August 1, 2025

Chairman Tim Scott, Senator Lummis, Senator Hagerty, and Senator Moreno
Committee on Banking
United States Senate
Via email to: MarketStructure_RFI@banking.senate.gov

Re: Digital Asset Market Structure Request for Information, Questions related to Decentralized Finance

Dear Members of the Senate Committee on Banking,

We write in response to the Committee's Digital Asset Market Structure Request for Information (RFI) and recently published discussion draft of the Responsible Financial Innovation Act of 2025 (RFIA). As Decentralized Finance (DeFi) builders, investors, and advocates, we at the DeFi Education Fund, a16z Crypto, Jito Labs, Inc., Jump Crypto, Multicoin Capital, Paradigm, Solana Policy Institute, Uniswap Foundation, Uniswap Labs, and Variant Fund, provide our perspective in response to the Committee's questions directly relevant to DeFi.

DeFi is a rapidly growing and innovative industry. According to the President's Working Group Report on Digital Assets (the "PWG Report"), DeFi utilization is on the rise, with the total number of protocols and services expanding rapidly.[1] The PWG writes that digital assets and blockchain technology will lead to "a more open and efficient financial system for all" and that American entrepreneurs who "pioneer new industries using these technologies deserve both clarity on the policies that affect their efforts and praise for the progress they have made."[2]

[1] President's Working Group Report on Digital Asset Markets (hereinafter PWG Report), *Strengthening American Leadership in Digital Financial Technology*, at 20 (July 30, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf ("As of July 2025, total volume locked (TVL), a statistic measuring total dollar value of digital assets locked or committed to DeFi protocols, decentralized applications, and other blockchain-based platforms, approached $130 billion. The Report also notes that private surveys show that more than 1 in 5 Americans—over 68 million people—own cryptocurrencies, and 'digital assets and blockchain technologies can revolutionize not just America's financial system, but systems of ownership and governance economy-wide.'").

[2] PWG Report at 5.

As the Committee rightfully recognized in its Crypto Market Structure Principles, DeFi presents distinct characteristics and risks compared to traditional, centralized finance.[3] "Legislation should not apply principles designed for centralized firms to decentralized protocols," but instead "should recognize the different risks and benefits between centralized firms, decentralized finance protocols, and non-custodial software platforms." Several members of the House of Representatives, including drafters of the House version of market structure legislation (the CLARITY Act) echoed the view that "DeFi is different"[4]—specifically because "DeFi developers do not take custody of user assets, nor do they control user assets"[5]—and should therefore "be treated differently from the centralized, custodial intermediaries"[6] that market structure legislation is designed to regulate.

The PWG also acknowledges the unique value of DeFi technology, noting that "By embracing and supporting the option of DeFi for investors, policymakers can help position the United States as a leader in the global crypto economy. Encouraging the development of regulatory frameworks that balance innovation with security will pave the way for a robust financial future."[7] In a speech following release of the Report, Chair Paul Atkins of the Securities and Exchange Commission (SEC) echoed this sentiment, saying that "[i]t is essential that any crypto asset regulatory market structure create a path for software developers to unleash on-chain software systems that do not require operation by any central intermediary."[8]

---

[3] U.S. Senate Committee on Banking, Housing, and Urban Affairs, *Market Structure Principles for Digital Assets* (June 24, 2025), https://www.banking.senate.gov/imo/media/doc/6-24-25_market_structure_principles.pdf.

[4] Rep. Glenn Thompson, remarks in House debate on digital asset regulation, 171 Cong. Rec. H3403 (daily ed. July 17, 2025) (statement of Rep. Thompson).

[5] Rep. French Hill, remarks in House debate on digital asset regulation, 171 Cong. Rec. H3397 (daily ed. July 17, 2025) (statement of Rep. Hill).

[6] Rep. Glenn Thompson, remarks in House debate on digital asset regulation, 171 Cong. Rec. H3403 (daily ed. July 17, 2025) (statement of Rep. Thompson); *see also* Rep. French Hill, remarks in House debate on digital asset regulation, 171 Cong. Rec. H3397; Whip Emmer, remarks in House debate on digital asset regulation, 171 Cong. Rec. H3399.

[7] PWG Report at 57.

[8] Paul S. Atkins, Chairman, Sec. & Exch. Comm'n, *American Leadership in the Digital Finance Revolution*, (July 31, 2025), https://www.sec.gov/newsroom/speeches-statements/atkins-digital-finance-revolution-073125 ("Decentralized finance software systems—like automated market makers—facilitate automated, non-intermediated financial market activity. Federal securities laws have always assumed the involvement of intermediaries that require regulation, but this does not mean that we should interpose intermediaries for the sake of forcing intermediation where the markets can function without them.").

Consistent with these insights, successful market structure legislation should incorporate four critical principles:

- A fundamental distinction between, on the one hand, software developers, the permissionless software they create or the technical activities in which they or others are involved, and, on the other hand, centralized intermediaries;
- Clear definitions for centralized intermediaries who are required to register rather than deferring such definitions to agencies;
- Definitive criteria to evaluate the absence of unilateral and independent control over decentralized systems and user assets, rather than delegating that critical task to agencies; and
- Blockchain technology itself should be treated as neutral infrastructure, akin to the internet, rather than as entities subject to ill-suited registration or compliance obligations.

With thoughtful market structure legislation, the United States is poised to establish itself as a global leader in digital asset markets and innovation.[9] We commend the Committee's inclusion of some protections for software developers, such as the Blockchain Regulatory Certainty Act (BRCA), and protections for persons to self-custody their own assets. We encourage Congress to adopt certain additional safeguards for software developers, as described in this submission. And finally, with additional regulation on the horizon, Congress should also mandate that the SEC consider promoting innovation when it conducts rulemakings or issues guidance, as suggested in RFI Question 30. A dynamic, forward-looking, and flexible regulatory framework will ensure that builders of decentralized technology can thrive in the United States.

Market Structure Laws Should Be Technology-Neutral (Response to RFI Question 1(f))

Congress should provide clear statutory guidance about the status of the technology that supports the operation of decentralized blockchain networks. Technical activities such as running consensus algorithms, validating transactions, executing smart contracts, and maintaining protocol software are essential to network operations. Critically, they do not involve custody of or discretionary control over user assets, or access to material non-public information, and should not be regulated as if they do.

