Veda Tech Labs Inc.

Veda Tech Labs Inc.
20 Jay Street Suite 402
Brooklyn, New York 11201

March 23, 2026

Division of Investment Management, Securities and Exchange Commission
Crypto Task Force, Securities and Exchange Commission
Division of Market Participants, Commodity Futures Trading Commission
Joint SEC-CFTC Harmonization Initiative

Re: Recommendations Regarding Recognition of Vaults as Satisfying SEC Qualified Custody and CFTC Segregation Requirements for Digital Assets

Dear Sir or Madam:

Veda Tech Labs ("Veda") submits this letter in response to (i) the SEC's Division of Investment Management's statement in the Commission's 2025-2026 Regulatory Agenda that it is considering recommending amendments to modernize the custody framework for advisory client assets, including crypto assets,[1] and (ii) the SEC-CFTC Memorandum of Understanding Regarding Harmonization in Areas of Common Regulatory Interest, signed March 11, 2026 (the "2026 MOU"), which commits both agencies to facilitating the exploration of alternative compliance frameworks capable of achieving regulatory objectives while preserving investor protection and market integrity.[2]

This letter proposes that the SEC and CFTC recognize certain non-custodial smart-contract vault architectures as satisfying the core safeguarding objectives of their respective customer asset protection regimes when defined structural guardrails are present. For the SEC, those objectives are reflected in Rule 206(4)-2 under the Investment Advisers Act of 1940, which is designed to protect client assets[3] from misappropriation, commingling, and exposure to intermediary insolvency. For

---

[1] U.S. Securities and Exchange Commission, Spring 2025 Regulatory Agenda, Division of Investment Management, Custody Modernization (2025-2026) (stating that the Division is considering recommending that the Commission propose amendments to existing rules and/or propose new rules under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 "to improve and modernize the regulations around the custody of advisory client and fund assets, including to address in each case crypto assets").

[2] SEC-CFTC Memorandum of Understanding Regarding Harmonization in Areas of Common Regulatory Interest (Mar. 11, 2026) ("2026 MOU"), Art. III, §3.

[3] For purposes of this letter, references to "client assets" refer to assets held by a regulated intermediary on behalf of its customers or investors under the applicable custody or segregation framework. In the context of the Advisers Act, this refers to assets held by an investment adviser on behalf of its advisory clients within

the CFTC, parallel protections arise under the Commodity Exchange Act and implementing regulations requiring segregation of customer property by Futures Commission Merchants and Commodity Pool Operators, including CFTC Regulations 1.20 and 4.20.

Vault architectures that eliminate unilateral withdrawal authority, prevent balance-sheet intermediation of client assets, and enable continuous on-chain verification of holdings can, when implemented with appropriate governance and security controls, directly address those protective objectives through technical architecture instead of reliance on a centralized custodial intermediary.

Rather than displacing existing qualified custodian or segregated intermediary models, this framework would provide an additional, crypto-native compliance pathway particularly well suited to the technical architecture of digital asset markets. In certain circumstances, it would also resolve an emerging operational constraint faced by investment advisers and other institutional market participants: the inability to custody certain digital assets because no qualified custodian currently supports them from an infrastructure standpoint.[4]

Veda builds institutional-grade, non-custodial vault infrastructure used by enterprise participants in digital asset markets across multiple chains and crypto protocols. Members of Veda's Legal and Compliance team have held senior legal, compliance, and policy roles within the existing qualified custodian framework, including at the SEC, at federally regulated digital asset custodians, and at Registered Investment Advisors ("RIAs") subject to Rule 206(4)-2. This experience informs Veda's perspective on how vault architectures can achieve the safeguarding objectives of the Advisers Act custody framework and the Commodity Exchange Act's customer property protection regime.

The sections that follow analyze the statutory objectives of the custody and segregation rules, the operational realities of digital asset infrastructure, and the comparative risk profile of vault-based custody models. The letter concludes with a recommended guardrail-based compliance pathway that would allow advisers and other regulated entities to satisfy custody and segregation requirements when client assets are maintained in vault architectures meeting defined structural conditions.

I. STATUTORY OBJECTIVES OF CUSTODY AND SEGREGATION RULES

Rule 206(4)-2 derives from the SEC's authority under Section 206(4) of the Advisers Act to prevent fraudulent, deceptive, or manipulative acts by investment advisers.[5] The rule was adopted to address

---

the meaning of Rule 206(4)-2. In the context of the Commodity Exchange Act, this refers to customer or pool property required to be segregated under CEA §4d and CFTC Regulations 1.20 and 4.20.

