technologies they manage; (ii) document those controls and periodically test their adequacy; and (iii) update these safety protocols as threat vectors evolve.

This approach encourages continuous improvement and adaptability while aligning with the SEC's historical reliance on principles of reasonableness.

In developing standards as to what constitutes reasonable efforts for safeguarding client assets, as it has in prior rulemakings, the SEC should draw on existing best practices. With respect to non-QC safeguarding solutions, the Commission should draw on the practices of institutional actors (including Advisers) who have expended significant resources developing these solutions over years of operating in the crypto space. The Framework distills many of these practices, mapping them against the Custody Rule's core policy objectives to demonstrate that those goals can be satisfied—even strengthened—without mandatory third-party intermediation. The SEC should draw on these best practices in evaluating updates to the Custody Rule and/or providing interpretive guidance or no action relief with respect to the same.

2. **Loss Exposure & Illiquidity**.

Likewise, a reasonableness-based rule would not prescribe required safeguarding architecture in granular detail but could entail minimum standards for segregation and recordkeeping. Namely, both Advisers and QCs would be required to demonstrate that client assets remain identifiable, segregated, and recoverable.

Whether assets are safeguarded through the use of a QC or a non-QC safeguarding solution, reasonableness could hinge on evidence of (i) clear beneficial ownership, (ii) traceable control, and (iii) backups/procedures to ensure continuity of access. While, loss exposures can be mitigated in part through insurance in the case of theft or loss of assets, other exposures remain. Centralized custody models inherently introduce both counterparty and insolvency risk. Even in instances where QCs represent that clients retain title to assets in their terms of service, these terms of service contain carve outs.[40] Further, bankruptcy proceedings can create extended periods of illiquidity and have resulted in uncertain outcomes, as seen in cases where pooled assets were deemed part of a bankruptcy estate.

While rulemaking cannot remove all risk in this area, it can set minimum standards to help ensure title stays with the client through bankruptcy where possible by requiring clear recordkeeping, disclosures and standards to verify beneficial ownership and continuity of control, ensuring that clients' assets remain safeguarded under all custody models.

b. Applying a Reasonableness Standard to Ensure Flexibility.

1. **Market Availability of Custody Solutions.**

Advisers often make investment commitments before a crypto asset or its network fully exists, or before any custodian (traditional or MS/MPC) offers support. Even under a flexible framework, there will be cases where no established institutional grade custody solution is immediately available. For instance,

[40] These carve outs are likely to persist even with a legislative framework. For instance, the draft of the Responsible Financial Innovation Act of 2025 (RFIA) released by the Senate Committee on Agriculture, Nutrition, and Forestry on November 10, 2025 carves out of customer protection from bankruptcy assets removed from segregation because the customer elects to participate in blockchain services (validation, staking, governance etc) and the draft legislation does not dictate how the custodian might be required to act or be held liable if they or their affiliates are the ones performing these services and subjecting the assets to possible loss. See Sec. 204(a), discussing standards for holding customer assets with a QC and when exceptions are granted, including 5i(d)(4)-(6). See U.S. Senate Comm. on Agric., *Boozman, Booker Release Bipartisan Market Structure Discussion Draft* (Nov. 10, 2025), https://www.agriculture.senate.gov/newsroom/rep/press/release/boozman-booker-release-bipartisan-market-structure-discussion-draft (linking to latest RFIA draft).

this occurs in practice when new chains come to market and there is initially only a native wallet solution available.

Therefore, rulemaking should adopt a reasonableness standard that accommodates these factual realities. Advisers should not face enforcement exposure merely because a QC or non-QC safeguarding solution has not yet integrated a new asset. Instead, the Commission should permit good-faith safekeeping arrangements subject to reasonable documentation and risk controls. This approach is consistent with the SEC's Project Crypto goals to "facilitate capital formation and accommodate innovation".[41]

2. **Enabling Functionality**.

