Veda Tech Labs, Inc.

August 4, 2025

Senate Banking Committee
United States Senate
Via Email to: MarketStructure_RFI@banking.senate.gov

Re: Response to Senate Banking Committee Request For Information on Digital Asset Market Structure

Dear Members of the U.S. Senate Banking Committee:

Veda Tech Labs, Inc. ("Veda") appreciates the opportunity to respond to the Senate Banking Committee's Request for Information ("RFI") regarding the recently published draft of the Responsible Financial Innovation Act of 2025 ("RFIA").[1] Veda is a crypto infrastructure company that builds vaults: programmable, non-custodial smart contracts that deploy DeFi strategies to earn yield. We pioneered the BoringVault–the most widely used vault standard in DeFi–an open, modular framework for building secure vault systems that is deployed across multiple protocols and blockchain ecosystems, including Ethereum, Base, Arbitrum, and soon Solana, and currently supports over $4 billion in total value locked (TVL), the total value of the assets currently deployed through our vault infrastructure.

The Committee will no doubt receive responses from parties about why it is critical to protect innovation in DeFi more generally, a position we endorse wholeheartedly. This letter focuses more specifically on the RFI questions that are most critical to programmable, non-custodial DeFi infrastructure such as vaults and the ability of users to benefit from DeFi yield–one of blockchain's most powerful capabilities–with particular attention to asset classification, custody and asset safety, market structure and token intermediation, bank access to DeFi, payment system access, and DeFi innovation policy. Not only are programmable smart contracts like vaults compatible with sound regulation**,** they offer a regulatory substrate: one where constraints and transparency are enforceable by code, and where risk can be managed in ways that are provable rather than presumed.

I. Introduction

Vaults are programmable smart contracts that deploy digital assets into predefined or actively managed DeFi strategies—such as staking, lending, or liquidity provisioning—using transparent, auditable, on-chain logic. They serve a role similar to mutual funds or investment wrappers in traditional finance but remove the need for multiple intermediaries or opaque custody structures.

[1] https://www.banking.senate.gov/imo/media/doc/market_structure_rfi.pdf.

Vaults can be customized for different risk profiles and use cases, and their composable token receipts (often ERC-4626[2] compliant) offer users self-custody, compliance features, and simplified access to complex yield strategies.

By enabling access to native yield directly at the protocol level, vaults unlock one of blockchain's most powerful capabilities: transforming idle capital into productive infrastructure. Their programmability allows for continuous optimization of yield—automatically rebalancing or reallocating based on risk, timing, or yield thresholds—while maintaining transparency and user control. This interoperability and flexibility have made Veda's "BoringVault"[3] architecture the most widely adopted standard in DeFi, prized for its simplicity, auditability, and modularity. Veda's vaults take this even further, allowing a single vault to optimize yield across multiple protocols, assets, and chains simultaneously.

Veda's approach is designed to meet the needs of both crypto-native developers and institutions. While core vault smart contracts remain open source, institutions can customize risk and governance controls using modular plug-ins—enabling features like strategy caps, audit triggers, oracle-based flow restrictions, and more. Because of this flexibility, vaults are increasingly powering DeFi yield strategies for fintechs, exchanges, custodians, and asset managers. Beyond just enabling access to yield, vaults offer a fundamentally better architecture for financial infrastructure: they minimize human discretionary risk, reduce opportunities for manipulation or fraud, provide real-time auditability, and deliver continuous proof of solvency and logic execution. Legislation should be carefully crafted to foster further innovation in this area.

II. Responses to RFI Questions

A. Question 1.f & 1.h – Digital Asset Definitions and Taxonomy

The current regulatory framework lacks sufficient precision to classify the diverse range of digital assets now in use, including programmable financial primitives like vaults. To ensure effective regulation without stifling innovation, we urge the Senate to adopt a taxonomy that reflects both the technical form and economic function of these assets.

i. Vaults vs. Traditional Instruments

Programmable, non-custodial infrastructure such as vaults are fundamentally different from traditional pooled investment vehicles or interest-bearing instruments. A traditional fund manager aggregates client capital and actively deploys it based on discretionary decision-making. In contrast, vaults can be designed as autonomous smart contracts that execute preprogrammed strategies and transparent logic.