[4] *See, e.g.*, Comment Letter from Bain Capital Crypto, Dragonfly Capital, Electric Capital, Haun Ventures, and Ribbit Capital in response to the SEC's 2023 Safeguarding Proposal re Safeguarding Advisory Client Assets, 88 Fed. Reg. 14,672 (Mar. 9, 2023) ("2023 Safeguarding Proposal"), *available at* https://www.sec.gov/comments/s7-04-23/s70423-186379-340322.pdf (explaining how the lack of certain qualified custody options hinders innovation and investment).

[5] 15 U.S.C. § 80b-6(4); Custody of Funds or Securities of Clients by Investment Advisers, Investment Advisers Act Release No. IA-2176 (Sept. 25, 2003), 68 Fed. Reg. 56,692 (Oct. 1, 2003).

three specific risks: misappropriation of client funds, commingling of assets, and exposure of client property to adviser insolvency.[6]

When the SEC amended the Custody Rule in 2003, it emphasized that requiring use of qualified custodians was designed to protect client assets from misuse and reduce opportunities for embezzlement.[7] Following the Madoff fraud, the SEC strengthened custody protections in 2009, again centering the rule on safeguarding and independent verification.[8]

The qualified custodian requirement was therefore a mechanism to achieve a statutory objective; not an end in itself. It reflected the prevailing structure of centrally recorded securities and balance-sheet intermediation. The Division of Investment Management's (the "Division") own agenda statement recognizes that existing custody regulations require modernization to address crypto assets. Veda's recommendation is grounded in that same goal: not whether safeguarding must occur, but what forms of it satisfy the rule's protective purpose when applied to digital assets. Unlike traditional securities and commodities, digital assets are controlled through cryptographic signing authority, recorded on distributed ledgers, and can be governed by deterministic smart contract logic — technical characteristics that the original custody framework never contemplated and that any modernized rule should address directly.

The CFTC's protective framework is structurally parallel. The Commodity Exchange Act and CFTC regulations require Futures Commission Merchants ("FCMs") to segregate customer funds from house funds and prohibit their use for the firm's own purposes.[9] CFTC Regulation 4.20 likewise requires Commodity Pool Operators ("CPOs") to hold pool property in the name of the pool, maintain it separately from non-pool property, and prohibits the CPO from using pool assets other than for the benefit of the pool.[10] The CFTC's protective purposes of preventing misappropriation, prohibiting commingling, and protecting customer property from insolvency exposure are identical to those of Rule 206(4)-2. Many institutional participants in digital asset markets are registered with or regulated by both agencies simultaneously. Thus, a guardrail-based compliance pathway that satisfies the SEC's custody rule through the structural conditions set out in Section V of this letter

[6] *Id.* See also Custody of Funds or Securities of Clients by Investment Advisers, Investment Advisers Act Release No. IA-2969 (Dec. 30, 2009), 75 Fed. Reg. 1,456 (Jan. 11, 2010) ("2009 Amendments").

[7] IA-2176, 68 Fed. Reg. at 56,693.

[8] IA-2969, 75 Fed. Reg. at 1,457.

[9] 7 U.S.C. § 6d(a)(2) (CEA § 4d); 17 C.F.R. § 1.20 (requiring FCMs to maintain customer funds in segregated accounts, keep them separate from the firm's own funds, and prohibiting use of customer funds for any purpose other than to margin, purchase, or protect customer trades).

[10] 17 C.F.R. §§ 4.20(a)–(c). Section 4.20(c) provides that a CPO "shall not use or permit the use of" pool property "other than for the benefit of the pool." See also 17 C.F.R. § 4.30 (prohibiting CTAs from commingling client trading accounts with non-client property).

should also satisfy the CFTC's customer property protections under CFTC Regulations 4.20 and 1.20.

II. INFRASTRUCTURE CONSTRAINTS AND FIDUCIARY TENSION

In digital asset markets, support for a given token by a qualified custodian is not universal. Onboarding a new asset requires engineering integration, node infrastructure, operational monitoring, and commercial prioritization. Custodian decisions often reflect infrastructure readiness and commercial viability rather than regulatory determinations of asset risk.[11]

RIAs may encounter assets to which clients are contractually entitled but for which no qualified custodian is technologically capable or available. In such circumstances, advisers face a difficult choice: decline to receive assets to which clients are entitled; delay receipt pending custodian integration, which may cause tax or timing harms to clients; or self-custody using makeshift solutions while accepting regulatory ambiguity.

This dynamic creates a structural tension with fiduciary duty. When infrastructure availability and not asset risk determines investment access, Rule 206(4)-2 risks functioning as a de facto innovation bottleneck rather than a calibrated investor protection mechanism. The proposed modernization of the custody framework presents a direct opportunity to resolve this tension by providing a clear, conditions-based pathway for digital asset custody that does not depend exclusively on the technical readiness or willingness of centralized intermediaries.