[9] *See also* Atkins, *American Leadership in the Digital Finance Revolution*, *supra*. ("Yesterday, the President's Working Group on Digital Asset Markets released the PWG Report with clear recommendations for the SEC and other federal agencies to build a framework to maintain U.S. dominance in crypto asset markets. This report is the blueprint to make America first in blockchain and crypto technology. The President said last week that he wants 'the entire world running on the backbone of American technology.' I stand ready to help get that job done.").

Effective legislation must be technology-neutral while utilizing consistent, unambiguous terminology.[10] Congress should avoid codifying specific architectural models or design choices that may benefit certain participants while excluding others. Legislating through the lens of particular technologies risks entrenching legacy systems, which could stifle competition and limit future developments. A sound regulatory framework should focus on solving actual risks to consumers without being so broad as to sweep new innovations into inapt financial regulatory regimes.

While legislation should remain technology-neutral as to the merits of distributed ledger technologies, it still must accurately describe such technologies. For example, in addition to the definitions of "distributed ledger" and "distributed ledger service" currently in the discussion draft, terms like "distributed ledger system" or "decentralized computing network" should also be explicitly defined and used uniformly to describe permissionless blockchain environments, technical infrastructure, and the associated applications. This overall approach aligns with the principles of President Trump's *Executive Order on Strengthening American Leadership in Digital Financial Technology* (EO 14178), which emphasized clarity, innovation, and the importance of technology-neutral legislation to preserve U.S. leadership in digital financial infrastructure.[11] It also aligns with the PWG Report call to Congress and federal regulators to approach certain DeFi activities on a technology-neutral foundation.[12]

---

[10] "Technology-neutral" legislation will establish principles-based standards focused on core underlying risks—standards that could be met even where new or evolving technologies are involved. This is especially relevant with respect to digital assets and DeFi, so that legislation can fulfill its mission without stifling innovation in this burgeoning industry. Fit-for-purpose legislation should be tailored to the realities of blockchain technology and acknowledge its value proposition, and should protect innovation and the unaffiliated network of participants who develop or operate the technology.

[11] Exec. Order No. 14178, *Strengthening American Leadership in Digital Financial Technology* (Jan. 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology (emphasis added) (stipulating that federal agencies should "provide regulatory clarity and certainty built on technology-neutral regulations, frameworks that account for emerging technologies, transparent decision making, and well-defined jurisdictional regulatory boundaries").

[12] PWG Report at 52 ("The CFTC should consider using its rulemaking, interpretative, and exemptive authority under the Commodity Exchange Act (CEA) to provide clarity on the applicability of various CFTC registration requirements to DeFi activities, smart contract protocols, or decentralized autonomous organizations (DAOs) consistent with technology-neutral principles."), at 74 ("The Banking Agencies should ensure that existing and new best practices or guidance on risk management and bank engagement are technology-neutral and that expectations regarding offering banking services do not discriminate against lawful businesses solely due to their industry").

DeFi Developers and Technology Should Be Protected From Inappropriate Regulation Meant For Intermediaries (Response to RFI Questions 2, 12, 17c and 26)

Decentralized Technology and Software Developers Should be Treated Differently Than Intermediated Finance

As suggested in the Committee's Crypto Market Structure Principles, software developers of non-custodial protocols and systems, who do not have customers, must be treated distinctly under digital asset market structure legislation. Blockchain technology makes it possible for people to transact peer-to-peer while maintaining custody and control of their own digital assets, which is in contrast to the traditional financial system, where centralized intermediaries manage assets, typically take custody, and take action *on behalf of* customers.

This understanding has already been codified into law. Earlier this year, bipartisan supermajorities in both Chambers of Congress recognized the fundamental differences between the regulation of DeFi and intermediaries by passing House Joint Resolution 25, nullifying the digital asset reporting obligations imposed by the Internal Revenue Service's (IRS) Broker Rule.[13] The legislation, which was swiftly signed into law by President Trump, recognizes that regulations written for financial intermediaries, who custody customer assets and exercise control over those funds, should not and cannot apply to non-custodial software developers or DeFi technology itself. As echoed in the Report, "Congress should enact legislation affirming that individuals can custody their own digital assets without a financial intermediary and engage in lawful peer-to-peer transactions using those assets."[14]

This coalition is grateful that the Senate Banking Committee emphasized in its principles for market structure that "legislation should recognize the different risks and benefits between centralized firms, decentralized finance protocols, and non-custodial software platforms."[15] This understanding is shared by regulators as well; it was reaffirmed by SEC Chairman Paul Atkins in his remarks at the Crypto Task Force's recent roundtable on DeFi, where he noted that "most current securities rules and regulations are premised upon the regulation of issuers and

[13] Pub. L. No. 119-5, 139 Stat. 48. *See also* President Trump Formally Voids the IRS's "DeFi Broker" Rule and Signs The United States' First Crypto Legislation, DeFi Educ. Fund (Apr. 10, 2025), updated Apr. 13, 2025, https://www.defieducationfund.org/post/policymakers-protect-defi-president-trump-signs-and-formally-voids-the-irs-s-defi-killing-broker.

[14] PWG Report at 6.

[15] Senate Banking, Hous., & Urb. Aff. Comm., *Crypto Market Structure Principles*.

intermediaries, such as broker-dealers, advisers, exchanges, and clearing agencies. The drafters of these rules and regulations likely did not contemplate that self-executing software code might displace such issuers and intermediaries."[16]

Legislation Should Clearly Define Covered Registrants

In market structure legislation, decentralized trading protocols, front-end interfaces, and related non-custodial technology should not be scoped into securities or commodities registrant definitions. The RFIA discussion draft does not provide definitions for registrants such as "brokers," "exchanges," or "dealers."[17] The Senate's final product should carefully define all such registrants and not leave such definitions for agencies to fill in in rulemaking in a way that could inappropriately scope in developers of non-custodial software or technology, as they have attempted to do in recent years.[18] Yet, leaving the definitions of covered registrants open to potentially overly broad interpretation would undermine the Senate Banking Committee's market structure principle that *"regulatory authority should be clearly allocated in statute, preventing an all-encompassing regulator from emerging*."[19]

Protections for Developers and Infrastructure are Essential

Market structure legislation should be written so that blockchain technology is appropriately treated as infrastructure, and so that developers building neutral infrastructure—who do not have custody or control of user funds—are not treated as intermediaries, financial institutions, or other registrants. While the United States has been a

[16] Paul S. Atkins, Chairman, U.S. Sec. & Exch. Comm'n, *Remarks at the Crypto Task Force Roundtable on Decentralized Finance: DeFi and the American Spirit* (June 9, 2025), https://www.sec.gov/newsroom/meetings-events/defi-american-spirit.