[2] *See* https://eips.ethereum.org/EIPS/eip-4626.
[3] *See* https://docs.veda.tech/architecture-overview.

For example, a staking vault that routes ETH into restaking platforms can be programmed to execute a deterministic process: deposit ETH, delegate to whitelisted nodes, accrue yield, and auto-compound or redirect fees as programmed. There is no reliance on a manager's judgment, no reallocation outside of code-based rules, and no off-chain custody or redemption risk.

ii. Functional Asset Classes

We recommend that Congress recognize the following functional asset categories:

- **Liquid Staking Tokens:** Vault strategies often involve liquid staking tokens (LSTs) deployed in DeFi protocols. LSTs are representative tokens that users receive when they stake their crypto on a proof-of-stake blockchain through a liquid staking protocol. They act as a receipt for the staked assets and can be used in DeFi applications while the underlying assets are staked and continue to earn staking rewards.

- **Vault Tokens**: Composable digital receipts issued by vaults that reflect proportional exposure to a specific strategy or portfolio of on-chain actions, often governed by permissioned logic and upgradeable modules.

- **Wrapped Yield Tokens**: Tokens such as stETH or wrsETH that represent claims on underlying staked assets and auto-compound protocol yield, respectively.

LSTs and vault tokens should be treated as programmable infrastructure, not as securities per se, where their value arises from automated exposure to protocol rules. In some cases, LST and vault token holders participate in governance and can propose or vote on changes, which further distinguishes them from passive investors under the *Howey* framework.

iii. Tailored Legal Treatment

A tailored legal regime would recognize that:

- Like staking returns, liquid staking returns are typically based on a user's contribution to securing a decentralized network rather than relying on a third party's managerial or entrepreneurial efforts, and are not securities per se;

- Programmable, non-custodial smart contracts like vaults are code-based logic systems more akin to infrastructure, not financial intermediaries;

- Vault tokens are access credentials to a smart contract–governed strategy, not claims on a pooled enterprise;

- Vault-level disclosures can be standardized via code (e.g., showing yield source, strategy type, risk band) without requiring issuer-based filings;

- Non-discretionary, non-custodial vaults with pre-programmed strategies are not acting as investment advisors nor offering securities;

- A more tailored regulatory approach for vaults deploying actively-managed strategies, recognizing their non-custodial and programmable nature, is appropriate. For example, legislation could authorize the SEC to adopt exemptions or graduated tiers based on the nature of the asset, strategy, and any built-in compliance guardrails.

These principles can both support innovation and mitigate risk. The failure to distinguish between these categories would result in misapplication of legacy regulations designed for fundamentally different financial systems.

B. Questions 10 & 15 – Custody, Proof of Reserves, and Asset Safety

i. The Need to Reframe "Custody" for Programmable Finance

Traditional custody frameworks are premised on the concept of exclusive control over client assets, held in segregated or omnibus accounts. In a programmable blockchain environment, this binary definition (either the user holds the private keys or a custodian does) fails to capture new, secure design patterns like vaults.

Vaults introduce a third model: programmable custody. Assets are held and governed not by a human or institution, but by smart contract logic that enforces verifiable access rules. For example, in a BoringVault deployed by a regulated institution, the following constraints can be applied simultaneously:

- Only KYC-verified wallets may deposit or withdraw;

- Governance actions must be approved by a multisig (e.g., 3-of-5 signers including a compliance officer);

- Strategy allocations are restricted to an allowlist updated via DAO or committee vote;

- Withdrawals are throttled based on real-time asset flows or TVL composition.

This design ensures that no single party, not even the vault infrastructure provider or an active strategy manager, can unilaterally move funds. Execution is decentralized, rule-bound, and subject to real-time public verification.

ii. Programmable Safety Features in Veda Vaults

The BoringVault standard offers modules for:

- **Merkle permissioning**: defining exactly which addresses can access which functions;
- **Strategy guards**: enforcing slippage caps, rebalancing tolerances, or whitelisted yield protocols;
- **Withdraw delay logic**: adding time buffers or rate limits to protect against front-running, liquidity shocks, or governance attacks;
- **Audit triggers**: automated mechanisms that alert users, governance participants, or regulators when certain predefined conditions are met, such as conditions that signal elevated risk, governance changes, or abnormal or suspicious behavior.