Beyond the infrastructure bottleneck, vaults offer other benefits to RIAs such as multi-asset and cross-chain coverage with little to no engineering integration required, particularly valuable for long-tail or early-stage token positions; vault redemptions execute on-chain in near real-time, 24/7, without wire cutoffs, T+1 settlement cycles, or custodian operating-hour constraints; on-chain vault balances are continuously verifiable by any authorized party, providing real-time proof of holdings that periodic account statements cannot replicate; and reduced custody costs at scale. Finally, as tokenized real-world assets such as securities, fund interests, real property, and commodities grow as a share of institutional digital asset portfolios, the custody question for those instruments becomes live. Vault architecture built for digital assets is natively suited to hold tokenized RWAs, whereas most existing qualified custodians have no established operational capacity for these instruments. A defined compliance pathway that accommodates vault custody now will provide the legal infrastructure for institutional RWA adoption as those markets develop.

[11] This dynamic was addressed in public commentary during the 2023 Safeguarding Proposal comment period. *See, e.g.*, letters submitted by Blockchain Association, Coinbase Global, Inc., and other market participants (Apr.–May 2023).

III. MISAPPROPRIATION, INSOLVENCY, AND OPERATIONAL SAFETY IN VAULT ARCHITECTURES

A. Misappropriation Risk

The Custody Rule's central aim is to prevent misappropriation. Any modernization analysis should therefore evaluate whether particular vault architectures meaningfully mitigate that risk, and how they compare to traditional custody models on that specific dimension.

Centralized custody models mitigate misappropriation risk through institutional key management systems, internal controls, compliance programs, and supervisory oversight. These systems can be robust and effectively achieve the protective purposes of the Custody Rule.[12]

Certain vault architectures address these same risks through a structurally different mechanism. Withdrawal logic is embedded directly in smart contract code. Asset movement may require threshold cryptographic authorization, structurally preventing unilateral withdrawal authority. Client redemption rights can be encoded as invariant features of the contract. Administrative permissions can be technically scoped and constrained.

In such systems, insider misappropriation risk is reduced *structurally*, by eliminating the unilateral authority pathways through which misappropriation could occur, rather than relying primarily on supervisory discipline applied after the fact. Detection dynamics also differ materially. Traditional custody relies on periodic account statements and examinations. Vault-based systems provide

[12] Before describing how vault architecture addresses these risks, it is important to distinguish vault custody from self-custody, where the RIA or CPO controls the private keys and asset movement is constrained only by behavioral compliance, fiduciary duty, and after-the-fact enforcement, is precisely the arrangement Rule 206(4)-2 and CFTC Regulation 4.20 are designed to prevent. Vault-based custody is structurally different and should not be understood as a more sophisticated form of self-custody.

The protection does not rest on identifying who holds the receipt token. In the fund context, an argument that the "fund holds the token" would be of limited force if the adviser could simply cause the fund to transfer it to an affiliate for redemption — a straightforward misappropriation vector. The more compelling answer is that the receipt token in a qualifying vault is non-transferable: the smart contract is designed so that the token cannot be moved to any other wallet by the vault owner. No instruction from the adviser, whether given directly, through the fund, or through any affiliate, can cause the vault to transfer the receipt token or redirect assets to any unauthorized destination. The only action available through the receipt token is redemption of assets back to the authorized wallet. The vault smart contract thus functions as the independent custodial counterparty, enforcing segregation in a way that cannot be overridden by the adviser, the fund, or any affiliate of either.

The question the SEC must resolve is therefore not whether vault custody is a permissible form of self-custody — it is not — but whether the structural constraints vault architecture imposes satisfy the rule's protective purposes through a different mechanism than traditional institutional custodianship. They do.

continuous on-chain visibility into balances and transactions, materially reducing detection latency relative to examination-based oversight.[13]

A further and analytically distinct safeguard arises from the mechanics of how cryptographic authority governs withdrawal rights. When a depositor places assets into a qualifying vault, the smart contract automatically issues a "receipt token": a cryptographic instrument that represents the client's proportionate claim against the vault's underlying assets and is redeemable for those assets upon presentation to the vault smart contract. Only the wallet holding this receipt token can initiate a withdrawal or deposit. In the RIA context, the receipt token is issued to the client or to the fund entity on behalf of its investors, not to the adviser.