[17] *See* RFIA Section 2.

[18] *See, e.g.*, Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales, 89 Fed. Reg. 106928 (Dec. 30, 2024) (final regulations defining "digital asset middlemen"—i.e., DeFi trading front-end service providers—as brokers obligated to report gross proceeds on Form 1099-DA for digital asset transactions effected on or after Jan. 1, 2027); *Crypto Freedom Alliance of Texas v. U.S. Securities & Exchange Commission*, No. 4:24-CV-00361-P (N.D. Tex. Nov. 21, 2024) (vacating SEC's February 2024 "Dealer Rule" as exceeding statutory authority and arbitrarily extending the dealer definition in a way that could encompass DeFi actors such as automated protocol developers and liquidity providers); Withdrawal of Proposed Regulatory Actions, 90 Fed. Reg. 25531 (June 17, 2025), https://www.sec.gov/files/rules/final/2025/33-11377.pdf.

[19] Senate Banking, Hous., & Urb. Aff. Comm., *Crypto Market Structure Principles.*

leader in development of blockchain technology, the total share of open-source software developers in the United States dropped from 25% in 2021 to 18% in 2025.[20] As the Report recently stated, "Reversing the decline of blockchain development in the United States is central to the goal of making America the crypto capital of the world."[21]

Important protections for software developers and technology were recently advanced in the bipartisan supermajority passage of the CLARITY Act, with 294 members voting in favor of protecting software developers and infrastructure.[22] These protections include clarifying the treatment of certain non-controlling blockchain developers through the BRCA (Section 109), self-custody protections (Section 105), and the protections for software developers and other non-custodial service providers in Sections 309 and 409. It is imperative that the Senate's draft build upon and strengthen these protections.

In order to achieve this objective, we appreciate and firmly support the inclusion of the bipartisan BRCA.[23] The BRCA, as introduced in the House by Majority Whip Tom Emmer, and cosponsored by Representatives Torres and Gottheimer, protects developers of "blockchain services," who do not custody or control user assets, from being improperly classified as financial intermediaries under the Bank Secrecy Act (BSA).[24] The BRCA also affirms the position of the Financial Crimes Enforcement Network's 2019 Guidance on Convertible Virtual Currencies, which concludes that those who do not exercise "total independent control" over user

---

[20] PWG Report at 25.

[21] PWG Report at 25.

[22] U.S. House of Representatives, Roll Call Vote No. 199 on H.R. 3633, 119th Cong., 1st Sess. (July 17, 2025) (294 yeas, 134 nays), https://clerk.house.gov/Votes/2025199.

[23] DeFi Education Fund, *Updated: Joint Statement from Crypto Policy Organizations on Blockchain Regulatory Certainty Act* (June 5, 2025), https://www.defieducationfund.org/post/updated-joint-statement-from-crypto-policy-organizations-on-blockchain-regulatory-certainty-act.

[24] *Blockchain Regulatory Certainty Act*, H.R. 3533, 119th Cong. (2025) (introduced May 21, 2025), https://www.congress.gov/bill/119th-congress/house-bill/3533. The BRCA defines a "blockchain service" as "any information, transaction, or computing service or system that provides or enables access to a blockchain network by multiple users, including specifically a service or system that enables users to send, receive, exchange, or store digital assets described by blockchain networks." And the term "blockchain network" "means any system of networked computers that cooperates to reach consensus over the state of a computer program and allows users to participate in the consensus-making process without the need to license proprietary software or obtain permission from any other user."

assets should not be improperly classified as money transmitters.[25] Likewise, and as discussed in detail below, the Senate should continue to protect self-custody in market structure legislation.

The Report recognized the importance of these protections, stating, "Congress should codify principles regarding how control over an asset impacts Bank Secrecy Act (BSA) obligations, particularly for money transmitters. A software provider that does not maintain total independent control over value should not be considered as engaged in money transmission for purposes of the BSA."[26] This point was further underscored with the PWG's policy recommendation that "Without the ability to exercise control over user assets or funds, a software application may not transmit money or exchange currency, and therefore might not be subject to the BSA as an MSB. Importantly, without control, software applications generally lack the ability to misappropriate user assets."[27]

In addition to the BRCA and self-custody, the Senate should explicitly protect developers who develop and publish software, as well as non-custodial service providers, from the regulatory regime set forth in the legislation. While CLARITY Sections 309 and 409 were intended to provide such protections, those sections were somewhat inaptly titled "Exclusion for Decentralized Finance Activities," even though they actually described developer and service provider activities critical for creating and maintaining blockchain networks in general. Going forward, the Senate can and should properly protect activities carried out by developers to create and maintain blockchain infrastructure and by service providers to support such networks. We firmly encourage framing these provisions as "Protections for Blockchain Infrastructure and Software Developers."

"Protections for Blockchain Infrastructure and Software Developers" should ensure that a person shall not be subject to the regulations promulgated under the bill based only on the person directly or indirectly: relaying or validating blockchain transactions; providing computing power, bandwidth, or similar network resources; providing software user interfaces to access blockchain data; developing or publishing blockchain systems, protocols, or liquidity pools; or creating tools like wallets that help users store, manage, or secure digital assets or private keys, among other

---

[25] FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[26] PWG Report at 108.

[27] PWG Report at 146.

things. It should also extend protections for developers from being inappropriately prosecuted as money transmitters under criminal law provision 18 U.S.C. 1960. Last, the section should preempt states from taking conflicting positions with the federal protections in the bill. Federal preemption is discussed in detail below, in response to RFI Question 35.

