



GBBC
Global Blockchain
Business Council

DECENTRALIZED FINANCE (DEFI) REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

DEFI GOVERNANCE: SETTING THE PATH FOR
FUTURE GROWTH



GBBCGSMI 6.0

ACKNOWLEDGEMENTS

Diana Oreto (Barrero Zalles)
Head of GSMI & Research, GBBC

Joseph Cutler - CO-CHAIR
Partner, Perkins Coie

Hedi Navazan - CO-CHAIR
Chief Compliance Officer, 1inch

Lee Schneider - CO-CHAIR
General Counsel, Ava Labs

Thank you to our working group participants and
review committee for your inputs.

**GLOBAL
BLOCKCHAIN
BUSINESS COUNCIL**

DC Location:

1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:

Rue de Lyon 42B
1203 Geneva
Switzerland

I) INTRODUCTION

Decentralized finance (DeFi) is emerging as one of the most transformative innovations for financial infrastructure, introducing new ways for individuals and institutions to transact, allocate capital, and coordinate economic activity without relying on traditional intermediaries. Built on open, programmable, and globally accessible blockchain networks, DeFi enables markets for financial services like lending, trading, payments, and asset management through code and automated, decentralized operations.

As the DeFi ecosystem matures, governance, both external via regulatory frameworks and internal via DAOs and protocol-level mechanisms, is a decisive factor shaping whether DeFi can evolve into a secure, scalable, and institutionally trusted financial system.

This paper covers the most important considerations for DeFi governance, drawing largely on selected submissions to the US Securities and Exchange Commission (SEC) Crypto Task Force's request for inputs¹ regarding the application of federal securities laws to blockchain and digital assets – specifically submissions that provide recommendations relevant for the DeFi ecosystem.

Regulatory Governance: Ideally, a globally harmonized and technology-neutral approach would allow blockchain innovation to flourish without requiring bespoke regulation for every new use case. For DeFi, and related activities such as tokenization, this means that compliance could be achieved under updated, but familiar, frameworks. This would reduce friction, encourage adoption, and support integration of Web3 with traditional finance. It would also support fairness and avoid regulatory arbitrage. For this section, we largely focus on insights from selected questions relevant for DeFi from US SEC Commissioner Hester Peirce's statement "There Must be Some Way Out of Here."² While some of these insights cover the US regulatory framework, many of the concepts are relevant globally, especially as DeFi operates on global liquidity pools by nature, and US regulations often influence those of other jurisdictions.

DAO Governance: Decentralized governance mechanisms remain among the least understood and most critical dimensions of DeFi. They distribute decision making across token holders, smart contracts, and global communities, creating new forms of coordination but also new vulnerabilities. This section covers how decentralized protocols and DAOs currently exercise governance, and how governance must adapt for protocols to remain decentralized while operating safely within legal and economic realities. We draw comparisons between decentralized and traditional corporate governance, identifying gaps where DAOs can adapt to provide equivalent accountability, risk controls, and investor protections.

Ultimately, effective DeFi governance, both on-chain and off-chain, is essential for transforming the evolving collection of open-source protocols into a resilient, legitimate, and globally interoperable financial ecosystem. Without thoughtful governance, DeFi risks remaining fragmented and fragile. On the other hand, with thoughtful governance structures, DeFi has the potential to reshape financial markets, expand global access to capital, and enable an open, programmable financial system for the long term.

II) WHY DEFI GOVERNANCE

What is the purpose of governance? It is crucial to ask this question before setting a governance model for any DeFi protocol. Because governance ensures legitimacy, accountability, and user trust in decentralized networks, it is essential for user retention, institutional adoption, and long-term stability. The exact format of governance likely looks different for different DeFi protocols, for which decentralized autonomous organizations (DAOs) are generally set up to carry out decision making, with no centralized party in control.

DeFi governance is important because it determines who controls financial infrastructure, how risks are managed, how value is allocated, and whether the ecosystem can scale responsibly. Governance matters at multiple layers: protocol governance, often via DAOs, user and community governance, and external governance through regulation. Each element plays a distinct role, and together they shape whether DeFi becomes a reliable, safe, and widely adopted financial system or remains fragmented, fragile, or vulnerable to abuse.

DeFi governance, whether it is carried out by DAOs, developers, communities, or regulators, is essential because it ensures that decentralization is genuine rather than superficial, preserving the core principles of distributed control. It manages risk and protects users in a permissionless environment where anyone can participate and where safeguards must be built into the system itself. Governance also allocates capital and oversees powerful financial infrastructure, determining how resources are deployed and how protocols evolve. It enables sustainable innovation by providing structured mechanisms for upgrades, improvements, and adaptation over time. Effective governance builds institutional and regulatory trust, making it easier for traditional financial actors to participate. It prevents the concentration of power and mitigates systemic vulnerabilities that could undermine the ecosystem. Ultimately, governance shapes the fairness, transparency, and legitimacy of the entire DeFi landscape.

In essence, governance is what transforms DeFi from a set of smart contracts into a functional, resilient, and credible financial system. Without governance—whether internal or external—DeFi cannot scale safely, attract mainstream adoption, or fulfill its promise of open, decentralized financial services.

Governance in DeFi is also closely connected to the broader ecosystem through social, technical, economic, and inter-protocol dynamics. Even in decentralized systems, social governance and community norms play a critical role: reputation, informal expectations, and off-chain coordination influence how contributors behave, how disputes are resolved, and how protocols evolve, helping maintain order where formal rules may be limited. Technical governance also shapes protocol behavior through code-based mechanisms such as time locks, upgradeability modules, fee switches, and circuit breakers; these embedded rules determine power dynamics, decentralization, and system resilience even in the absence of human voting. Economic and incentive governance adds another layer, as token distributions, rewards, liquidity incentives, and staking structures determine participation, alignment, and potential vulnerabilities—poorly designed incentives can lead to plutocracy, voter apathy, or manipulation, while well-designed systems encourage fairness and sustainable engagement. Finally, because DeFi protocols are deeply interconnected and composable, governance decisions in one protocol can have cascading effects on others—for example, lending markets rely on price oracles, and DEX liquidity tokens feed into vault strategies. For this reason, governance must be considered not only at the individual DAO level but across the broader ecosystem, where interdependencies create shared risks and collective responsibilities.