Above, this Whitepaper discusses that QC staking and governance functionality is typically published as a limited list of supported protocols and often rolled out after standard custodial support. Thus, mandatory QC custody can often prevent Advisers from exercising key functionalities of assets, such as participation in certain protocol-native yield and governance mechanisms, even when such activities are low-risk. Third-party custody can also prevent the functional use of certain crypto assets, such as in-game assets (*e.g.*, for gameplay/earning other rewards). Permitting non-QC safeguarding can expand functional use, but does not fully resolve these limitations.

For instance, there seems to be a general acknowledgement that staking should be permissible. However, given staking often requires "locking" assets into a third-party smart contract, it's unclear whether staking solutions offered by QCs even confer the benefit of Custody Rule compliance on their customers.

The SEC should provide guidance clarifying how the Custody Rule applies to activities that involve temporary or functional transfer of assets onchain, such as liquid staking[42] or participation in decentralized finance protocols.[43] These activities are increasingly integral to how many crypto assets are used and derive value, yet current guidance leaves Advisers uncertain as to whether engaging in them constitutes a breach of the Custody Rule.

Depositing client assets into a staking contract, liquid staking protocol, or DeFi smart contract could be viewed as violations of the Custody Rule because the assets are no longer 'held' directly within the Adviser's or the QC's multisig or MPC-controlled wallet. Likewise, platforms like Liquifi, Magna and others that programmatically enforce lockups fall into a grey area given most investors would argue they hold title to the underlying asset as of the time the lockup commences.

With respect to onchain participation, a reasonableness-based standard would help resolve this ambiguity by evaluating whether the Adviser maintained effective control and documentation of the activity. Where the Adviser (or its designated Signer framework) maintains verifiable authority to initiate, monitor, and redeem such positions, and where the transaction is executed under disclosed policies and risk parameters,

---

[41] *SEC's Approach to Digital Assets: Inside "Project Crypto"*, Paul S. Atkins, Nov. 12, 2025, *available at* https://www.sec.gov/newsroom/speeches-statements/atkins-111225-secs-approach-digital-assets-inside-project-crypto.

[42] For instance, liquid staking guidance could indicate that where the staked asset is converted into a derivative or receipt token, it does not automatically constitute a custody breach if the Adviser maintains continuous recordkeeping, valuation, and redemption controls.

[43] DeFi participation guidance could clarify that where assets are deposited into smart contracts for yield generation, collateralization, or governance, it is not per se prohibited, provided that reasonable due diligence, protocol risk assessments, and client disclosures are documented.

the Adviser should be deemed to have maintained custody consistent with the Custody Rule's safeguarding objective.

Accordingly, Commission guidance could clarify that custody is preserved through demonstrable control, traceability, and recoverability, all of which can be demonstrated in a manner of ways. Such clarification would promote regulatory certainty and allow Advisers to manage client assets in a manner consistent with both technological realities and fiduciary duties, while preserving the Custody Rule's core goal: ensuring client assets remain safeguarded.

IV. Conclusion: The Case for Regulatory Pragmatism

These remaining frictions underscore the importance of regulatory pragmatism. Rulemaking should implement a reasonableness-based standard that measures Adviser conduct by evaluating the soundness of their controls and processes, not by the presence or absence of a specific custodian. Even with flexible, technology-neutral rulemaking, the SEC cannot regulate away every risk or anticipate every new asset type. There will always be areas that warrant continued coordination among regulators and active industry self-governance. What rulemaking *can* do is create adaptive principles that evolve with market practice.

Crypto technology was designed to enable secure, verifiable self-custody. When properly implemented, non-QC safeguarding solutions can satisfy, and in some respects better advance, the core investor-protection objectives of the Custody Rule. Blockchain-based systems already support transparent accounting, continuous auditability, and real-time reconciliation, offering a pathway to stronger, not weaker, safeguards for client assets. Blockchain-based recordkeeping could allow administrators and auditors to monitor asset flows continuously, reducing reconciliation errors and improving fraud detection, advancements that align directly with the Custody Rule's investor-protection objectives. Permitting non-QC safeguarding solutions, with the addition of software that tracks transactions and provides real time data, could present an improvement over the status quo, if allowed to continue to develop.