The practical consequence is that the vault does not need to verify who is requesting a withdrawal or otherwise authenticate the requestor through callbacks, biometric authentication, credentials, or other procedural mechanisms. The smart contract performs a single, unfalsifiable cryptographic check: does the requesting wallet hold the receipt token? If not, the transaction is rejected. This replaces the identity verification layer – which in many human-administered custody systems carries inherent exposure to social engineering, impersonation, and credential fraud, not as a function of any particular institution's practices but as a structural feature of human-executed processes – with a single cryptographic check that cannot be spoofed. A fraudster who successfully impersonates a fund manager or LP receives nothing, because impersonation confers no cryptographic entitlement. Withdrawal authority is determined solely by possession of the receipt token representing the depositor's entitlement to vault assets. The smart contract performs a cryptographic check confirming that the requesting wallet holds this entitlement before permitting redemption. Neither the vault infrastructure provider nor any other participant can transfer or redirect assets absent control of that cryptographic entitlement. This architecture provides a structural answer to the misappropriation concern at the very core of Rule 206(4)-2.

B. Insolvency Risk

Insolvency risk likewise manifests differently. Centralized custodians operate within balance-sheet structures, and even with contractual segregation, bankruptcy proceedings may generate disputes regarding pooling and customer property treatment. Recent digital-asset platform insolvencies have illustrated the practical importance of clearly defined asset segregation mechanisms. In the bankruptcies of Celsius Network, Voyager Digital, and BlockFi, courts were required to determine whether customer crypto assets deposited under various account structures constituted property of the estate or property of the customer, a question that turned on the specific terms of each platform's

[13] Where depositors have legitimate confidentiality requirements (a valid consideration for retail and institutional parties alike), cryptographic privacy tools, including zero-knowledge proofs and selective disclosure mechanisms, can scope that visibility so that balances and transaction history remain verifiable by the account holder and authorized parties, including regulatory examiners, without being exposed to the general public. This preserves the auditability that the Custody Rule requires while accommodating the commercial confidentiality expectations of end users, and does so through cryptographic guarantees rather than contractual ones.

user agreements and the nature of the custody arrangement, not on any settled legal principle. In Celsius, the bankruptcy court ruled that assets held in certain "Earn" accounts were property of the estate, leaving retail customers as unsecured creditors with pro rata claims rather than as owners of segregated property. And in ongoing litigation in In Prime Trust, LLC, a major state-chartered custodian urged the court to provide legal clarity as to the status of customer's crypto assets in insolvency.

Vault architectures that segregate assets at the smart-contract level address this risk through a different structural mechanism: because client assets in a qualifying vault are never on any vault participant's balance sheet and no vault participant holds a proprietary interest in those assets, there is no estate into which client assets could be drawn in an insolvency proceeding. The protection is a function of the vault's architecture rather than of contractual terms, judicial interpretation, or the specific regulatory framework governing any particular custodian. This complements rather than displaces the protections available under existing federal and state-chartered frameworks, including OCC-chartered custodians operating under the National Bank Act, which provide meaningful and legally robust asset protection through a different structural means.

One important clarification is warranted here: qualifying vault architectures do not require that each depositor's assets be held at a unique, individually segregated on-chain address. As a practical and technological matter, depositor assets in a vault are pooled (aggregated within a single smart contract that holds the collective assets of all depositors). What vault architecture provides is not physical separation of assets, but a functional equivalent: cryptographic segregation of withdrawal rights. Each depositor's proportionate entitlement is precisely defined by the smart contract and represented by their receipt token; the contract will enforce that entitlement programmatically, and no other party can reach it.

From a functional perspective, vault custody more closely resembles a separately managed account than a pooled balance-sheet vehicle: assets remain attributable to the client and redeemable directly through the vault contract rather than through an intermediary's discretionary release process. The insolvency protection that vault architecture provides thus rests not on the fiction that assets are physically separated, but on the structural reality that no vault participant holds any proprietary claim against the pool, and each client's entitlement is cryptographically invariant and publicly auditable.

C. Operational Risk

a. Reducing Security Risks

Vault architectures with whitelisted withdrawals also address a distinct and increasingly serious category of operational risk — fraudulent or erroneous transfers to incorrect wallet addresses — through structural rather than procedural means. Any custody model that relies on human authorization of withdrawal instructions must manage the risk that those instructions are falsified or erroneous; a whitelisted vault eliminates that attack vector by restricting transfers to governance-approved addresses at the contract level.

The consequences of transfer errors in digital asset markets are categorically different from their equivalents in traditional finance. A misdirected wire can be recalled and an ACH payment reversed, but digital asset transactions on public blockchains are final and irreversible. There is no recourse, no correspondent to call, no supervisory body with authority to reverse a confirmed on-chain transfer. The attack surface is broad: social engineering of staff (the crypto equivalent of Business Email Compromise fraud, which the FBI consistently identifies as the highest-dollar cybercrime category) exploits falsified withdrawal instructions; address poisoning attacks lead personnel to copy a visually similar but fraudulent address from transaction history; and a single transposed character in a forty-two-character hexadecimal address results in permanent, unrecoverable loss.