III) CONSIDERATIONS FOR DEFI GOVERNANCE

Below is a set of considerations that are fundamental for DeFi governance. Many of these are represented in the SEC RFI submissions for regulatory consideration, as reflected in the context of the questions below. It is important to note that considerations for DeFi governance go significantly beyond the securities classification rhetoric that has been so often raised (e.g., other issues include treasury, custody, financial regulation, money transmission, trusts, banking, AML/KYC controls). These issues have simply not been as actively focused on in legal enforcement actions. While falling within a “securities” designation may determine the jurisdiction of US regulation, there is a wide range of additional themes that must be dealt with for DeFi governance.

3.1) REGULATORY CLASSIFICATION & SECURITY STATUS

Transactions: The nature of a transaction and distinction of purpose matter greatly for classification. For example, if a developer sells tokens they created and uses the proceeds to build a project that increases the token’s value (e.g., ICOs), the arrangement fits the Howey test and is considered an investment contract. By contrast, a native blockchain token (e.g., XRP, Filecoin) may function primarily as a medium of exchange or access right, leading to the argument that these tokens are not securities, even if certain institutional sales of them might constitute securities transactions. Drawing on the experience of Ripple, programmatic sales considered as a commodities transaction are distinct from secondary sales on crypto exchanges, with the main difference being funds going directly to the founders or not. Institutional sales were originally by founders, designed fund builders to build infrastructure. The argument is that XRP, as a native DLT token, is never a security.

Tokens: Yet regulators should not fixate solely on the transactional structure at the expense of recognizing the nature of the underlying asset.³ If a token represents intellectual property, it should be treated accordingly; if it represents a commodity such as gold, it should be regulated as such, without unnecessary legal gymnastics. Moreover, securities transactions can involve non-securities, making it crucial to distinguish between the token itself and the underlying asset it may reference or represent. The goal is to create a rational framework where tokens are classified according to what they represent, rather than relying on rigid or overly prescriptive rules. This approach would help regulators account for the diverse roles tokens play while improving legal clarity for DeFi and broader digital-asset markets.

When it comes to tokens, it is important to consider differentiating “Protocol Tokens,” that is, Digital Native Assets from Traditional Securities. Thus, tokens that represent classic securities on a blockchain should inherit the corresponding protections and regulatory responsibilities. Others, considered native tokens, may warrant different treatment. This differentiation helps preserve investor protections where needed, while avoiding over-regulating fundamental blockchain infrastructure.

DeFi may interact with both kinds of tokens. If regulators accept a distinct “protocol token” category, it would lower legal risk for many DeFi and blockchain projects, reducing uncertainty for builders, users, and investors, and ultimately enable broader innovation without immediate securities law constraints. Moreover, Perkins Coie’s second submission to the SEC calls for the adoption of a workable taxonomy that remains merit- and technology-neutral.⁴

- **As an alternative to forcing protocol tokens into existing securities laws, the Ava Labs submission to the SEC proposes a rulemaking framework, with a new exemption for tailored disclosures, AML/KYC, and filing requirements.⁵**
- **Perkins Coie’s first submission to the SEC also acknowledges that tokenized securities should be treated as traditional securities.⁶**

The Sidley Austin submission to the SEC representing Owl Explains powered by Ava Labs presents 5 categories that represent the vast majority of tokens, for an asset-based test⁷:

1) Asset token	Physical representation of something physical that is recorded on a blockchain
2) Service token	Digital representation of services (e.g., accounting services, legal services, streaming)
3) Intangible asset token	While other existing regimes already define intangible assets (e.g., accounting term), such as money transfer licenses that require maintaining a net worth, it is important to consider how this applies to crypto companies with assets in the form of digital assets? There can be a gap when cryptocurrencies, for instance, are classified as intangible assets when the majority of US of states don’t count intangible assets as net worth. Yet these companies may have substantial balance sheets, which are represented inaccurately as very small when deducting cryptocurrency holdings
4) Native DLT token	This is an avenue to get out of the gap illustrated above, relevant for most Layer 1 blockchains, with tokens as bundles of rights
5) Stablecoins	Retain a stable value against an underlying reference

Lending Activities: Finally, because many DeFi protocols provide lending services, it is important to consider when a loan may or may not be classified as a security. Traditionally, loans are treated as securities, especially in retail contexts, when the funds lent belong to someone other than the lender: particularly banks reloaning customer deposits. DeFi challenges this model because lending is often peer-to-peer and involves individuals loaning their own funds directly to counterparties through smart contracts, thus removing the intermediary relationship that historically triggered securities concerns.

3.2) DECENTRALIZATION & CONTROL

As regulators and market participants evaluate DeFi systems, it is essential to consider carefully what decentralization means, how it is implemented, and where meaningful control actually resides. The mere existence of non-centralized swapping software or partially decentralized functions does not automatically make a system “DeFi.” Many entities in the blockchain space remain centralized in practice and may not be leveraging blockchain technology as originally intended, or may not clearly explain their role when referring to decentralized operations.

With an initial focus on tokenized securities rather than blockchain native digital assets, smart contract automation and programmatic controls can assume roles traditionally filled by centralized transfer agents. This suggests that decentralized technical operations could be recognized as legitimate within securities law frameworks.⁸

Yet while U.S. securities law is built around concepts of control and reliance on managerial efforts, decentralization fundamentally alters this approach by reducing or eliminating reliance on a managerial team under the Howey test.⁹ Many networks evolve into autonomous systems where upgrades, governance, and growth are not directed by a single promoter. This calls for a regulatory framework that distinguishes between tokens tied to entrepreneurial oversight and tokens embedded in decentralized protocols where no identifiable party “controls” the system. Decentralization changes the regulatory approach required because the foundational elements of securities analysis (e.g., control, managerial reliance, and information asymmetry) manifest themselves differently in blockchain networks, if at all.

When it comes to novel issues raised by blockchain-based solutions, regulators should recognize that where no central party exercises meaningful control, securities obligations may need be reduced or eliminated. For example, protocol tokens used for staking, validation, transaction fees, or governance should not be treated as securities because their value derives from network functionality rather than managerial promises.¹⁰ The transparency and automation of on-chain systems, which operate through open source, non-custodial mechanisms, differs fundamentally from intermediated securities markets.¹¹ This transparency lowers information asymmetry and enables new forms of self-governance.