The Framework demonstrates *an implementation of indicative best practices* for achieving these protections through MS/MPC-based safeguarding models. It is not intended to be a single, static standard, but an illustration of how Advisers are already meeting the Custody Core Tenets. As market practices, technologies, and assurance methods evolve, so too must Adviser practices, guided by ongoing regulatory engagement, guidance and empirical feedback.

In all, this Whitepaper requests rulemaking that invokes a reasonableness standard, permits non-QC safeguarding, harmonizes cross-agency standards, and incentivizes competition and custody market growth. By adopting a tech-neutral, principles-based safeguarding framework, while providing guidance on standards of conduct in each safeguarding paradigm, the Commission can ensure that investor protection and market innovation advance in tandem. This ensures that as the ecosystem evolves, the regulatory framework for safeguarding can evolve on a parallel basis.

Exhibit A
Framework

The below chart: (i) lists the components of our model non-QC safeguarding solution and operating parameters; (ii) maps their implementations to the policy goals of the Custody Rule and the Custody Core Tenets; and (iii) explains how the model components and parameters achieve the underlying policy objectives of the Core Custody Tenet to which they correspond.

Tenet 1: ***Safeguarding*** – Client funds and securities must be kept in a place safe from misuse, misappropriation, loss and Adviser financial reverses.		
Framework Implementation	**Current Custody Rule Implementation & Policy Rationale**	**Explanation of Redress by Framework / Policy Analysis**
Client cryptoassets[44] are safeguarded utilizing institutional grade MS/MPC software, with Adviser-tailored parameters and controls such as the following:[45] Construct MS/MPC instances such that a minimum threshold of persons with authority to "sign" transactions ("***Signers***") are necessary to facilitate the movement of assets. 1. No single person is capable of moving client assets. Rather, a specified number of individual Signers must sign a transaction to execute the transfer of client assets. 2. Signer thresholds for moving assets may be differentiated based on transaction value (*e.g.,* 3/5 for transactions of less than $1M, but 4/5 for transactions of $1M or more, etc.).[46] 3. To the extent practical, geographically distribute Signers, to mitigate the risk of in-person compromise. 4. Ensure Signers are senior, trusted, tenured and span various divisions of the Adviser's operations (e.g.,	Current Implementation: RIAs must custody client funds and securities *with a qualified custodian* ("***QC***"). High Level Policy Rationale: Ensure client assets are safe and secure. Advisers must keep client assets safe from theft, loss, misappropriation and financial reverses of the Adviser. From 1962 until 2003, the Custody Rule required only that Advisers custody client funds and securities "*in some place reasonably free from risk of destruction or other loss*".[49] In 2003, the SEC amended the rule to require that client funds and securities be kept with QCs.[50] In making this amendment, the SEC indicated the QC requirement was intended to memorialize existing market best practices. The SEC found that most Advisers were already keeping stock certificates and funds with	While the Framework departs from the QC requirement, it does not depart from the Custody Rule's underlying policy objective of ensuring client assets are safe from theft, loss, misappropriation and Adviser financial reverses. To the contrary, the Framework provides Advisers an option to manage client crypto assets in a manner that (i) is arguably as safe or safer than QC custody, (ii) permits Advisers to take advantage of productive applications of crypto assets, such as staking, thereby maximizing value for clients and (iii) reduces costs and administrative overhead. Importantly, the Custody Rule does not impose any requirements on the technologies and procedures deployed by QCs to custody crypto assets. Applying the QC requirement to client crypto assets simply assumes that because an entity is equipped to safely custody funds and securities, it is also equipped to safely custody crypto assets. This is not the case, as there are unique technical procedures and safeguards required to safely control crypto assets. The Framework, on the other hand, outlines specific practices for safekeeping crypto assets that are tailored to address their unique properties.