A whitelisted vault addresses this structurally: transfers can be restricted to governance-approved addresses, and no single operator, however deceived or compromised, can authorize a transfer to an unvetted address in the moment of execution. The safeguard is structural and prevention-based rather than procedural and detection-based, though it does not eliminate the underlying key security risk that all digital asset custody must manage, addressed separately in Section IV.

b. Enforcing Transfer Restrictions

Finally, vaults also reduce a broad category of operational risk that some centralized custodians encounter in providing services to their RIA and other customers in the enforcement of transfer restrictions that attach to digital assets under securities law, contract, and regulation. Token lockup schedules are the most common example. These customers typically distribute or receive token allocations subject to contractual lockup periods under SAFTs, token purchase agreements, or founder or employee lockup schedules. Some centralized custodians implement these restrictions through internal administrative workflows like manual release processes, compliance sign-off procedures, and internally maintained records which, like any human-administered process, require careful operational execution. The vault architecture makes a different design choice: encoding lockup logic directly in smart contract code so that enforcement is programmatic rather than process-dependent.

The consequences of a manual error in this context can have serious regulatory consequences for RIAs as well as token issuers. Permitting a fund or its LPs to withdraw or trade tokens that remain subject to a lockup can constitute a violation of Rule 144 under the Securities Act, which governs the resale of restricted and control securities and imposes specific holding period requirements before such securities may be distributed into the market. Depending on the circumstances, premature release may also give rise to liability under Rule 10b-5 if the transferee possesses material non-public information at the time of transfer.

Beyond securities law exposure, a premature release is a breach of the SAFT or token purchase agreement itself, which may trigger clawback provisions, unwind obligations, or other remedies in favor of the token issuer. And to the extent the error provides one limited partner with liquidity that others do not receive during the same period, it may also constitute a breach of the adviser's fiduciary duty to treat investors equitably, as well as a violation of applicable fund governing documents. A qualifying vault substantially reduces this category of risk by encoding lockup and vesting logic directly in smart contract code, making enforcement programmatic, automated, and auditable,

which removes the human execution variable that is the proximate cause of most lockup violations. Residual risk, principally from smart contract bugs or unauthorized upgrades, is addressed by the independent audit and governance requirements in Section V.

Token lockup enforcement is only one of several categories of transfer restriction that vault architecture can enforce programmatically for entities subject to the qualified custody and segregation rules. The full range includes (i) Rule 144A and Regulation S restrictions, which limit resale of privately placed securities to qualified institutional buyers or non-U.S. persons during the applicable distribution compliance period: a vault could encode the eligible transferee universe as a whitelist and reject transfers to non-qualifying wallets at the contract level, replacing reliance on DTC legends, transfer agent records, and broker representations; (ii) Regulation D and Section 4(a)(2) holding periods, which restrict resale of unregistered private placement securities until the applicable holding period is satisfied: a vault could make these time-locks self-executing and absolute; (iii) Rule 144(d) and (e) affiliate and control person restrictions, which impose additional holding period and volume limitations on officers, directors, and 10 percent or greater shareholders, currently managed through compliance sign-offs and broker representations, could be directly managed through wallet-level contract logic; (iv) contractual rights of first refusal, ubiquitous in venture and crypto fund deal documents, which require that a holder offer interests to existing investors before transferring to a third party: a vault could enforce the ROFR notice period and exercise window programmatically, making interests transferable to third parties only after the window closes without exercise; (v) co-sale and tag-along rights, which entitle other investors to participate pro rata in a transfer by a major holder: a vault could hold the pending transfer in escrow until the participation window closes; (vi) fund governing document transfer restrictions, which typically limit LP transfers to "permitted transferees" such as affiliates and controlled entities: a vault could directly encode these as whitelist conditions in place of manual fund administrator review; (vii) OFAC and sanctions compliance, which prohibits transfers to designated wallets: a vault with a real-time sanctions-list whitelist enforces this structurally rather than through post-transaction monitoring, directly addressing an enforcement priority of both agencies; and (viii) ERISA prohibited transaction restrictions, which restrict transfers to or transactions with "parties in interest" for funds that have accepted plan assets: the prohibited counterparty list could be directly encodable as a negative whitelist condition.

In each case, vault architecture could convert transfer restriction enforcement from a compliance process dependent on notice, human review, and after-the-fact detection into a structural feature of the asset or vault itself. Any restriction that can be expressed as a rule can in theory be encoded in a smart contract. Vault custody is the first custody model capable of simultaneously holding a digital asset and enforcing the full stack of transfer restrictions that attach to it, without relying on a transfer agent, a compliance officer, or a broker-dealer's gating function.