Because these features are implemented on-chain, they are not circumventable and do not rely on institutional trust. Any user, auditor, or regulator can independently verify the vault's state, parameters, and constraints at any given time.

iii. Proof of Reserves: Moving from Trust to Verification

Vaults make "proof of reserves" possible. In Veda's architecture:

- The vault token supply is on-chain and traceable;
- The vault asset balance is held by a single smart contract address;
- The vault strategy allocations can be published in real time;
- Third-party oracle feeds can be integrated to provide mark-to-market valuation and detect deviation from solvency thresholds.

This enables true continuous attestation, without the need for periodic accounting reports or auditor certifications. This standard is far stronger than most CeFi "proof of reserve" frameworks, which often rely on unverifiable snapshots, vague attestations, or exclusion of liabilities.

iv. Recommended Regulatory Considerations

We recommend that custody frameworks:

- Recognize programmable custody as a distinct category, separate from traditional custodial and self-custodial models;
- Allow non-custodial vaults to be used by regulated entities (e.g., RIA-managed SMAs or bank-deployed deposit products);
- Provide exemptions or no-action relief to allow experimentation with vault-based models that improve consumer safety.

All of these features potentially offer superior investor protection and market stability than traditional forms of compliance and audit.

C. Questions 11–14 – Market Infrastructure and Token Intermediation

i. Vault Tokens as Core Market Infrastructure

Vault tokens are not just financial instruments—they function as infrastructure rails. Each vault token represents a composable, on-chain claim on underlying assets governed by deterministic rules. As these tokens circulate across centralized exchanges (CEXs), decentralized exchanges (DEXs), custodial platforms, and smart contract protocols, they enable seamless, interoperable access to programmatic yield.

Unlike traditional fund shares or derivative contracts, vault tokens:

- Can be transferred peer-to-peer or used in DeFi without counterparty exposure;
- Retain embedded compliance constraints (e.g., KYC gating, withdrawal limits) across platforms;
- Are auditable in real time, revealing the strategy composition, fee history, and performance of the underlying vault.

This positions vault tokens as more akin to market rails or digital bearer instruments than to traditional securities or derivatives. Their infrastructure-like function warrants a differentiated regulatory approach.

ii. Programmable Intermediation Without Human Intermediaries

In traditional market structure, intermediation involves broker-dealers, clearing agents, custodians, and funds–each adding layers of friction, opacity, and delay. Vault tokens collapse much of this stack into composable, verifiable logic. For example:

- An institutional user may deposit stablecoins into a Veda vault with a smart contract–enforced yield strategy (e.g., allowing only specified functions within specified protocols);

- The vault token can then be listed on a DEX or CEX and priced algorithmically;

- The platform may layer on secondary controls, such as AML screening or whitelisting, without altering the core vault logic.

This enables institution-grade compliance and liquidity without traditional intermediaries. Vault logic becomes the intermediation layer.

iii. Implications for Regulation of Trading Venues and Market Participants

We recommend that the Committee:

- Recognize on-chain infrastructure providers (e.g., vault protocol developers) as distinct from traditional "dealers" or "exchanges." These protocols do not match orders, hold custody, or charge trading fees.

- Direct the relevant regulators to adopt standards akin to Reg SCI for high-impact infrastructure protocols that surpass certain thresholds (e.g., $1B TVL, 1M users, or integrations with national exchanges).

    - These standards could cover uptime SLAs, transparency reporting, vulnerability disclosures, and public governance processes.

- Allow regulated entities to custody and list vault tokens without treating them as full-scope securities, where vaults:

    - Restrict discretionary control,

    - Make yield sources and logic auditable, and

    - Include embedded risk controls.