[44] Traditional (*i.e.,* fiat) funds should continue to be maintained with QCs (*e.g.*, banks). Fiat-backed stablecoins, to the extent they constitute funds for the purposes of the Act, should be maintainable in accordance with the non-QC safeguarding framework outlined herein, as the protections it affords to other crypto assets apply equally to fiat-backed stablecoins.

[45] Note that all of the parameters referenced here are implementable via currently available institutional grade MS/MPC software.

[46] Signer thresholds would follow best practices, such as those articulated in the Security Alliance's Multisig Wallets For Advanced Users & High Funds, available at https://frameworks.securityalliance.org/wallet-security/secure-multisig-best-practices/.

[49] *See, e.g.*, FN 20.

[50] This was a function of the SEC determination that, with respect to certificated securities and client funds, a QC was the clear choice to meet the reasonableness standard to keep assets free from loss or malfeasance.

finance, investment team, legal, etc.) or other agents of a client, and, in each case, have expertise in onchain signing, and are subject to ongoing training in operational security practices. a. If the MPA Sponsor determines it prudent, Signers may also include third-party personnel who work for the Adviser in a fiduciary or similar capacity (*e.g.,* administrator, audit or accounting team personnel). 5. Only utilize MS/MPC software that has passed extensive code audits. 6. Ensure MS/MPC software providers maintain certain operational security certifications (*e.g.,* SOC2).[47] 7. Subject Signers to a policy set or Multisig Participation Agreement ("***MPA***") that establishes Signer roles, protections, obligations, standards of care, liabilities to clients and operating and removal procedures. MPAs should ensure some or all of the following: a. Client assets are subject to insurance coverages for loss, theft, misappropriation, etc. up to commercially reasonable limits available in the market.[48] b. Third-party auditors, Signers, and/or fund administrators have real time "view-only" access to MS/MPC balances and contents,	entities that constitute QCs, but it codified this convention via rulemaking to eliminate edge cases of poor custodial practices. In fact, the proposed rule underpinning the 2003 amendments[51] stated that "*[a]lmost all advisers that have custody of client securities maintain them in accounts with a broker or a bank, but on occasion our examiners discover an adviser keeping [stock] certificates in office files or a safety deposit box. Such custodial practices do not provide adequate protection for client securities, because these certificates may be too easily lost, stolen or destroyed*" (emphasis added).[52] Thus, the principal purpose of the Custody Rule is, and has been, ensuring client assets are properly safeguarded from theft, loss, misappropriation and adviser financial reverses. The QC requirement is merely a codified approach to serving this purpose. But, new asset classes and safeguarding solutions have emerged that require revisiting the utility of the QC requirement.	Modifying safeguarding practices based on the properties of specific asset forms is not a novel concept. The Custody Rule and related SEC guidance acknowledge that the practicality and utility of QC custody is not uniform across all assets (or even across all funds and securities). For instance, privately offered securities ("***POS***") need not be maintained with a QC where the POS are uncertificated and meet certain additional specifications that minimize risk of loss or malfeasance by the Adviser[53](the "***POS Exception***"). In 2013, via written guidance (the "***2013 Guidance***"), the SEC expanded the POS Exception to apply to certificated POS that are held by pooled investment vehicles and meet certain criteria to minimize the risk of loss and malfeasance.[54] In implementing the POS Exception (as expanded by the 2013 Guidance), the SEC acknowledged that in certain instances, the QC mandate may impose undue costs and burdens while adding little protection for clients, and in such instances, it should not apply. The departure from the QC mandate requested by this Whitepaper is no different. For the reasons stated herein, mandating that Advisers maintain client crypto assets with QCs (i) in certain cases, constitutes an operationally infeasible directive; (ii) fails to ensure adequate safeguards; (iii) imposes undue costs, administrative burdens and overhead; (iv) creates friction with an Adviser's fiduciary duties; (v)

[47] *See,* e.g., SEAL Framework Checklist (SFC) for Multisig Operations, SECURITY ALLIANCE, https://frameworks.securityalliance.org/certs/sfc-multisig-ops/ (last visited Dec. 18, 2025) (setting forth industry best practices for secure multisig custody operations, including access controls, transaction authorization, and key management).