IV. OPERATIONAL RISKS AND TRADEOFFS

Vault architectures are not without risk. Smart contract vulnerabilities can result in loss of assets. Upgradeable contracts introduce governance risk. Multi-signature arrangements require disciplined operational processes. These risks are real and must be addressed in any framework for recognizing vault-based custody.

One risk specific to receipt token-gated vault architectures warrants direct acknowledgment: the possibility that a receipt token itself is stolen. If a depositor's wallet is compromised and the receipt token transferred to an attacker's wallet, the attacker would acquire the cryptographic entitlement to withdraw the underlying assets. This risk is real and should not be minimized. However, three considerations bear on its significance in the context of a modernized custody framework.

First, this is the same private key security problem that qualified custodians already manage with respect to any digital asset in their custody. It is therefore a familiar risk for which established solutions exist, including hardware security modules, multi-signature wallet arrangements, and institutional key management systems. Second, and more importantly, if the receipt token itself is held in a multi-signature wallet requiring threshold authorization to transfer or redeem, theft requires the simultaneous compromise of multiple independent keyholders, a materially higher bar than stealing a single credential or deceiving a single operator. Third, the receipt token theft scenario represents a meaningfully narrower attack surface than traditional custodial models, where misappropriation can be accomplished through social engineering, spoofed instructions, insider access, or identity fraud without ever needing to compromise a cryptographic key. The receipt token architecture does not eliminate custody risk; rather, it transforms a broad, multi-vector misappropriation problem into a narrower, well-understood key security problem for which the industry has developed robust mitigations. That transformation is precisely what a modernized custody framework should recognize and incentivize.

That said, these risks are qualitatively distinct from insider misappropriation risk, the primary risk Rule 206(4)-2 was designed to prevent. Smart contract logic can be audited ex ante, independent third-party security audits can review code before deployment, governance processes can incorporate time locks and mandatory transparency, threshold cryptography distributes authority across multiple actors, reducing single points of failure, and layered operational controls like kill-switch design, multi-signature governance, business continuity and disaster recovery planning can supplement code-level protections.

The SEC's 2023 Safeguarding Proposal acknowledged that digital assets may require different safeguarding practices given their technological characteristics.[14] The appropriate analytical framework is therefore comparative: not whether vault architectures are risk-free, but whether specific vault architectures, under defined structural conditions, produce a risk profile that addresses the misappropriation and insolvency risks that motivated the rule with comparable or superior effectiveness.

It bears noting that the risks vault architectures present, like smart contract vulnerabilities, governance failures, and key security incidents, are not categorically different in kind from the risks that exist within the traditional qualified custodian framework. Qualified custodians can and do fail: through fraud, negligence, operational failure, or insolvency. Market participants who believed their assets were fully protected by the existing regulatory framework have not always recovered in

[14] 2023 Safeguarding Proposal, 88 Fed. Reg. at 14,673 ("[T]he particular challenges posed by crypto assets may require different safeguarding practices than those applicable to other assets.").

full. The Lehman Brothers bankruptcy illustrated that even highly regulated financial institutions operating within an established supervisory regime can fail in ways that impose losses on clients who reasonably believed their assets were segregated and safe. The question is therefore not whether vault-based custody is risk-free; no custody model is. Rather, it is whether a vault architecture satisfying the structural guardrails in the next section produces a risk profile that is reasonably comparable to the protections available under traditional qualified custodianship, and that addresses the core risks the rules were designed to prevent.

V. RECOMMENDED RULE AMENDMENTS: A GUARDRAIL-BASED COMPLIANCE PATHWAY

Not all vaults are the same. Veda recommends that the SEC's proposed amendments to Rule 206(4)-2 include a defined compliance pathway establishing that an RIA and other registrants required to custody crypto at a qualified custodian affirmatively satisfy the rule's custody requirements with respect to a digital asset when that asset is maintained in a vault-based structure meeting all of the following structural conditions. This pathway should be available only where the vault architecture, taken as a whole, satisfies each guardrail:

(1) No unilateral withdrawal authority. No vault infrastructure provider, adviser, related person, or curator/strategist may possess unilateral authority to withdraw client assets outside predefined contract logic. The core withdrawal and redemption logic must either be immutable or, where upgradeable, subject to mandatory time locks, on-chain transparency, and the constraints in Guardrail (4) below.

(2) Programmatic preservation of redemption rights. Client withdrawal, redemption, and transfer restrictions must be embedded as invariant or time-governed features of the smart contract. This includes the programmatic enforcement of any lockup or vesting schedule applicable to token distributions, or other types of transfer restrictions, which in a qualifying vault must be governed by contract logic rather than manual administrative process, and may only be modified under pre-specified permissions.