3.3) WHO NEEDS TO BE A REGULATED ENTITY

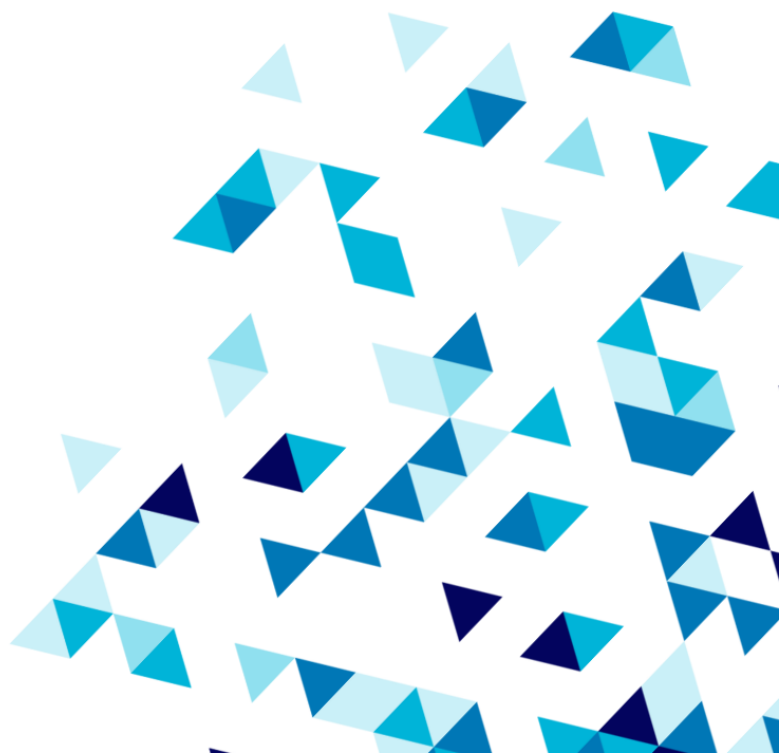
When assessing which actors in the blockchain and digital assets ecosystem should be regulated, a key principle arises: regulate the activities or intermediaries performing traditional financial functions, not the underlying protocol or token itself. Overall, regulation should follow the function, not the technology.

Under this principle, protocol-level actors (e.g., developers, validators, token holders, sequencers, smart contract deployers, DAO participants) should not be treated as regulated entities simply by virtue of interacting with a blockchain.¹² Protocol participants performing automated or mechanical roles should generally fall outside regulated classifications unless they act like traditional intermediaries. Moreover, actors involved in network operations (e.g., miners, validators) should not be treated as regulated entities because they do not exercise discretionary control or perform managerial actions on behalf of investors.¹³

Instead, regulation should focus on centralized intermediaries (e.g., exchanges, custodians, broker-dealers) and on actors who take on fiduciary or custodial roles (e.g., holding customer assets, making recommendations, running order books, soliciting investments). [Sec]When tokenized securities are issued, the issuer, transfer agent, broker-dealer, and custodian must follow existing securities rules, but the underlying blockchain infrastructure or smart contracts enabling fund transfers would not themselves become regulated financial entities.¹⁴

For the purposes of trading, regimes for exchanges (e.g., US ATS regimes) can be adapted for crypto trading platforms only when they perform functions equivalent to those performed by traditional exchanges.¹⁵ Yet non-custodial and smart contract-based trading protocols should not automatically be treated as regulated entities. There remains a need for greater clarity and distinguishing the following roles:

- Centralized exchanges
- Smart contract protocols
- Front-end operators
- Network validators



3.4) MARKET FRAGMENTATION

Blockchain infrastructure is inherently token agnostic. As long as a token has compatible security and interoperability, it can trade. As open marketplaces are evolving to reinstitute the benefits of previous barter systems, market fragmentation is an important concern. This requires a system where digital assets, both blockchain native tokens and tokenized securities, can trade, settle, and be custodied across interoperable ecosystems to maintain market integrity and efficiency.

However, the current regulatory environment poses several challenges that have led to fractured liquidity, siloed markets, and eventually traders moving their activities offshore.¹⁶ For instance:

- Digital asset exchanges cannot register or pursue licenses in harmonized ways
- Tokenized assets cannot seamlessly trade alongside blockchain native digital assets
- Inconsistent state and federal rules raise questions

Fragmentation is a negative outcome of regulatory uncertainty and incompatible frameworks. Without adequate regulatory developments, markets will continue to experience fragmentation in ways that hinder price discovery, increase market manipulation risks, and undermine U.S. competitiveness in capital formation involving digital assets. For instance, market fragmentation is concerning when tokenized securities are forced to trade within isolated permissioned ecosystems due to regulatory challenges, rather than circulating and settling on public blockchains. This fractures liquidity and prevents interoperability across trading venues. Fragmentation can also arise from a lack of taxonomy and inconsistent treatment of tokens, which leads to uncertainty and market bifurcation.¹⁷

In this context, rules recognizing public chains as acceptable settlement rails would reduce fragmentation between tokenized securities markets and broader crypto liquidity.¹⁸ Moreover, a unified taxonomy would help courts and regulators reach consistent conclusions, increasing predictability and reducing both geographic and functional fragmentation of crypto networks. It would also be helpful to distinguish between protocol tokens and securities, to reduce the risk of innovation splitting between jurisdictions and between “compliant” and “grey market” ecosystems.¹⁹



3.5) ROLE OF PROPERTY & PRIVATE LAW

Private law (e.g., property law, commercial law, and contract law) is foundational for DeFi, providing the underlying reasoning to conceptualize digital assets and related activities. Private law concepts (e.g., possession, transfer, beneficial ownership) are essential for regulatory clarity. Moreover, the focus on transparency, private key control, and ledger verifiability for governance echoes private law notions of possession and ownership.²⁰ Notably, property law is central to the vision of blockchain systems, which seek to “rewire” traditional financial norms, reduce frictions inherent in monetary intermediation, and enable fractional, in-kind forms of ownership and exchange. For example, the following digital assets and related activities can be approached from a private law lens:

- Protocol tokens can be treated as property rather than securities. Specifically, protocol tokens can be characterized as intangible personal property rather than contractual claims.²¹ These tokens do not create a legal relationship between the holder and an issuer but instead function as commercially fungible digital property within a network, strengthening the argument that such tokens fall outside the scope of securities law.
- Tokenized securities can be seen as digitally represented property rights.²² Specifically, tokenized securities representing traditional property rights, such as equity ownership or debt claims, are simply recorded and transferred using blockchain technology.
- Blockchain ledgers can be interpreted to function as property registries.
- Smart contracts can be considered to implement property law concepts (e.g., transfer restrictions, beneficial ownership rules, creditor priorities)
- In the context of historical SEC positions on mining and in-protocol rewards, it can be noted that these rewards stem from the use of personal property (e.g., computing resources or staked assets) rather than from reliance on a common enterprise.²³

This suggests that securities regulation may operate alongside, rather than override, private law principles. Thus, securities regulation can be better suited to integrate with, rather than displace, the underlying property law framework that can give digital assets legal meaning.