[48] Currently, such policies are difficult to obtain, and even if obtainable, may be cost prohibitive. However, it's expected that the insurance market will develop and evolve with time. The SEC's blessing of well-tailored self-custody solutions may catalyze such development.

[51] Securities and Exchange Commission, *Custody of Funds or Securities of Clients by Investment Advisers*, Release No. IA-2044, File No. S7-28-02 (July 18, 2002) (67 Fed. Reg. 48,579 (July 25, 2002)), https://www.sec.gov/rules-regulations/2002/07/custody-funds-or-securities-clients-investment-advisers.

[52] *Id*.

[53] Specifically, the requirements are that the POS are (i) acquired from the issuer in a non-public offering; (ii) uncertificated, with ownership recorded only on the books of the issuer or its transfer agent in the name of the client, and (iii) transferable only with prior consent of the issuer or holders of the outstanding securities of the issuer.

[54] These requirements dictated that (i) the stock certificate can only be used to effect a transfer/facilitate a change in beneficial ownership of the security with the prior consent of the issuer or holders of the outstanding securities of the issuer; (ii) ownership of the security is recorded on the books of the issuer or its transfer agent in the name of the client; (iii) the stock certificate contains a legend restricting transfer; and (iv) the stock certificate is appropriately safeguarded by the adviser and can be replaced upon loss or destruction.

and may receive real-time notifications of transactions. c. Proper implementation of back-up procedures and distribution of backup keys, so a Signer's unavailability/incapacitation, or key loss, does not compromise asset safety. d. Client assets are held in trust by the Adviser for the clients and that the Signers are engaged by the Adviser to fulfill the Adviser's duty to safeguard client assets. e. Title to assets remains with the client and that client assets are not deemed Adviser estate assets in the event of the Adviser's insolvency.		fails to acknowledge that novel asset classes may require tailored custody solutions; and (vi) frustrates the three-part mission of the SEC. Permitting Advisers to utilize non-QC safeguarding solutions like those described in the Framework serves the policy objectives of the Custody Rule, ensures adequate protections for client crypto assets, reduces costs and administrative overhead, resolves tensions between an Adviser's fiduciary duties and the Custody Rule and serves the SEC's three-part mission.
Tenet 2: ***Segregation*** – Client assets must be segregated from Adviser assets.		
Framework Implementation	**Existing Implementation & Policy Rationale**	**Explanation of Redress by Framework / Policy Analysis**
Each MS/MPC wallet should control assets attributable only to a single client, such that client assets are not commingled with the assets of the Adviser or another client of the Adviser. 1. Alternatively, Advisers may establish omnibus wallets in the Adviser's name as agent or trustee for the client(s), which wallets contain only client assets (not Adviser assets), in a manner akin to the practice permitted by Section (a)(1)(ii) of the Custody Rule. In each case, MPAs should further delineate the scope of coverage of a particular MS/MPC signature scheme and the client(s) for each.	Current Implementation: Client funds and securities must be held: (i) in a separate account for each client under that client's name; or (ii) in accounts that contain only client funds and securities, under the Adviser's name as agent or trustee for the clients.[55] High Level Policy Rationale: Commingling client and Adviser funds and securities (i) creates accounting hurdles, (ii) increases the risk of disguisable misappropriation and (iii) increases risk of loss in the event of Adviser insolvency.	Existing institutional grade MS/MPC technologies permit segregation of assets in the same manner as QC accounts. Wallets are easily established for each client (and if desired, for each position of a client). Alternatively, omnibus wallets for client assets can be established in the Adviser's name, as agent/trustee for the clients with ownership of the underlying assets. Segregation using MS/MPC software is actually easier than in the QC context, as establishing new wallets in an MS/MPC instance is generally more efficient than establishing new QC accounts and sub-accounts, a process which often carries administrative/bureaucratic overhead.
Audited Private Funds: While the remainder of this chart outlines how non-QC safeguarding solutions can satisfy the Client Notifications, Account Statements and Independent Verification Core Custody Tenets, it should be noted, once again, that with respect to private fund clients, Advisers may satisfy these Custody Core Tenets by relying on the exception provided in Section (b)(4) of the Custody Rule for audited private funds (the "***Audit Exception***"). The Audit Exception would remain available for Advisers to private fund clients utilizing non-QC safeguarding solutions, rendering the below proposed implementations largely inapplicable for such Advisers.		
Tenet 3: ***Client Notifications –*** Clients must be properly notified when custodial accounts are established or changed.		
Framework Implementation	**Existing Implementation & Policy Rationale**	**Explanation of Redress by Framework / Policy Analysis**