(3) Cryptographic segregation of withdrawal rights. Client assets must be segregated at the smart-contract or address level from proprietary holdings of any vault participant. No vault participant may hold a balance-sheet claim against client assets. This guardrail does not require that each depositor's assets be held at a unique, individually segregated on-chain address. Depositor assets in a qualifying vault may be pooled within a single smart contract. What this guardrail requires is cryptographic segregation of individual withdrawal rights: each depositor's proportionate entitlement must be precisely defined by the smart contract, represented by a receipt token or equivalent cryptographic instrument, and enforceable by the depositor independently of any action by the vault operator or any other depositor.

(4) Constrained and transparent governance mechanisms. Any upgrade mechanisms must be subject to mandatory time locks, public on-chain transparency, and prohibitions on retroactive impairment of client withdrawal rights without advance notice and a reasonable opportunity to exit. In addition, where a vault incorporates a curator or strategy manager

with authority to direct deployment of client assets into specific protocols, that authority must be constrained to a defined, on-chain-verifiable set of permitted protocol interactions, enforced through cryptographic validation mechanisms such as Merkle proof verification against a publicly accessible allowlist. This condition ensures that strategy execution authority does not encompass authority to redirect assets to arbitrary addresses, and that the boundary between the curator's instructional authority and the client's assets is enforced by the vault's architecture rather than solely by contractual or compliance-based constraints.

(5) Security operational controls. Code-level structural protections must be supplemented by documented operational controls, including the ability to temporarily pause deposits or withdrawals (for example, to investigate and respond to security incidents), multi-signature governance procedures, and written business continuity and disaster recovery frameworks.

(6) Independent verification and auditability. Vault balances and transaction history must be publicly verifiable on-chain. Smart contracts must undergo independent third-party security audits prior to deployment and following any material upgrade. RIAs relying on this compliance pathway must remain subject to all applicable examination and audit obligations under Rule 206(4)-2.

(7) No affiliated protocol routing. No vault infrastructure provider, adviser, related person, or curator/strategist may operate, control, or hold a material economic interest in any protocol into which vault assets are deployed, or receive compensation from any third-party protocol based on asset routing decisions. This condition is designed to eliminate the affiliated transaction and self-dealing risks — routing incentives, venue-preferencing, and conflicts between an adviser's economic interest and the client's interest — that custody and fiduciary rules are designed to address. It is a structural complement to Guardrail (1)'s prohibition on unilateral withdrawal authority: together, they ensure that neither the ability to improperly redirect assets nor the incentive to do so improperly exists within the qualifying vault arrangement. The compliance pathway should not be available where a vault participant holds an economic interest in an underlying protocol that creates an incentive to route client assets in a manner that benefits that participant over the client.

VI. VAULT CUSTODY AND VAULT INVESTMENT STRATEGY ARE DISTINCT ANALYSES

The existence of a strategy manager or curator exercising investment discretion over vault assets should not, in itself, disqualify a vault from this compliance pathway, provided that such discretion does not encompass unilateral withdrawal authority or the ability to override client redemption rights. The structural separation between custody infrastructure and investment strategy, as with traditional assets, is the feature that makes this compliance pathway analytically coherent and consistent with the rule's existing framework. The SEC should also consider, in future analysis, how this framework applies to vault architectures that incorporate bounded, audited deployment features, so that the pathway remains durable as the technology and its institutional use cases develop.

Veda further recommends that the SEC's proposed amendments expressly state that recognition of a vault structure as satisfying the rule's custody requirements does not constitute SEC approval of any underlying investment strategy, digital asset protocol, or yield-generating activity conducted within that vault. Custody analysis and investment strategy analysis are distinct inquiries under the Advisers Act and possibly other federal securities law statutes, and the amended rule should make that separation explicit.

Two analogies from existing regulatory frameworks illustrate why this structure is analytically coherent. The first is the separately managed account. In a traditional separately managed account, the client holds the account at a qualified custodian and grants the RIA a limited trading authority (the authority to direct transactions on the client's behalf within the account). The RIA cannot withdraw assets to itself; the custodian holds the assets and enforces that constraint contractually and operationally. In a qualifying vault, the same structure is replicated cryptographically: the client holds the receipt token, the smart contract enforces the custodial constraint, and the RIA or curator has strategy authority over vault positions but zero withdrawal authority. The enforcement mechanism changes; the structural relationship does not.

The adviser cannot cause fund assets to be directed to itself, to an affiliate, or to any wallet not authorized under the vault's governance logic — for the reasons described in Section III.A above. The smart contract enforces this constraint regardless of the adviser's instructions, and the structural answer to the misappropriation concern in the fund context is the same as in the individual client context: the vault's architecture forecloses the outcome the rule is designed to prevent.