Yet private law remains underdeveloped when it comes to clarity for digital assets and related activities. Private law emerges as a critical missing piece for DeFi and key themes like tokenization. While tokens can represent rights to real-world assets (RWAs), most jurisdictions lack clear property law that recognizes tokenized ownership. At best, holders may have contract rights, which are enforceable but less robust and transferable than property rights. For example, tokenized real estate might contractually promise ownership, but without statutory backing (such as Article 12 amendments in the U.S. or new UK proposals), the claim is limited.

Moreover, many unresolved issues arise when attempting to ground digital asset taxonomies in private law. Tokenized real-world assets (RWAs) in particular highlight this gap. While contract law can specify that a token represents an asset, contract rights are weaker and less transferable than property rights. Contractual claims may allow damages for breach but do not provide the clarity or enforceability expected of ownership. In many jurisdictions, private law has not fully adapted to support tokenized property claims. Thus, RWA tokenization often relies on imperfect contract structures rather than robust property rights, limiting scalability and legal certainty.

As potential avenues for future steps, ongoing efforts are developing principles to harmonize private law treatment of digital assets (e.g., focused on decentralized trading and tokenized carbon credits). These initiatives recognize that private law must evolve for DeFi and areas like tokenization to achieve its potential, even though certain structural concerns (e.g., bankruptcy treatment with digital assets) may add further complexity. Still, the legal system needs frameworks analogous to the invention of deeds for real estate to support digital property. Until private law catches up with these innovations, DeFi innovation will continue to face legal constraints that hinder the ability to deliver the frictionless ownership transfer that the technology promises. Below are examples of initiatives to set key principles to harmonize private law around digital assets and related activities:

- The International Institute for the Unification of Private Law (UNIDROIT)²⁴, with the *UNIDROIT Principles on Digital Assets and Private Law*,²⁵ aims to provide clarity to facilitate transactions with digital assets for activities including control and transfer, custody, secured transactions, procedural law including enforcement, and insolvency.
- Uniform Law Commission (ULC) has developed a legal framework for digital assets through amendments to the Uniform Commercial Code (UCC), allowing the use of digital assets as collateral and ensuring their control can be established similarly to traditional property. These amendments include a new Article 12 for Controllable Electronic Records (CERs) and revisions to Article 9 for secured transactions.

3.6) ROLE OF INTERMEDIARIES

Whether DeFi protocols, or any elements of protocols (e.g., DEXes), should be treated as intermediaries, is fundamental. While traditional intermediaries formalize their relationships through contracts, DeFi often relies on code and user behavior to create implicit arrangements.

Principle suggests that regulators should not target the underlying technology but rather the applications and business activities built on top of it. Writing or deploying code should not, by itself, expose someone to liability, just as paving a road does not make one responsible for speeding drivers crashing into each other. For instance, from a purely technical standpoint, a DEX is simply software that enables peer-to-peer transactions.

However, if a DEX facilitates the trading of securities without identifying counterparties, the DEX's legal status becomes more complex, requiring clearer definitions. Moreover, if a DEX operator, or any identifiable party, earns revenue from providing trading access, collecting fees, or packaging data, that entity may be functioning as an intermediary and could reasonably fall within a regulatory perimeter. If a DEX generates trading fees, whoever receives those fees is more likely to be treated as a regulated actor. This concept can be in some way analogous to distinguishing royalties, where a creator earns income from future sales of an asset, from securities transactions, where income flows from the rising value of an investment or from facilitating trades.

Investor protections and market integrity remain essential priorities. While DeFi protocols improves capital market efficiency by reducing frictions, the challenge lies in protecting users when no centralized gatekeeper exists. A critical distinction to consider is between the technology itself and the business model that may form around it. Ultimately, determining whether a DeFi such as a DEX is an intermediary requires separating the technology from the business conducted through it and assessing who, if anyone, exercises meaningful control or benefits financially from the platform's operation.



3.7) SMART CONTRACTS & AUTOMATION

In the DeFi ecosystem, smart contracts consistently execute predefined actions, and participants interact with them in predictable ways that resemble contractual performance. This raises the question of whether and how these informal interactions driven by code should be interpreted in legal terms. A key theme for DeFi regulation is whether smart contracts themselves should be treated as brokers or other regulated intermediaries simply because they execute order routing or transactional functions.

The consensus in many emerging legal and policy discussions is that smart contracts should not be regulated as entities, but rather audited to ensure they perform as intended. Regulating technology directly is problematic: a smart contract is fundamentally a tool, much like written contracts or software systems, not a market participant. In traditional finance, a written contract is not regulated but governs a regulated activity, such as the issuance or trading of a bond. With this principle, a bond should be treated as a bond regardless of whether it trades through paper certificates or blockchain rails. Smart contracts should not be presumed to be legal contracts purely because they automate actions that resemble contractual activities.

This distinction raises aspects of the long-standing “code vs. law” debate in the space. The definition of a legally binding contract in the traditional sense requires it to have: 1) an offer (contract presents itself as such), 2) an exchange of consideration (e.g., exchange of value), and 3) performance (e.g., a user). Some state laws have begun to recognize that if a smart contract functions in a manner consistent with these principles, it may be given legal effect. However, smart contracts do not always involve two identifiable parties, a clear offer, or an explicit exchange of consideration. Code by itself does not constitute an offer; rather, legal enforceability depends on the surrounding context and whether the parties clearly manifested the intent to enter into a binding arrangement.

Therefore, a smart contract does not automatically qualify as a legally binding contract. A better regulatory may instead lie in assessing the activities facilitated by smart contracts (e.g., such as issuance, trading, custodial functions) rather than treating the technological mechanism as the regulated actor.

3.8) SECURITY & PRIVACY

KYC requirements remain outdated, and many current practices amount to performative compliance rather than meaningful risk mitigation. Decoupling KYC from AML is an important conceptual shift that can be beneficial for DeFi security, recognizing that identifying attempts to launder money is far more effective than simply knowing a user's name. From this lens, KYC can be seen as only one component of a broader risk assessment framework that incorporates blockchain analytics, behavioral monitoring, and protocol-level safeguards. AML in particular also needs to develop in effectiveness and sophistication.