In addition, Reg SCI–like compliance for protocols could align incentives for security, reliability, and public accountability without imposing additional burdens designed for centralized firms.

iv. Composability and the "Super-Platform" or "Super App" Model

Vault tokens are inherently composable—they can be embedded in wallets, financial apps, synthetic structures, and governance systems. This supports the rise of programmable "super-apps" where:

- Users deposit capital via UI or API;
- Assets are routed through vault logic (e.g., staking, restaking, lending);
- Yield is accrued transparently and distributed to wallet addresses;
- Audit and compliance data is broadcast on-chain.

Veda's SDK is already used to power vaults that can embed directly into custodial banks, DeFi frontends, and retail fintech savings apps.

D. Questions 18–20 – Bank Access to Digital Asset Systems

i. Programmable Vaults as a Bridge Between Banks and DeFi

Banks and trust companies increasingly seek exposure to digital assets to not only to hold them in custody but to offer value-generating products to clients. However, direct participation in DeFi protocols raises complex issues around control, compliance, transparency, and consumer protection. Vaults offer a powerful solution: a programmable interface between traditional financial institutions and decentralized protocols, with built-in compliance and security logic.

Unlike open DeFi smart contracts, Veda's vault infrastructure allows banks to:

- Deploy capital using whitelisted strategies (e.g., LSTs, validator delegation, protocol-stable liquidity pools);
- Gate access through Merkle-based permissioning, ensuring only eligible customers participate;
- Impose real-time withdrawal constraints and risk parameters (e.g., per-wallet limits, strategy allocation caps, slippage tolerances, and time-locks);
- Maintain continuous audit trails that regulators and internal compliance teams can verify directly from the blockchain.

ii. Examples of Bank and Custodian Use Cases

Illustrative applications of programmable vaults in bank and trust environments include:

- **Trust Banks** may deploy staking-as-a-service offerings where client ETH is deposited into a Veda vault governed by a custodian-managed multisig, with restaking logic gated by policy rules (e.g., EigenLayer caps, validator vetting, protocol allowlists).

- **Retail Banks** could offer stablecoin deposit products that route to a vault aggregating yield from tokenized T-bills, lending, or protocol fees, with strict constraints on asset type, wallet eligibility, and duration.

- **Fintech-licensed payment platforms** may embed Veda vaults directly into savings apps, enabling end-users to earn native yield while preserving institutional control, real-time solvency checks, and integrated customer reporting.

iii. Why Vaults are Safer than Direct Protocol Access

The traditional concern with banks interacting with DeFi is unpredictability and lack of oversight. Vaults directly address this by:

- Encoding strategy risk upfront;

- Allowing only pre-approved addresses to deposit or withdraw;

- Supporting continuous monitoring of vault health, composition, and user exposure;

- Disabling governance upgrades or logic changes without multi-party approval.

In contrast to directly calling unverified DeFi contracts, vaults act as controlled gateways, ensuring the bank retains control over the compliance perimeter, while still leveraging the composability and performance of public infrastructure.

iv. Recommended Policy Accommodations

To enable bank participation in programmable DeFi infrastructure, we recommend:

- Allowing regulated banks to deploy capital into non-custodial vaults, where vault logic is verified, immutable, and enforced on-chain;

- Permitting banks to custody vault tokens that represent exposure to these regulated vaults, with appropriate KYC/KYB restrictions;

- Encouraging banking regulators (e.g., OCC, Federal Reserve, FDIC) to develop technical review standards for smart contract-based yield infrastructure;

- Supporting sandbox or pilot programs where state-chartered or federally-regulated banks can test vault-based yield products in a controlled environment.

E. Question 21 – Access to Federal Payment Systems

i. The Case for Tiered, Risk-Based Access

As financial services evolve, digital asset firms increasingly require access to core payment infrastructure, particularly the Federal Reserve's master accounts and real-time settlement systems. While granting such access raises valid prudential concerns, not all digital asset actors pose the same risk profile. A one-size-fits-all exclusion risks entrenching intermediaries and discouraging innovation.