As the Report stated, "American entrepreneurs and software developers should have the liberty, and regulatory certainty, to upgrade all sectors of our economy using these technologies."[28] The Senate must play its part in solidifying America's position as the crypto capital of the world by recognizing the differences between DeFi and centralized intermediaries, including the BRCA, and passing robust protections for blockchain infrastructure and software developers.

Congress Should Define Criteria to Assess "Control" Over Digital Networks and Related Digital Assets (Response to RFI Question 6(a))

Congress should define in market structure legislation how the absence of unilateral and independent control over digital networks and related digital assets should be assessed. Rather than leave such a critical framework to future rulemaking, Congress should ensure that there are appropriate metrics to determine whether a system is, in fact, decentralized. As of now, the discussion draft characterizes this analysis as "common control by related persons" and mandates that the SEC promulgate rules that would further define "common control" criteria. However, it is our view that, for token holders, developers, and users in the DeFi and digital asset spaces to thrive, they need durable clarity: long-term regulatory certainty that only legislation can provide.

A control-based test is meant to account for the risks traditionally addressed by the securities laws, such as information asymmetries and conflicts of interest. These risks are mitigated when token holders no longer depend on privileged parties with greater powers or superior access to information. However, the term "common control" alone, without further explanation, inadequately describes the type of centralized group that creates such risks. The SEC could construe this term overbroadly to include a group of unaffiliated parties that reach consensus through a public process and thereby together control the rules of a blockchain system, even though that group does not pose any centralization risks to users.

We suggest that the proper conception of a control test is the "lack of unilateral and independent control," or other language that clarifies that no centralized group of people or entities are able to unilaterally effect the kinds of decisions or changes described in the list

[28] PWG Report at 6.

below. The proposed metrics below align with what the PWG stated in the Report, that "Policymakers should embrace decentralized finance as an option for individuals and investors and appreciate the extent to which a given software application: (i) exercises "control" over assets; (ii) is technologically capable of being modified; (iii) operates with a centralized structure or management; and (iv) is logistically capable of complying with current regulatory obligations when determining its regulatory treatment."[29] This list is similar to the maturity criteria in Section 205 of the CLARITY Act, which outlines when a blockchain system may be deemed "mature" and free from centralized control.[30]

- Maximum Transparency: The deployed instance of the code is publicly available and auditable, the network's functionality is clearly described and publicly disclosed, any existing permissions—such as the ability to run, modify, or redistribute the source code, upgrade the protocol, or delegate powers to others—are clearly described and publicly disclosed, and any known insiders who retain significant ownership stakes in the network are identified.

- Permissionless: No person or group of persons under common control has the ability to unilaterally exclude, block, or approve persons or entities from (i) using or modifying the network, (ii) participating in consensus mechanisms, (iii) building software that provides access to the network, or (iv) otherwise interacting with the network, its underlying technology, or the associated digital asset.

- Non-Custodial: Users of the network retain custody, possession and control over their digital assets. No person or group of persons under common control maintains custody over third-party assets without consent. Put differently, no person or group of persons has the unilateral legal authority or technical ability to initiate transactions involving digital assets without the approval, consent, or direction of the asset holder or an authorized third party.

- No Centralized Network Control: No person or group of persons under common control should be able to unilaterally modify the network unless that authority has been delegated by an unaffiliated, dispersed group of token holders or validators within the consensus mechanism, which shall retain the ultimate authority to revoke such delegation. If an initial development team, or any person, entity or group of related persons under common control, has unilateral authority to restrict or prohibit others from using, earning or transmitting the token, deploying software that uses or integrates with the technology, or participating in governance of the technology, then

[29] PWG Report at 6.

[30] *See* CLARITY Act, H.R. 4763, 119th Cong. § 205 (2025) (defining "mature blockchain system" as one not subject to centralized control and establishing certification, review, and rebuttal processes based on criteria such as decentralization, programmatic operation, and distributed ownership).

they would be deemed to have control. The Commission should ensure that "network control" is defined in a way that permits restrictions that are non-discriminatory, transparent, and do not impose unreasonable barriers to participation so long as they do not conflict with the other principles included here.

- Fully Automated Transactions: The network operates continuously without human intervention and functions according to transparent, pre-established rules encoded in its source code. Transactions are executed, validated, and enforced automatically without human intervention.

- No Retained Economic Authority: The economics of the network may be modified but are not dependent on any person or group of persons under common control. No changes to economic drivers are possible unless such authority and ability has been delegated by an unaffiliated and dispersed group of token holders or validators within the consensus mechanism.[31]

In short, Congress has the tools it needs to define clear criteria to determine when a network lacks unilateral and independent control and does not need to rely on an agency's expertise to do so. Leaving an agency with wide latitude to do rulemaking on this point (for example, by including language such as that in Section 103(b)(2)(E), allowing the SEC to include "any other factor that the Commission determines relevant to assessing control and independence with respect to the digital network") does not provide the industry with sufficient certainty as to what the law is; it risks creating unjustified restrictions and discouraging legitimate activity by developers and ecosystem participants.

Self-Custody Protections for All US Persons Is Essential (Response to Question 15(g))

A core innovation of blockchain technology is that it provides users with the ability to securely custody and control their own digital assets. "Self-custody" is a critical aspect of DeFi and the broader digital asset ecosystem because it empowers users to retain independent control of their own assets through the use of cryptographic private keys in a non-custodial wallet,[32]

---

[31] DeFi Education Fund, *Token Safe Harbor Guiding Principles* (Apr. 18, 2025), https://www.defieducationfund.org/_files/ugd/84ba66_04e7a0f6cd7e4c95b47b08e0db16abb0.pdf (proposal submitted to SEC Crypto Task Force).

[32] DeFi Education Fund, *Comment on the Proposed Rule on Electronic Fund Transfers Through Accounts Established Primarily for Personal, Family, or Household Purposes Using Emerging Payment Mechanisms, CFPB-2025-0003* (Mar. 31, 2025), https://www.defieducationfund.org/_files/ugd/84ba66_1354e55a26fb4bd2af5167c4343ddedf.pdf (explaining that each self-custody wallet is associated with a unique pair of cryptographic keys: a public key, which serves as an address for the wallet, and a private key, which grants exclusive control over the assets within the wallet; that transactions are signed locally using the private key and broadcast to the

eliminating the need to trust third-party intermediaries like banks or custodial exchanges. We are grateful to the Committee for including self-custody protections similar to those in the Keep Your Coins Act, as introduced by Senators Budd and Lee,[33] in the discussion draft.