Moreover, as institutions look to participate in the DeFi ecosystem, they seek models that preserve user privacy while still enabling compliance. This raises questions about whether whitelisting, selective disclosures, or more advanced systems (e.g., such as self-determined KYC/AML attestations) may be better suited for decentralized environments. A user could, for example, cryptographically prove they are not a sanctioned or high-risk individual without revealing their full identity. A global or interoperable identity verification system, conceptually similar to Global Entry or CLEAR systems for global travel, could allow wallets to display a “green check” confirming AML/KYC compliance while preserving anonymity. This way, instead of stating “metamask put xyz user through a KYC process,” a DeFi protocol can add a verification that xyz user is cleared. Law enforcement would be on board because if there is a suspicious transaction, authorities would have access to the KYC data. self-determinative KYC/AML verification systems allow protocol users to self-attest to non-launderer status and retain ownership and control over their personal data.

These considerations go hand in hand with emerging developments in privacy technology (e.g., particularly zero-knowledge proofs, decentralized identity, and self-sovereign identity principles), which must evolve to keep pace with DeFi's growth. DeFi already incorporates sophisticated RegTech solutions, and future protocols are expected to increasingly embed compliance directly at the protocol layer rather than outsourcing it to centralized intermediaries. Under such a model, users would undergo verification through a trusted third party, and the protocol would only receive confirmation that the user is cleared, not their personal data. Law enforcement would also retain access to underlying information in the event of suspicious activity, while the overall system would preserve user privacy. Ultimately, more effective AML frameworks, privacy-preserving verification tools, and integrated RegTech solutions are fundamental for DeFi to remain decentralized and privacy-respecting, ensuring a “clean DeFi” future that operates cooperatively within global financial crime obligations.



IV) REGULATORY GOVERNANCE FOR DEFI

From a regulatory standpoint, effective governance is crucial because first, legal clarity reduces uncertainty and builds market confidence. Regulatory frameworks provide clarity on which activities are permitted, which tokens are securities, how custody should work, and what standards apply to trading and settlement. Without this clarity, developers and investors often limit participation, build offshore, or avoid the U.S. market entirely. Regulation, if well designed carefully, can enable DeFi growth by reducing legal risk. Moreover, regulatory clarity protects users while preserving innovation. Regulation establishes guardrails to prevent fraud, market manipulation, and systemic risk, all of which can undermine trust in DeFi ecosystems. Good regulation can coexist with decentralization: for example, recognizing self-custody, using on-chain transparency for compliance, or applying tailored rules for smart-contract-based trading platforms. Ultimately, effective regulation enables institutional participation (e.g., funds, custodians, asset managers, and banks). Institutions cannot meaningfully participate in DeFi without regulatory clarity. Tailored custody rules, tokenization frameworks, KYC/AML standards, and clear classification rules make it possible for institutions to interact directly with DeFi protocols, bringing liquidity, stability, and legitimacy.

4.1) SEC REGULATORY QUESTIONS & RELEVANCE FOR DEFI

Under U.S. securities laws, transactions involving securities or investment contracts must be handled by a registered broker-dealer. This requirement stems from the 1930s, when widespread securities fraud, often involving paper certificates stolen from unsuspecting retail investors, led to mandates requiring intermediaries as gatekeepers to protect market participants. As a result, the current legal framework does not accommodate for securities transactions occurring in a peer-to-peer manner. Securities laws were created to require the use of registered broker-dealers. Yet in distributed ledger technology (DLT), transactions are transparent, auditable, and resistant to the types of fraud that prompted existing rules. The law has not yet caught up to reflect these advances.

In this context, US SEC Commissioner Hester Peirce released a statement with the SEC Crypto Task Force Request for Information titled “There Must be Some Way Out of Here”²⁶, posing questions to set the stage for regulatory developments for blockchain and digital assets. While not every one of the 48 questions is equally applicable for DeFi,²⁷ below is a selection and assessment of those questions that are most highly relevant to DeFi’s growth and governance.

The selected questions cover issues that can determine how DeFi protocols can operate, how users can interact with them, and whether these systems are lawful under existing securities laws. Many touch directly upon DeFi’s foundations and where regulation must strike the right balance between innovation and investor protection. Addressing these questions for DeFi will influence everything from architecture and governance to market access and institutional participation. We highlight the importance of these questions for the DeFi ecosystem especially because regulatory clarity:

- Reduces regulatory risk, enabling developers, users, and investors to operate with more confidence.
- Encourages adoption through regulatory legitimacy for DeFi. If policymakers recognize certain tokens or activities as non-securities or create bespoke regimes for them, mainstream financial institutions and retail users will be more willing to participate.
- Unlocks innovation, where tailored frameworks like safe harbors, sandboxes, and rules specific to smart contracts and custody for DeFi can provide builders with room to experiment without fear of enforcement.
- Adds predictability to governance and decentralization, allowing DeFi to operate in both a compliant and decentralized way.
- Helps bridge DeFi with traditional finance, through updated rules for tokenized securities, custody, atomic settlement, and exchange requirements. This is key for interoperability, institutional capital inflows, and the long-term viability of DeFi infrastructure.

4.2) SELECTED DEFI QUESTIONS

SECURITY STATUS QUESTIONS

Q1: What type of regulatory taxonomy would provide a predictable, legally precise, and economically rational approach to determining the security status of crypto assets and transactions in such assets without undermining settled approaches for evaluating the security status of non-crypto assets and transactions?

Relevance for DeFi

A clear and predictable taxonomy for digital assets is foundational to the growth and governance of DeFi. It determines whether governance tokens, LP tokens, vault tokens, staking tokens, stablecoins, wrapped tokens, NFTs, and other DeFi primitives are considered “securities,” which in turn dictates the regulatory obligations that apply. Because DeFi encompasses a wide spectrum of token types with different purposes and technical functions, uncertainty around classification exposes projects, users, and investors to significant legal risks. This uncertainty discourages institutional participation, complicates DAO governance design, and can cause builders to delay or halt development for fear of retroactive enforcement.

Clarity in classification is also important for tokens that fall outside traditional investment frameworks (e.g., stablecoins, wrapped assets). DeFi’s composability relies on the reliable interaction of many token types across protocols. Taxonomy also matters for staking and network participation tokens, which are central to many DeFi protocols. If these tokens are to be treated as securities, common DeFi mechanisms such as staking, liquid staking, and governance-based coordination could become impractical or subject to burdensome compliance requirements. Taxonomy ultimately points to regulatory clarity for token functionality and security status, providing the certainty developers, users, and institutions need to confidently build, use, and scale DeFi systems.