[55] *See*, Custody Rule, Section (a)(1).

Advisers could provide clients with notifications when onboarding with new MS/MPC software solutions and/or when making other material changes to their safeguarding program. Advisers can also notify clients of custodial arrangements via the distribution/availability of Forms ADV. ADV Brochures contain high-level summaries of safeguarding procedures and solutions and the Commission could mandate that ADVs are updated when material modifications are made to such procedures.	Current Implementation: If an Adviser opens an account with a QC on its client's behalf, either under the client's name or under the Adviser's name as agent, the Adviser must notify the client in writing of the QC's name, address, and the manner in which the funds or securities are maintained, promptly when the account is opened and following any changes to this information. If an Adviser sends account statements to a client for which it is required to provide this notice, the Adviser must include in the notification and in any subsequent account statement the Adviser sends that client, a statement urging the client to compare the account statements from the custodian with those from the Adviser.[56] High Level Policy Rationale: Clients should be made aware of where their assets are held and when custodian relationships are established and modified.	As the Framework demonstrates, non-QC safeguarding solutions like the Framework address this tenet without issue. Notification should balance meaningful disclosure while retaining good operational security. Safeguarding arrangements can be broadly described in marketing materials and ADVs, while forgoing granularity such as wallet configurations and specific assets held with a particular custodian. This is consistent with good operational security practices. Limiting the public footprint of custody arrangements will reduce the surface area for phishing attacks, which are increasingly a threat for investors.[57] As noted above, consistent with the Custody Rule, Advisers properly relying on the Audit Exception are not required to comply with these notification requirements.
Tenet 4: ***Account Statements*** – Clients should receive account statements identifying funds and securities held in, and transactions occurring from, the applicable account, during the period covered by such statements.		
Framework Implementation	**Existing Implementation & Policy Rationale**	**Explanation of Redress by Framework / Policy Analysis**
Account Statements: 1. Advisers and/or their third-party administrators are responsible for ensuring statements are delivered to clients (and/or PIV LPs, if applicable). 2. MS/MPC instances are designed to provide real-time view-only access to wallet contents for Adviser administrators and/or accountants or auditors, which solutions may also enable at-will report generation.[58]	Current Implementation: Advisers must have a reasonable basis, after due inquiry, for believing that their QCs send an account statement, at least quarterly, to each Adviser client for which the Adviser maintains funds or securities, identifying the amount of funds and each security in the account at the end of the period and setting forth all transactions in the account during that period.[59]	Non-QC safeguarding solutions like the Framework meet and potentially improve upon this tenet. Rather than relying on a "reasonable basis for believing" account statements are distributed to clients, Advisers and/or their third-party administrators will be responsible for ensuring account statements are delivered. Non-QC safeguarding solutions like the Framework can be designed to provide real-time view-only access to wallet contents for Adviser administrators, accountants and/or auditors, which solutions may also enable at-will report generation.