Clear, affirmative, and enforceable protections for self-custody are essential for all U.S. persons. Any effort to establish a regulatory framework for digital assets in the United States must prioritize protecting Americans' right to self-custody their digital assets. Specifically, this means establishing statutory safeguards to protect consumers' self-custody rights from prohibition, restriction, encroachment, or infringement.

The Administration and Congress have Recognized the Critical Importance of Self-Custody

The PWG Report stated that legislation should recognize "The importance of U.S. individuals maintaining the capability to lawfully hold, or custody, their own digital assets without a financial intermediary."[34] President Trump's EO 14178 also specifically states that it is the policy of the United States to protect and promote the ability of individual citizens *and* private-sector entities to maintain self-custody of their digital assets.[35] GOP Majority Whip Tom Emmer likewise noted the importance of self-custody on the House floor just prior to passage of the CLARITY Act, saying that "The United States stands at the forefront of the next digital renaissance, a transformative shift towards a decentralized, peer-to-peer, digital economy.... [Market structure] will help further decentralize our financial system so that Americans can forego intermediaries and transact directly with each other."[36]

SEC Chairman Paul Atkins recently stated in his opening remarks at the Crypto Task Force's Roundtable on DeFi and the American Spirit: "The right to have self-custody of one's private property is a foundational American value that should not disappear when one logs onto the internet. I am in favor of affording greater flexibility to market participants to self-custody crypto assets, especially where intermediation imposes unnecessary transaction costs or restricts

---

blockchain network for decentralized verification and recording; and that the user retains full control over their assets, with private keys stored locally rather than entrusted to a third party).

[33] *Id*.

[34] PWG Report at 108.

[35] Exec. Order No. 14178 at § 1.

[36] Rep. Tom Emmer, remarks in House debate on digital asset regulation, 171 Cong. Rec. H3399 (daily ed. July 17, 2025) (statement of Rep. Emmer).

the ability to engage in staking and other on-chain activities."[37] Chair Atkins recently affirmed his commitment to self-custody by stating that "the right to have self-custody of one's private property is a core American value. I believe deeply in the right to use a self-custodial digital wallet to maintain personal crypto assets and participate in on-chain activities like staking."[38]

The House passage of CLARITY also signals overwhelming support for self-custody protections.[39] Specifically, Section 105 clarifies that U.S. *individuals* "retain" the right to self-custody digital assets in a hardware or software wallet and engage in direct peer-to-peer transactions, provided that the digital assets are used for lawful purposes, that such other individual or entity is not a financial institution, and the transactions do not involve any property or interests in property that are blocked pursuant to economic sanctions.[40] We believe the Senate can strengthen and improve this language, in line with the Senate Banking Committee Principles for Market Structure Legislation: "self-custody of digital assets should be explicitly preserved."[41]

Inclusion of Self-Custody Protections for All Persons Is Essential

The inclusion of self-custody protections for all American citizens, businesses, and private-sector entities[42]—in other words, all "U.S. persons"—in Section 403 of the RFIA discussion draft are essential.[43] Self-custody protections should also be legally enforceable by containing a private right of action or a tailored restriction on a government entity infringing on that right, or some other clear legal prohibition or enforcement mechanism. Finally, there should

---

[37] Paul S. Atkins, U.S. Sec. & Exch. Comm'n, *Remarks at the Crypto Task Force Roundtable on Decentralized Finance: DeFi and the American Spirit*.

[38] *Id.*

[39] Clerk of the House, *Roll Call No. 199* (July 17, 2025) (on passage of H.R. 3633, the Digital Asset Market Clarity Act), https://clerk.house.gov/Votes/2025199.

[40] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Cong. § 105(c) (2025), https://www.congress.gov/bill/119th-congress/house-bill/3633/text.

[41] Senate Banking, Hous., & Urb. Aff. Comm., *Crypto Market Structure Principles* (June 24, 2025), https://www.banking.senate.gov/imo/media/doc/6-24-25_market_structure_principles.pdf.

[42] Chainalysis Team, *Institutional Investment Creates Need for Enterprise-Grade Self-Custody Solutions*, Chainalysis (Dec. 22, 2022), https://www.chainalysis.com/blog/personal-wallets-institutional-crypto-adoption-self-custody-defi/ (Describing how institutions use self-custody solutions to manage their own assets and conduct direct on-chain transactions; notes widespread adoption among major blockchain firms.)

[43] *See* Senate Banking, Hous., & Urb. Aff. Comm, *Market Structure Principles for Digital Assets*.

be no limitation on a person's ability to hold their own property. Digital assets held on a blockchain and accessed through private keys in a non-custodial wallet should be treated with the same standard as physical cash in a wallet.[44]

The Senate's market structure legislation should incorporate the Keep Your Coins Act in order to achieve all of the outcomes mentioned above, implement President Trump's EO 14178, and follow the Senate Banking Committee's outlined market structure principles. The Keep Your Coins Act achieves the objectives of self-custody protections because it is clear, affirmative, legally enforceable, and protects all U.S. persons. Specifically, the legislation's definition of ''covered user'' protects "a person that obtains convertible virtual currency to purchase goods or services on that person's own behalf, without regard to the method in which such covered user obtained such convertible virtual currency."[45] The Keep Your Coins Act also critically recognizes the realities of non-custodial blockchain technology by defining a "self-hosted wallet," under which the "owner of convertible virtual currency retains independent control over such convertible virtual currency that is secured by such digital interface." That definition of self-hosted wallet makes clear that a non-custodial software provider who does not possess total independent control over user assets is not an intermediary, reaffirming a perspective expressed by the Department of Treasury Financial Crimes Enforcement Network (FinCEN) in their 2019 Guidance.[46]

That's why leading wallet software providers, including Exodus, Ledger, Casa, Block, MetaMask, and Uniswap Labs joined in celebrating the reintroduction of the Keep Your Coins Act, stating: "As leading providers of self-custodial wallets, we applaud Senator Budd's introduction of the Keep Your Coins Act, which mirrors Congressman Davidson's bill in the House. This crucial legislation protects individuals' fundamental right to own digital property by safeguarding against regulatory overreach. We look forward to continuing to support this legislation and establishing the United States as a haven for financial autonomy and economic freedom."[47]

---

[44] Ledger, *What Is Self-Custody in Crypto?*, Ledger Academy (May 27, 2024, updated Apr. 3, 2025), https://www.ledger.com/academy/topics/security/what-is-self-custody-in-crypto.