Q3: Certain crypto assets are used in a variety of functions inherent to the operation of a blockchain network, such as mining or staking as part of a consensus mechanism or securing the network, validating transactions or other related activities on the network, and paying transaction or other fees on the network. These technology functions may be conducted directly or indirectly, such as through third-party service providers.

What types of technology functions are inherent to the operation of a blockchain network? Should the Commission address the status of technology functions under the federal securities laws and, if so, what issues should be addressed?

Relevance for DeFi

DeFi relies heavily on blockchain-native functions such as staking, gas payments, validator rewards, and governance mechanisms tied directly to protocol operations. Tokens that serve these functions (e.g., paying transaction fees, securing consensus, incentivizing validators, sequencers, or relayers, and enabling governance participation) are foundational to the operation of L1s, L2s, and rollups. On the one hand, if these network function tokens are to be characterized as securities, core infrastructure providers would fall under securities regulation, fundamentally altering how DeFi protocols reward validators, design staking-based governance, or structure yield products built on staking and gas tokens. Because many DeFi protocols rely on staking and liquid staking derivatives to secure networks and generate yield, the regulatory status of these assets is crucial. If staking or liquid staking tokens are deemed to be securities, DeFi platforms may face registration requirements and compliance burdens that could undermine existing consensus and yield models. On the other hand, if these tokens are recognized as non-securities, this would legitimize the foundational economic mechanisms of blockchain networks under U.S. law, providing regulatory certainty that could encourage broader adoption, institutional participation, and continued innovation in DeFi infrastructure.

Q4: Users of liquid staking applications receive a so-called “liquid staking token.” This token represents their staked crypto asset, and the token can be used in other activities, all while continuing to participate in the proof-of-stake protocol. Should the Commission address the status of liquid staking tokens under the federal securities laws, and, if so, what issues should it address?

Relevance for DeFi

Liquid staking tokens (LSTs) (e.g., stETH, cbETH, etc.) are deeply integrated into DeFi as forms of collateral, Liquidity Provider tokens (LP shares), and yield-bearing assets. Their treatment as securities or non-securities will directly impact lending, leverage, and risk management across DeFi. For governance, DAOs that issue or rely on LSTs need regulatory clarity for the design of safe policies around collateralization, rehypothecation, and systemic risk.

Q5: Should the security status of certain categories of crypto assets be addressed, such as stablecoins, wrapped tokens, and NFTs?

Relevance for DeFi

Stablecoins and wrapped tokens are core building blocks of DeFi liquidity, collateral, and cross-chain composability. Their security status would shape a variety of key issues, from DEX trading pairs to money market design. Governance of DeFi protocols must account for whether these assets carry securities style constraints, particularly in cases wrapped, bridged, or synthetic assets are used as governance or collateral tokens.

PUBLIC OFFERINGS QUESTIONS

Q8: Should the Commission develop tailored disclosure requirements for offerings or classes of specific categories of crypto assets? What types of disclosures would be important for investor protection? Should disclosure occur both at the time of sale and on an ongoing basis? If so, what information should the ongoing disclosure contain and how should that disclosure occur?

Relevance for DeFi: Tailored disclosures could standardize how DeFi protocols report on token economics, protocol risks, admin keys, upgrade paths, and governance structures. This can greatly support strong DeFi market growth by improving due diligence and reducing information asymmetries. For governance in particular, tailored disclosures can compel DAOs to adhere to more formal transparency practices, making token holder voting and risk decisions better informed.

SAFE HARBOR FROM REGISTRATION QUESTIONS

Q10: Should the Commission consider a version of Rule 195, my proposed token safe harbor? Is the iteration on my proposed safe harbor known as “Safe Harbor X,” or some other iteration, a better approach?

Relevance for DeFi

A regulatory safe harbor would allow early-stage and experimental DeFi protocols to launch tokens and evolve toward decentralization without facing immediate and burdensome registration requirements. This type of framework is particularly important because many DeFi projects begin as community-driven, open-source initiatives with small teams and no traditional venture backing, making full securities-registration processes unrealistic or cost-prohibitive. A safe harbor would give these projects room to innovate, iterate rapidly, raise funds, and build community ownership while still requiring basic disclosures and antifraud protections for users.

It would also support healthier governance evolution by giving protocols time to transition from founder-led development to genuinely decentralized, DAO-based control under a transparent and predictable regulatory pathway. By lowering barriers to entry and providing structured flexibility, a tailored safe harbor could significantly expand the diversity, resilience, and long-term viability of DeFi ecosystems.

Q12: If a safe harbor of some form is the right approach, what disclosure requirements would be feasible for early-stage projects to provide to token purchasers the material information regarding the blockchain project, crypto assets, and development team? What information should be required to be updated on an ongoing basis, and how should that information be provided?

Relevance for DeFi: This question points to the need for a practical “rulebook” for DeFi start-ups: what must be disclosed about token allocations, governance rights, protocol risks, and roadmap? Well-designed requirements could become standard practices for DeFi whitepapers, dashboards, and DAO reporting. This would improve market discipline and support more responsible, accountable governance structures from day one.

Q13: At the expiration of the safe harbor as envisioned, if the network were sufficiently decentralized or functional, registration of the tokens would not be required.

If decentralization is used as an indicator of network maturity, should the Commission define objective quantitative thresholds (such as percentage thresholds for ownership and control) to provide greater clarity for issuers, developers, or minters of tokens regarding whether their networks and protocols are sufficiently decentralized and to allow third parties to verify decentralization?

- a. Is dispersion of control a better framework than decentralization? If so, how should ownership of governance tokens and voting rights be considered in assessing dispersion of control? How should the delegation of voting rights be taken into account?
- b. If an exit marker is achieved, who should be responsible for notifying the Commission?

Relevance for DeFi

Determining when a protocol is genuinely governed by a DAO rather than a centralized team is fundamental to legal and operational identity for DeFi. Clear, objective thresholds for decentralization and dispersion of control would guide how teams design token distributions, governance structures, and delegation mechanisms. Today, “decentralization” is often subjective and inconsistently measured, creating uncertainty for builders and investors. If regulators were to establish concrete decentralization metrics—such as standards for token ownership distribution, voting power dispersion, or governance participation—protocols would gain a predictable compliance target. This clarity would enable projects to intentionally design governance frameworks that meet regulatory expectations while preserving decentralized ownership and decision-making. It would also strengthen investor confidence and support institutional participation by signaling when a network can be treated more like an autonomous protocol than a company. Ultimately, objective decentralization criteria would provide a roadmap for DeFi protocols to mature in a way that aligns regulatory legitimacy with the ethos of decentralization, resolving one of the most persistent tensions in DeFi governance.