Vault-based infrastructure offers a new way to evaluate risk not based on entity type, but on operational integrity. Vaults allow the enforcement of capital requirements, solvency rules, and flow controls directly in smart contract logic, making them well-suited to serve as trusted infrastructure for firms that may not fit within the traditional banking perimeter.

The Federal Reserve's 2022 guidelines for evaluating master account access (87 Fed. Reg. 51099[4]) lay out a risk-based framework centered on transparency, operational integrity, and systemic safety. While designed for traditional financial institutions, these principles can apply to blockchain-native systems like non-custodial vault protocols. Vaults, built on open standards like ERC-4626,[5] offer real-time, on-chain transparency into assets, strategies, and governance. Every user action, yield deployment, and fee change is publicly auditable, enabling a level of disclosure and control that exceeds what's available in conventional financial infrastructure.

Critically, vault protocols manage risk not through opaque processes or discretionary oversight, but through verifiable code. Features like circuit breakers, strategy gating, and concentration caps could be enforced programmatically, reducing operational and cybersecurity risk. These systems can also embed safeguards such as timelocks, multisig permissions, and automated de-risking triggers. By satisfying the spirit of the Fed's transparency and control requirements through public, auditable smart contracts, vaults demonstrate how compliance can be reimagined as code. Future regulatory frameworks could recognize programmable infrastructure as a legitimate and often superior form of risk management.

[4] *See* https://www.federalregister.gov/documents/2022/08/19/2022-17885/guidelines-for-evaluating-account-and-services-requests.

[5] *See* https://ethereum.org/en/developers/docs/standards/tokens/erc-4626/.

ii. Programmable Risk Controls for Stablecoin and Settlement Vaults

A stablecoin issuer or tokenized cash platform integrated with vaults could:

- Require that minting and redemption occur only via KYC'd, allowlisted addresses;
- Enforce over-collateralization ratios or capital buffers on-chain, verifiable by any observer;
- Use oracle-based real-time solvency attestations, allowing both users and regulators to audit balance sheets continuously.

These safeguards go beyond what is required in traditional money market fund operations or custodial stablecoin models, and they are provable rather than reliant on attestations, audits, or discretionary judgment, reducing compliance costs and increasing trust, in contrast to opaque reserve structures that may mask mismanagement or fraud.

iii. Vaults as Compliant Bridges Between On-Chain Assets and Off-Chain Payments

For nonbanks (e.g., fintechs, trust companies, or stablecoin issuers), vaults could serve as:

- Real-time asset encumbrance mechanisms: ensuring assets held on-chain match liabilities in circulation;
- Settlement engines: where a Fedwire or RTP payment can trigger a token mint or redemption on-chain;
- Compliance layers: providing built-in AML/KYC logic, circuit breakers, and withdrawal authentication.

This makes them ideal candidates for conditional access models, where a firm's vault architecture could be reviewed by the Federal Reserve as part of a technical onboarding and monitoring process. For example, a hypothetical "payment settlement vault" could allow USD inflows and token issuance linked via oracle-verified processes.

iv. Recommendations for Policy Design

We propose the following framework to expand safe access to the Fed's payment systems for vault-integrated digital asset platforms, perhaps spearheaded by the OCC's Office of Financial Technology:

- **Risk-based tiering**: Allow nonbank entities with vault-mediated infrastructure and audited smart contracts to apply for limited or conditional access (e.g., for settlement purposes only).

- **Infrastructure review track**: Create a supervisory mechanism for evaluating whether vault design meets real-time solvency, withdrawal throttling, and AML/KYC enforcement standards.

- **Sandbox support**: Encourage pilot programs with Fed regional banks and trust institutions to test vault-based payment gateways, particularly for dollar-backed stablecoins or tokenized deposits.

- **Interoperability protocols**: Develop Fed-compatible APIs or event-driven messaging standards that vaults could integrate for synchronization with FedNow or RTP rails.

F. Questions 23, 25, and 26–33 – Innovation, Yield, and DeFi-Specific Regulation

i. Vaults as a Safer, More Transparent Foundation for On-Chain Innovation

The past decade of DeFi innovation has shown both immense promise and novel challenges. While composable smart contracts and open liquidity systems have enabled broad access and experimentation, they have also introduced risk: unaudited protocols, hidden leverage, and over-financialization have led to spectacular failures.