[45] *Keep Your Coins Act of 2025*, S. 2284, 119th Cong. § 2(a)(2) (2025), https://www.budd.senate.gov/wp-content/uploads/2025/07/Keep-Your-Coins-Act-of-2025.pdf. (introduced by Sen. Ted Budd).

[46] FinCEN, FIN-2019-G001 at 1.

[47] Senate Banking, Hous., & Urb. Aff. Comm., *Crypto Market Structure Principles.*

We firmly support the self-custody protections already in the discussion draft and are grateful to the Committee for their inclusion. It is imperative that these protections are maintained throughout the legislative process, and therefore we strongly encourage the inclusion of the language from the Keep Your Coins Act.

Addressing Illicit Finance and DeFi (Response to Questions 17(a), (b), (d))

As the RFI suggests in Question 17, appropriating additional resources to FinCEN and OFAC in order to promote partnership with the digital asset industry would be worthwhile. FinCEN has proactively engaged with the industry to learn about technological solutions and on-chain methods to address illicit finance, and the industry broadly supports that effort.

Broadly speaking, it would be most pertinent to focus efforts on strengthening cybersecurity and a private-public partnership for addressing hacks involving the appropriate federal agencies. The industry has already begun these efforts with the introduction of the Security Alliance (SEAL) in 2024 to remedy security risks, provide legal protection for white hat hacking in crypto, and help with incident response, among other initiatives.[48] The industry has also developed a best practice and competitive marketplace for security audits of DeFi protocols, as well as an industry standard of making such protocols open-source or source-available for broad inspection and audit. Public and private auditors are able to identify vulnerabilities and submit their reports to protocol developers, often receiving compensation for their work and developing a sustainable market for such work.[49]

The federal government should encourage these efforts by funding and collaborating with existing cybersecurity experts. Furthermore, in response to hacks, the federal government should consider simplifying the Federal Bureau of Investigation's (FBI) cyber crime reporting[50] and increase resources to respond to trusted tipsters through a whitehat hotline. In either case, federal agencies and law enforcement should not work alone, as there are many trusted cybersecurity experts and researchers within the industry who can serve as a primary resource for efforts to prevent illicit finance through hacks and breaches.

---

[48] Security Alliance, https://www.securityalliance.org/ (last visited July 28, 2025).

[49] *Bug Bounty Program*, Immunefi, https://immunefi.com/bug-bounty-program/ (last visited July 28, 2025) (explains how Immunefi connects protocols with security researchers by hosting a platform for registering and participating in bug bounty programs).

[50] Fed. Bureau of Investigation, Internet Crime Complaint Ctr., https://www.ic3.gov (last visited Aug. 1, 2025).

Technology Neutrality

President Trump's EO 14178 specifically outlines technology neutrality as a focus for digital asset policy, including language focused on protecting Americans' right to individual privacy.[51] EO 14178 also establishes that it is the policy of the United States to support the responsible growth of blockchain technology and related technologies by "protecting and promoting the ability of individual citizens and private-sector entities alike to access and use for lawful purposes open public blockchain networks without persecution, including the ability to develop and deploy software, to participate in mining and validating, to transact with other persons without unlawful censorship, and to maintain self-custody of digital assets."

This is the right step forward. Legislation should refrain from picking winners and losers based on the nature of the technology in order to prevent illicit activities, as design and operational choices offer their own legitimate benefits. Specifically, the privacy-preserving qualities and technology of DeFi are necessary for the safety and dignity of the American people, as it is designed for consumer privacy and its subsequent rights.[52]

Legislation that applies existing compliance regulations to DeFi, such as those that require the collection and reporting of personally identifiable information, would require developers to fundamentally alter the nature of the technology they create and abandon the benefits of decentralization. Imposing these sorts of burdens would create sizable barriers to entry—as most core developer teams are small—stifling innovation, while entrenching larger players with more resources.

Furthermore, Congress must keep in mind that preserving one's privacy is not an inherently criminal activity and is actually in line with consumer protection goals. Americans have perfectly lawful, legitimate reasons for choosing to protect their sensitive information. A person's financial transactions can paint the most intimate picture of their beliefs, associations, and activities – aspects of their lives which could lead to discrimination or harassment at the very least. Exposing users' identities would also provide the world with unprecedented access to all

[51] Exec. Order No. 14178 at §1.

[52] This is a bipartisan issue, as it aligns with the New Democrat Coalition Innovation Agenda, which states that among its policy priorities is the need to "Protect Online Privacy, Safety, and Cybersecurity" by ensuring "technologies are designed with the privacy and related rights of consumers as a priority." New Democrat Coalition, *Innovation Agenda* (2025), https://newdemocratcoalition.house.gov/imo/media/doc/new_dem_innovation_agenda.pdf.

past and present transactions of users, as well as their balances, which could make users with large amounts of sums the targets for exploitation or worse.[53]

The House of Representatives recently acknowledged this need for privacy in passing the "Anti-CBDC Surveillance State Act."[54] The bill effectively prohibits the Federal Reserve from directly or indirectly issuing a central bank digital currency (CBDC), and codifies EO 14178, prohibiting any exploration of its development.[55] Whip Emmer, author of the bill, made clear in his remarks that the introduction of a CBDC would effectively "give the federal government the ability to surveil and restrict Americans' transactions and monitor every aspect of our daily lives."[56] The same would hold true if legislation from the Senate were to fundamentally alter DeFi in order to unmask transacting individuals.