Q14: How should the decentralization of a deployed protocol best be evaluated? How should permissioned aspects of crypto-adjacent software or participant roles, such as validators, relayers, and sequencers, be considered? Are there tech-neutral thresholds that can be agreed upon for determining thresholds for decentralization?

Relevance for DeFi

Most DeFi activities run on infrastructure (e.g., L1s, L2s, rollups) with specific roles like sequencers and relayers that may be partially centralized. How regulators account for these roles affects whether DeFi built on this infrastructure is considered “decentralized.” Governance frameworks for DeFi and rollups need to align validator and sequencer design and incentives with any “tech-neutral thresholds” that may emerge.

TRADING QUESTIONS

Q15: Should the Commission create a new entity registration status with tailored registration requirements for any platform that trades crypto assets that are securities? Should the Commission use or adapt the existing requirements for national securities exchange registration or the alternative trading system exemption from such registration, and if so, how?

Relevance for DeFi: DeFi relies on on-chain trading platforms (DEXs, AMMs, aggregators). If any traded tokens are considered to be securities, those platforms may fall under exchange/ATS frameworks. A tailored regime that accounts for smart contract-based, and non-custodial trading is critical to maintain the composability that is inherently part of DeFi, while providing investor protections. DeFi governance approaches need to be designed with an understanding of whether and how the DAOs or front end operators may be treated as “platforms.”

DeFi relies fundamentally on on-chain trading platforms (e.g., DEXs, AMMs, liquidity pools, and aggregators) that enable peer-to-peer exchange of diverse digital assets. If any of the tokens traded on these platforms are deemed securities, the platforms themselves could fall under exchange or ATS regulatory frameworks, raising profound questions about how smart-contract-based, non-custodial systems fit into rules designed for centralized intermediaries. A tailored regulatory regime is therefore essential: one that recognizes the unique nature of decentralized, automated trading while still providing investor protections. Such a regime would allow DeFi-native market infrastructure to operate legally without compromising core features like permissionless nature, composability, and decentralization. This clarity is also critical for governance, because DAOs and even front-end operators need to understand whether their activities could cause them to be treated as regulated trading platforms.

Moreover, market structure issues extend beyond registration. DeFi’s power comes from its composability—the ability to combine governance tokens, stablecoins, wrapped assets, derivatives, and other instruments within unified protocols. Legal clarity around how mixed trading of “security” and “non-security” tokens is treated is essential to ensuring these innovations can scale. Additionally, because blockchains provide inherent transparency, regulators could leverage public on-chain data, APIs, and tools like proof-of-reserves or proof-of-holdings to conduct oversight more efficiently. Acceptance of such mechanisms would preserve DeFi’s transparency advantage while reducing compliance burdens. The SEC’s attention to MEV (Maximal Extractable Value) also highlights an understanding of DeFi’s unique mechanics—where transaction ordering can create fairness concerns such as front-running or sandwich attacks. Guidance in this area would influence how protocols design fair-execution mechanisms, risk disclosures, and user protections. Ultimately, appropriately designed market-structure, transparency, and fairness frameworks are foundational to building a scalable, trusted, and institutionally compatible DeFi trading ecosystem.

Q16: What updates to the Commission rulebook are needed for side-by-side pairs trading of securities and non-security crypto assets to allow for enhanced interoperability and composability in finance?

Relevance for DeFi

Many DeFi protocols aim to blend tokenized securities (RWAs, bonds, funds) with non-security tokens in the same pools and products. Regulatory tolerance for mixed-asset pools will determine how far DeFi may bridge on-chain and traditional assets. The DeFi ecosystem should account for rule changes that might require segregating or specially handling security tokens in governance, risk, and pool design.

Q18: The crypto markets are inherently transparent because they use open-source data, from public blockchains to open application programming interfaces (“APIs”). Are there programmatic/technological ways that crypto market participants, intermediaries, potential self-regulatory organizations, or regulators can monitor crypto markets using open-source data? How would this take into consideration nested accounts on centralized exchanges, given that this activity may not appear in public ledgers? Is open-source data sufficient for the market to monitor trading and therefore what non-public information might warrant mandatory disclosure? What sort of open-source tools can be used for enhanced transparency, such as proof of reserves, or proof of holdings? What are the limitations of such tools and such data?

Relevance for DeFi

DeFi is built on transparent, publicly accessible ledgers, raising an important question about whether this openness can serve regulatory and self-regulatory functions. If regulators accept on-chain analytics, proof-of-reserves, and similar blockchain-native tools as credible mechanisms for oversight, DeFi’s transparency can shift from being an uncharted challenge to becoming a regulatory advantage. This would allow DAOs and protocol teams to formalize on-chain reporting, audits, and real time dashboards as part of compliant operations, strengthening trust and operational integrity. The stakes are significant, as transparency is one of DeFi’s defining features, and formal recognition of open source blockchain data as a legitimate basis for investor protection and regulatory monitoring would meaningfully legitimize the sector. This could lower compliance costs, simplify auditing, and enhance systemic-risk surveillance, ultimately paving the way for broader adoption and deeper integration between DeFi and traditional finance.

Q20: How should Commission registrants assess Maximal Extractable Value (“MEV”) when they consider building or transacting in these environments? How best should Commission registrants delineate between the different types of MEV occurring onchain? In what ways is the market addressing the MEV in which MEV extractors order or re-order transactions to engage in front running, back running, or so-called “sandwich attacks”?

Relevance for DeFi

MEV is a central theme for fairness and user protections in DeFi. Regulatory focus on MEV would influence how protocols design mempools (“waiting areas” where unconfirmed transactions wait to be verified and added to a block), batch auctions, commit-reveal schemes, and other mitigations. Governance decisions about routing, block-builder relationships, and protocol-level MEV capture vs. redistribution will be shaped by how MEV risk is assessed for regulated participants.