[56] Advisers relying on the Audit Exception need not comply with this requirement.
[57] See *e.g.*, recent reports on past instances of security threats, available at https://x.com/zachxbt/status/1886411891213230114, and analysis indicating these threats will only increase with the advent of deepfake technology, available at https://x.com/reidhoffman/status/1783145009153450374.
[58] While public blockchains are publicly viewable, the wallet addresses will generally be guarded as a matter of operational security. These wallet addresses are often provided to parties with a need to know, e.g., for verification purposes by fund administrators, accountants and auditors.
[59] *See*, Custody Rule, Section (a)(3).

3. Administrators, accountants and/or auditors may be required to certify to quarterly review of statements before such statements are circulated or made available to clients.	High Level Policy Rationale: Clients should have visibility into the state of their accounts with an Adviser, and should receive transaction logs and updates for reconciliation purposes.	This can improve efficiency, reduce errors created by manual data entry and improve delivery times to clients. As an additional check, administrators, accountants and/or auditors could be required to certify to quarterly review of statements before such statements are circulated or made available to clients.
Tenet 5: ***Independent Verification*** – Client assets under custody must be subject to third-party independent verification.		
Framework Implementation	**Existing Implementation & Policy Rationale**	**Explanation of Redress by Framework / Policy Analysis**
Verifications. Advisers remain subject to the Custody Rule's independent verification requirements (satisfiable through the Audit Exception, if applicable). 1. Accountants and/or auditors utilize established, market procedures for (i) verifying and/or auditing assets managed via non-QC safeguarding solutions and (ii) ensuring the Adviser can demonstrate control over any such assets. 2. Advisers will be subject to verification and/or audited in accordance with the Custody Rule (and those relying on the Audit Exception will distribute audited financials in accordance with the rule). 3. At the accountant's or auditor's request, Advisers can ensure such accountants or auditors are auto-notified of transactions occurring from monitored wallets and of the establishment of a new wallet within an MS/MPC instance.	Current Implementation: Ensure that all client funds and securities are verified by actual examination at least once during each calendar year by an independent public accountant at a time which shall be chosen by such accountant without prior notice to the investment adviser, with the accountant providing a certificate to the SEC memorializing the examination of such funds and securities, and describing the nature and extent of such examination.[60] Alternatively, for private fund clients, ensure annual audits and distribution of audited financials in accordance with the Audit Exception. High Level Policy Rationale: Advisers should be subject to checks and reconciliations by qualified third-party accountants or auditors to ensure the Adviser has implemented good accounting practices and to deter and detect Adviser foul play.	Advisers will remain subject to Custody Rule independent verification requirements, whether pursuant to Section (a)(4) of the Custody Rule or the Audit Exception. However, non-QC safeguarding solutions such as the Framework may ease the burden of independent verifications and audits for the Adviser and the accountants or auditors. Independent verification can be accomplished by requiring micro/test transactions to demonstrate retained control of wallets and client assets. With respect to assets kept onchain, MS/MPC solutions can provide accountants and auditors 24/7 real time, view-only access to wallets containing client assets. Thus, these verifying bodies are enabled to conduct reconciliations on a surprise and/or scheduled basis annually, quarterly or on any other cadence, as necessary. Internationally reputable (Big Four) accounting and audit firms have established procedures for ensuring Adviser control of MS/MPC solutions used to manage client assets, including leveraging test transactions performed while on video calls. MS/MPC solutions can be designed to auto-notify accountants, auditors and/or administrators of (i) transactions occurring from monitored wallets and (ii) establishment of a new wallet within an MS/MPC instance. This could enable administrators, accountants and/or auditors to tie out each transaction in real time and set alarms for transactions outside of expected parameters.

[60] *See*, Custody Rule, Section (a)(4).