Cybersecurity and Consumer Protections

Legislation that imposes information collection and reporting requirements would introduce cyber and consumer risks to retail consumers that did not previously exist in DeFi in its attempt to combat illicit activity. This is especially true when the benefits of these requirements have failed to overcome the costs.

The BSA, originally designed to combat illicit finance, has become a largely ineffective and burdensome regulatory framework for financial institutions. Despite imposing immense

[53] In January 2025, David Balland founder of Ledger – the self-custodial hardware company – was kidnapped and held for ransom, along with his wife and children. Balland had his hand mutilated, leading him to pay the kidnappers a large sum of cryptocurrency. Aurelien Breeden, *French Crypto Entrepreneur Abducted and Held for Ransom, Officials Say*, New York Times (Jan. 23, 2025), https://www.nytimes.com/2025/01/23/world/europe/france-crypto-kidnapping.html.

[54] Press Release, Off. of Whip Emmer, *Majority Whip Tom Emmer's Flagship Legislation, the Anti-CBDC Surveillance State Act, Passes House of Representative*s (July 17, 2025), https://emmer.house.gov/media-center/press-releases/majority-whip-tom-emmer-s-flagship-legislation-the-anti-cbdc-surveillance-state-act-passes-house-of-representatives.

[55] Anti-CBDC Surveillance State Act, H.R. 1919, 119th Cong. (as passed by House July 17, 2025), https://www.congress.gov/bill/119th-congress/house-bill/1919/text.

[56] Whip Emmer, *Whip Tom Emmer Gives Floor Speech in Support of the Anti-CBDC Surveillance State Act* (YouTube July 17, 2025), https://www.youtube.com/watch?v=hFRY6twD3Fs (last visited July 28, 2025).

compliance costs—amounting to nearly $59 billion annually in the U.S. alone[57]—the BSA demonstrates minimal success in proactively detecting and prosecuting financial crimes. Although millions of transactions are reported, law enforcement rarely utilizes these reports to initiate investigations or proactively prevent and detect illicit finance.[58] Additionally, while the BSA has proven ineffective in accomplishing its intended objective, the sensitive information that is collected by intermediaries is often the target of large scale hacks so that illicit actors are able to immediately control accounts and conduct fraudulent transactions or drain funds,[59] or impersonate law-abiding citizens and launder money through traditional channels.[60] Legislation should not increase these risks by mandating further information collection.

Meanwhile, distributed ledgers and DeFi protocols are made more secure by spreading authority and data so thin that there is no single point of failure nor means for any person or entity to exert control and act maliciously.[61] Therefore, by centralizing ledgers or protocols through information collection requirements, honeypots of sensitive data would emerge for hackers to target or for trusted intermediaries to exploit, introducing a type of cybersecurity risk that DeFi's decentralized infrastructure has already resolved by neither requiring sensitive data to transact, nor storing it in one central location.

---

[57] LexisNexis Risk Sols., *True Cost of Financial Crime Compliance Study for the United States and Canada*, https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-for-the-united-states-and-canada (last visited July 27, 2025).

[58] Only 13.3% of investigations conducted in 2024 originated from BSA reporting, compared to 13.9% in 2023 and 15.8% in 2022. Nicholas Anthony, *Reporting FinCEN's Suspicious Activity, Again*, Cato at Liberty (Cato Inst.) (July 9, 2025), https://www.cato.org/blog/reporting-fincens-suspicious-activity-again.

[59] *Data Breaches in the Financial Sector [2025]*, Corbado Blog, (June 10, 2025), https://www.corbado.com/blog/data-breaches-finance.

[60] "Cybercriminal groups continue to develop and sell malware via darknet markets and online forums, while others use the malware to harvest and monetize financial data and other [personal identifiable information] on an industrial scale. Criminals can traffic the harvested data, such as banking passwords and login credentials, through marketplaces that specialize in the sale of compromised or stolen personal, financial, and banking information. Malicious actors can use this data to initiate unauthorized transfers from compromised bank accounts or to perform social engineering attacks against victims whose data was stolen." U.S. Dep't of the Treasury, *2024 National Money Laundering Risk Assessment* 25 (2024), https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

[61] On May 15, 2025, Coinbase was the target of a cyber crime, where criminals recruited insiders abuse their privileged access to steal sensitive customer data, including government-issued identification (e.g., driver's licences or passport). *Protecting Our Customers - Standing Up to Extortionists*, Coinbase Blog (May 15, 2025), https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists.

An information collection regime would also violate consumer rights already in place and protected within DeFi, and introduce a relationship between software developers and users that did not exist before. Prior to the digital age, Americans could transact and interact with each other without being identified and profiled for profit-seeking objectives. That was lost with the world rapidly moving online. However, with the introduction of DeFi, Americans are now able to transact and exist within the ecosystem without corporations extracting their data and violating their privacy and autonomy for profit. Legislation should not pull back the consumer rights that have been regained from emerging technologies.

FinCEN Rulemakings

Legislation should also direct FinCEN to drop its "Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern" (Docket No. FINCEN-2023-001).[62] Its overbroad definitions could label nearly all crypto transactions as "high risk," and this approach misunderstands the legitimate uses of "mixers" for financial privacy and imposes disproportionate compliance burdens on the industry. Instead, FinCEN should focus on enforcing existing regulations rather than creating new rules that risk driving innovation offshore and infringing on users' privacy.

Legislation should also direct FinCEN to update and codify its 2019 Guidance, titled "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (FIN-2019-G001),[63] to reflect the realities of DeFi technology in more detail and develop a binding framework that accounts for rapidly emerging technology. Specifically, the rulemaking should reflect that technology that solely consists of non-custodial, non-controlling software shall not be regulated as a financial institution or financial intermediary. It should also clarify that developers and providers of technology that enable communication of data and messages do not exercise total independent control over the content of said data and messages (e.g., users' digital assets on a distributed ledger), and are therefore not engaged in "money transmitting" or "the transportation or transmission of funds" on behalf of the public. If a "mixer" or "tumbler" reflects these facts and circumstances, then the developers and providers should not be treated as money transmitters.

---

[62] Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72,701 (proposed Oct. 23, 2023), https://www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions.

[63] FinCEN, FIN-2019-G001 at 1.