Vaults represent a shift toward secure, modular, programmable financial infrastructure. They are a response to DeFi's early excesses: by embedding strategy constraints, permissioning, circuit breakers, and automated reporting directly into vault logic, builders can create products that are safer by design, without sacrificing openness or innovation.

ii. The Importance of Yield Differentiation

Not all yield is created equal. Some yield arises from:

- Lending and borrowing (e.g., Aave, Morpho);

- Protocol-level activity (e.g., staking rewards, validator fees, sequencer rebates, trading fees for liquidity providers);

- Economic coordination (e.g., MEV smoothing, fee routing, liquidity incentives).

Vaults that restrict themselves to native yield strategies enforced via code should not be regulated as interest-bearing deposit accounts or pooled investment vehicles. Instead, they should be treated as infrastructure layers, akin to money transmission logic or automated trust arrangements. Functionally similar analogues in the securities world are sweep accounts or SMA structures.

iii. How Innovation Can Be Safely Encouraged Through Programmatic Guardrails

The BoringVault standard includes native support for:

- Withdrawal queues (similar to an unstaking queue) and time-locks, limiting exposure to governance attacks and hacks;
- Risk bands, defining how much capital can be allocated to any one protocol or asset class;
- Public audit interfaces, exposing strategy weights, fee history, and reserve composition.

By designing safety into the vault layer itself, innovation can proceed with built-in risk management. Code standards or certification could arise from industry self-regulatory organizations or regulators.

iv. Sandbox and Safe Harbor Recommendations

To support continued DeFi innovation and vault experimentation, we recommend:

- A regulatory safe harbor for smart contract protocols that:
    - Do not take custody of depositor funds;
    - Operate with immutable or governance-restricted code;
    - Disclose strategy logic and constraints on-chain;
    - Submit to public auditing and reporting standards.
- A dedicated vault innovation sandbox, perhaps led by FinCEN, the CFTC Lab, or a joint agency task force, focused on:
    - Developing baseline compliance modules (e.g., AML logic, KYC oracles);

    - Creating testnets with simulated user flows or test vaults on chain using small amounts of funds;
    - Piloting risk disclosure standards for vault tokens.
- Recognition of vault tokens as infrastructure, not financial products, when:
    - No counterparty risk exists;
    - Yield arises from protocol-level rewards;
    - Strategy logic is immutable or transparently governed.

We recommend including a new category of "native yield vault" in statute or regulation, distinct from pooled funds or securities.

v. Cross-Chain Interoperability and Global Standards

Veda's vaults operate across more established blockchain networks like Ethereum as well as emerging ecosystems like MoveVM. Yet regulation remains jurisdiction-bound and chain-specific. If a vault token is recognized in one regime but restricted in another, composability, and thus safety and reliability, breaks down.

We urge Congress to:

- Recognize chain-agnostic standards (including but not limited to ERC-4626, ERC-6909) for composable yield assets;
- Engage with global regulators (e.g., UK FCA, MAS, MiCA supervisors) to harmonize treatment of non-custodial infrastructure;
- Encourage the development of international interfaces for on-chain auditability, such as metadata standards, risk labeling, and permissioning protocols.

Congress should call for international coordination (e.g., IOSCO DeFi Policy Recommendations, BIS innovation hubs) with the U.S. leading this charge.

III. Conclusion

Vaults offer a transformative opportunity to upgrade financial infrastructure with embedded safety, transparency, and programmability. As Congress considers how best to regulate digital asset markets, we urge policymakers to recognize the potential of programmable smart contract infrastructure like vaults to deliver both innovation and consumer protection, and to preserve access to DeFi yield. By tailoring regulatory frameworks to reflect the capabilities of programmable infrastructure, the United States can foster a responsible and competitive digital financial system. We appreciate the Committee’s leadership on this issue and stand ready to support further dialogue and technical engagement as needed.

Respectfully submitted,

Tuongvy Le

General Counsel, Veda Tech Labs, Inc.

https://veda.tech