VII. THE 2026 MOU AND THE CASE FOR COORDINATED SEC-CFTC CUSTODY RULEMAKING

The 2026 MOU establishes a Joint Harmonization Initiative specifically charged with "providing a fit-for-purpose regulatory framework for crypto assets and other emerging technologies" and supporting joint rulemakings in areas of common regulatory interest.[15] Digital asset custody is precisely such an area. The SEC and CFTC regulate many of the same institutional participants, share identical protective objectives with respect to customer assets, and face the same technical constraints in applying legacy custody frameworks to digital assets. A guardrail-based compliance pathway developed jointly would give both agencies' registrants a single coordinated standard: reducing compliance friction for the growing class of dually registered digital asset managers while ensuring both frameworks' protective purposes are met through identical structural conditions.

The SEC and the CFTC have established this principle before. In the 2013 Harmonization Release, the CFTC confirmed that CPOs and CTAs dually registered with the SEC could comply with certain SEC requirements in lieu of parallel CFTC obligations where the SEC's framework achieved comparable regulatory outcomes.[16] Extending that logic to custody and confirming that a vault

[15] 2026 MOU, Art. III, §2(d); SEC-CFTC Joint Harmonization Initiative, https://www.sec.gov/featured-topics/sec-cftc-harmonization-initiative.

[16] Commodity Pool Operators and Commodity Trading Advisors: Harmonization with the Securities and Exchange Commission, 78 Fed. Reg. 52,308 (Aug. 22, 2013) ("2013 Harmonization Release") (establishing

architecture satisfying the structural guardrails in Section V simultaneously satisfies CFTC Regulation 4.20's pool property segregation requirements and CFTC Regulation 1.20's customer fund segregation requirements for FCMs would be a direct and consequential application of the 2026 MOU's harmonization mandate. Veda accordingly recommends that the SEC and the CFTC engage through the Joint Harmonization Initiative to develop a coordinated vault-based custody standard, using the guardrail framework proposed in this letter as a starting point for that work.

VIII. SUMMARY OF RULEMAKING RECOMMENDATIONS

Veda respectfully recommends that the SEC's proposed amendments to Rule 206(4)-2 include the following:

- **A defined compliance pathway for qualifying vault-based architectures.** The amended rule should include a provision establishing that an RIA and other regulated entities required to hold assets at a qualified custodian affirmatively satisfies Rule 206(4)-2 with respect to a digital asset maintained in a vault structure that meets all seven structural guardrails described in Section V of this letter. Satisfaction of all seven conditions should be required; the pathway should not be available on a partial-compliance basis.

- **Express separation of custody analysis from investment strategy analysis.** The amended rule should state that recognition of a vault structure as a qualifying custody arrangement does not constitute SEC approval of any investment strategy, protocol, or yield-generating activity conducted within that vault. Custody status and investment activity remain distinct inquiries under the Advisers Act and possibly other federal securities laws. Likewise, the existence of an investment strategy in a vault should not in itself disqualify a vault from qualified custodian status.

- **A technology-neutral drafting approach.** The compliance pathway conditions should be drafted in terms of functional and structural characteristics like elimination of unilateral withdrawal authority, programmatic preservation of redemption rights, cryptographic segregation of individual withdrawal rights, constrained governance, and independent verification, rather than by reference to specific protocols, token standards, or blockchain networks, so that the framework remains durable as technology evolves.

CONCLUSION

The Custody Rule's objective of protecting client assets from misappropriation, commingling, and insolvency exposure remains important and unchanged, but the mechanisms through which that purpose can be achieved have evolved as technology has advanced, and will continue to do so. A defined compliance pathway for vault-based architectures satisfying enumerated structural guardrails would extend the rule's protective logic to digital asset markets using mechanisms purpose-built for

---

that CPOs and CTAs registered with both the CFTC and SEC could comply with certain SEC requirements in lieu of parallel CFTC obligations where the SEC's framework achieved comparable regulatory outcomes).

those markets' technical architecture, without displacing the existing qualified custodian framework, and without implicitly endorsing any particular investment strategy or protocol.

This is precisely the kind of targeted, principled modernization the Division's agenda statement contemplates. Veda respectfully urges the SEC to include it in any proposed amendments to Rule 206(4)-2, and urges both the SEC and the CFTC to treat coordinated vault-based custody standards as a priority deliverable under the Joint Harmonization Initiative. Veda further submits that a well-constructed compliance pathway for static vault custody will serve as the appropriate foundation for future SEC action addressing more dynamic vault use cases.

Veda appreciates the SEC's and CFTC's consideration and stands ready to provide additional materials, participate in staff discussions, or respond to any questions the staff may have.

Respectfully submitted,

Tuongvy Le
General Counsel
Veda Tech Labs Inc.
Vy@Veda.Tech

cc:
Brian R. Forman
Jason P. Gottlieb
Morrison Cohen LLP