Importantly, this rulemaking should not replace the introduction of the BRCA in Section 402 of the discussion draft. Rulemaking is a necessary complement to the BRCA, serving as additional clarity related to federal money transmission law. Further, legislation should direct the Department of Justice (DOJ) to adhere to FinCEN's 2019 Guidance and additional guidance or rulemaking that follows regarding the BSA. The DOJ's novel interpretation of 18 U.S. Code § 1960 has led to criminal prosecution of software developers and proven to be the most critical issue in the industry.

Congress Should Include Federal Preemption for Developer Protections (Response to Question 35)

As Congress considers legislation to provide regulatory clarity, it must also address the patchwork of state laws that threaten innovation, create legal uncertainty, and expose developers to inconsistent and potentially conflicting obligations. The PWG specifically discusses preemption and directs Congress to ensure that there is one federally defined, unified framework for digital assets: "Congress should provide that federal law preempts state law with respect to securities and commodities laws applicable to SEC- and CFTC-registered intermediaries, including in the areas of state virtual currency business, "blue sky," and commodity broker laws."[64] In addition to the regulatory regime in market structure preempting state law, it is likewise critical that the Senate include explicit federal preemption of state law where it addresses developer protections. While CLARITY Sections 309 and 409 provided federal exemptions for certain developer-related activities from the statutory definitions of regulated conduct, they were silent on whether states could take inconsistent positions with those exemptions. Since courts may not find that federal exclusions override state regimes without explicit statutory language, without federal preemption, Congress risks losing the certainty it will provide to the digital asset market to a patchwork of state authorities.

Federal preemption is particularly important given the wide variance in state securities laws, commonly known as Blue Sky laws. The SEC traditionally applies the *Howey* test to determine if digital assets are securities, but the states have vastly differing tests that may expose DeFi developers to improper regulation. For example, in the Oregon Attorney General's lawsuit against Coinbase, the state applies its own *Pratt* test, which omits the "solely through the efforts of others" prong from the *Howey* test, thereby expanding the definition of an investment contract under state law.[65] This divergence leaves DeFi developers vulnerable to state action even where

[64] PWG Report at 55.

[65] *State of Oregon v. Coinbase, Inc.*, No. 3:25-cv-00952 (D. Or. July 2, 2025) (motion to remand), https://assets.ctfassets.net/sygt3q11s4a9/1fMeIQ7zNjC0Num5XNEXWq/b99887f6c1bd6e7916c75fb79a8752f2/State_of_Oregon_v._Coinbase__Motion_to_Remand__filed_7.2.25_.pdf.

federal guidance would suggest otherwise. Moreover, absent federal preemption, well-resourced traditional financial institutions may exploit the fragmented regulatory landscape by funding or encouraging state-level enforcement actions against DeFi developers—not to protect consumers, but to stifle competition.

Congress can preempt state laws in several ways. It can preempt state law expressly—for example, by creating a right and specifying that States cannot interfere with that right.[66] And it can preempt state law impliedly—for example, by passing a comprehensive federal scheme that occupies an entire field.[67] But either method of preemption is sufficient; express preemption alone will displace state law.[68] As the Supreme Court has explained, "[t]here is no doubt that Congress may withdraw specified powers from the States by enacting a statute containing an express preemption provision."[69] Congress has clearly manifested its intent to preempt state law on digital asset market structure regulation as a whole and it should extend that preemption specifically to developer protections.

Without a targeted express preemption clause that prevents states from taking conflicting positions with the federal protections for blockchain infrastructure and software developers, any market structure legislation would be largely symbolic. The Senate should affirm that no state-level securities, commodities or digital assets laws will apply to those developing or providing blockchain infrastructure or software. This would include: relaying or validating blockchain transactions; providing computing power, bandwidth, or similar network resources; providing software user interfaces to access blockchain data; developing or publishing blockchain systems, protocols, or liquidity pools; or creating tools like wallets that help users store, manage, or secure digital assets or private keys, among other things.

Federal preemption is critical given that DeFi technology is borderless and globally accessible by nature, meaning a DeFi developer cannot restrict access in states that take a hostile view toward the industry. Federal preemption would not only ensure that Congress's hard work in implementing tailored protections for blockchain and DeFi developers is respected and

---

[66] *Egelhoff v. Egelhoff ex rel. Breiner*, 532 U.S. 141, 146 (2001).

[67] *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947).

[68] *Arizona v. United States*, 567 U.S. 387, 399 (2012).

[69] *Id*.

followed nationwide, but would also ensure that the industry thrives in the United States, consistent with President Trump's Executive Order.[70]

President Trump has emphasized the need for a federal standard with respect to evolving technologies. In the context of AI regulation, the President highlighted that we "have to have a single federal standard, not 50 different states, regulating this industry of the future," and underscored the need for "one common sense federal standard that supersedes all states, supersedes everybody, so you don't end up in litigation with 43 states at one time."[71] These same principles apply to DeFi, and the success of U.S. innovation depends on consistent rules that don't fragment compliance across state lines.

The consequences of failing to adopt adequate policies are already visible in the data. According to Electric Capital's 2024 Developer Report, the U.S. share of crypto developers has declined from 38 percent in 2015 to 19 percent in 2024, and North America has dropped from first to third place in terms of the proportion of developers (behind Asia and Europe, respectively).[72] This reflects a steady erosion in domestic talent, and if Congress fails to act and states are allowed to pursue divergent approaches to regulation, this trend will accelerate. Preemptive federal protections for DeFi developers are essential to reversing this trajectory and reestablishing the U.S. as a global leader in innovation. As the PWG recently stated, "American entrepreneurs and software developers should have the liberty, and regulatory certainty, to upgrade all sectors of our economy using these technologies."[73]

With clear preemptive protections, innovators and infrastructure providers will be protected from the same fragmented, high-risk legal environment that crypto market structure legislation was meant to reform.

---

[70] Exec. Order No. 14178 at § 1.

[71] President Donald Trump, Remarks at the Winning the AI Race Summit (July 23, 2025), https://youtu.be/HmxbPH1PL_A.

[72] Electric Capital, *2024 Crypto Developer Report* (Dec. 12, 2024), https://www.developerreport.com/reports/devs/2024.

[73] PWG Report at 6.