CUSTODY QUESTIONS (ALSO RELEVANT FOR QS 24-32 GENERALLY DEALING WITH INSTITUTIONAL ADOPTION AND THE ROLE OF BROKER-DEALER CUSTODY, INVESTMENT ADVISER CUSTODY, AND INVESTMENT COMPANY CUSTODY)

Q21: Should the Commission amend existing rules, propose new rules, or provide guidance to facilitate custody arrangements for crypto assets? If so, what rule amendments or new rules would be appropriate, and to which types of activities should they apply? Should the Commission propose any specific changes to its rules to accommodate the self-custody of crypto assets by entities registered with the Commission? If so, what conditions should apply to self-custody arrangements to mitigate any related risks? Should the requirements for crypto assets that are securities and those that are not differ?

Relevance for DeFi

Self-custody and smart-contract-based custody are fundamental to how users and protocols operate in DeFi. Recognizing self-custody, multisig arrangements, and smart-contract vaults within regulatory frameworks would enable regulated institutions to interact more directly and safely with DeFi systems. For DAOs and protocol governance, this means developing custody-conscious risk policies—such as timelocks, emergency controls, or circuit breakers—that support institutional compliance without compromising decentralization. As DeFi increasingly incorporates tokenized real-world assets and permissioned tokens alongside native crypto assets, custody rules specific to these instruments will also determine whether they can be used as collateral or within liquidity pools. Governance must therefore evaluate the distinct legal and operational risks associated with native tokens versus tokenized securities, particularly regarding redemption rights, blacklisting, and compliance with enforcement actions.

Custody is a critical barrier because traditional custody regulations assume centralized intermediaries like banks or broker-dealers, which do not align with decentralized systems where users hold keys directly or rely on smart-contract custodians. If regulators update or clarify custody rules to accommodate crypto-native models—including self-custody—they would remove one of the biggest obstacles to institutional and broader retail participation in DeFi. Modernized custody guidance would support safer interaction between traditional financial entities and DeFi protocols while preserving the core user-controlled custody model that defines decentralized finance.

For DeFi to grow beyond its retail and early-adopter base, institutional participation is essential. Funds, asset managers, and investment advisers face strict regulatory requirements around custody, recordkeeping, valuation, and disclosures. Resolving these issues in a way that is compatible with DeFi's technical architecture could unlock significant institutional capital and dramatically scale the ecosystem. Because interacting with DeFi protocols typically requires the use of hot wallets or smart contracts, overly restrictive rules on hot-wallet use could prevent advisers and funds from accessing DeFi yields, liquidity, and governance opportunities. This makes it critical for DeFi governance to consider institutional-oriented design elements (e.g., non-custodial interaction models, permissioned or whitelisted vaults, and low-risk participation mechanisms) that align with evolving regulatory expectations.

Institutional exposure also hinges on whether custody rules can accommodate smart-contract-based assets, including LP tokens, governance tokens, and staking derivatives. If existing custody frameworks prove incompatible with DeFi-native custody models, institutional funds will remain on the sidelines. Conversely, if regulators clarify how funds may hold, stake, or actively participate in DeFi positions, the result could be transformative for market depth and liquidity. Participation in active strategies (e.g., staking, voting, providing liquidity, or engaging in DAO governance) is central to DeFi's value proposition, and institutional access to these activities would meaningfully increase the sophistication and stability of the ecosystem. Relatedly, funds need clarity on how to treat airdrops, staking rewards, or protocol-distributed incentives, which are ubiquitous in DeFi. Regulatory acknowledgment of these mechanisms would normalize DeFi-style yield generation for regulated products. Ultimately, enabling RIAs and funds to safely participate in DeFi's active economic mechanisms would strengthen governance, broaden user bases, and accelerate the integration of decentralized finance into mainstream financial markets.

CRYPTO LENDING QUESTIONS

Q33: How should the Commission approach various crypto lending concepts in a way that doesn't stifle the potential opportunities they provide?

Relevance for DeFi

DeFi lending (money markets, over-collateralized loans, under-collateralized protocols) is a core pillar of the ecosystem. A balanced regulatory approach can safeguard users while enabling innovation in credit markets, interest-rate products, and collateral design. Governance will need to set parameters (collateral factors, liquidations) in light of how "lending" is viewed and regulated.

TOKENIZED SECURITIES QUESTIONS

Q40: Tokenization enables dematerialized securities to be mobilized (i.e., not held in and confined to a single centralized ledger). Are there any provisions under the federal securities laws that prevent these securities from being used in new blockchain-based transactions and applications, and, if so, what steps should the Commission consider taking to facilitate this innovation while mitigating any related risks? Are there amendments or new rules that the Commission should consider to ensure a merit- and technology-neutral approach to tokenization? Does the type of blockchain used (i.e., permissioned versus permissionless) bear on this risk assessment?

Relevance for DeFi

Tokenized securities represent a major pathway for bringing real-world assets (RWAs) into DeFi, but legal barriers and regulatory preferences for permissioned or KYC-gated chains may limit how much of this activity can occur in open, permissionless environments. DeFi governance must therefore grapple with whether and how to integrate tokenized or permissioned assets without undermining composability, one of DeFi's core strengths. If regulators ultimately recognize tokenized securities and permit blockchain-based transfer agents, smart contract-driven settlement, and atomic on-chain clearing, it would create a powerful bridge between traditional finance and decentralized markets. Such a framework could support faster, cheaper, and more transparent settlement processes, unlock massive pools of institutional capital, and enable fractional ownership and greater liquidity for traditionally illiquid assets. The broader promise of tokenization is that, when combined with DeFi rails, it could catalyze new financial products and make mainstream on-chain finance a reality.

V) DECENTRALIZED GOVERNANCE MECHANISMS FOR DEFI

For the DeFi ecosystem, decentralized governance exists to give blockchain-based communities a way to collectively steer the development, resources, and evolution of a protocol without relying on a central authority. As stated above, and supported by DeFi players like Ava Labs²⁸ and academic research,²⁹ the first and most important question focuses on what its governance is meant to accomplish. Decentralized Autonomous Organizations (DAOs) use decentralized mechanisms, often powered by governance tokens, to replace the role traditionally filled by corporate boards, executives, or foundation stewards. This ensures that no single actor controls the protocol's direction and that decisions reflect the will of the community. Proper governance prevents misuse or unilateral extraction of value.

Without DAO governance as intended, most DeFi protocols would be restricted to governance by centralized teams, undermining the core value proposition of decentralization. Protocols would stagnate or rely on unilateral decisions by core developers. DAOs enable communities to decide on upgrades, set parameters, choose partnerships, and make strategic adjustments to the protocol. In all cases, governance structures must be designed thoughtfully, as low participation can undermine legitimacy, poorly designed token models can concentrate power, and excessive safeguards can paralyze decision making.



DECISION MAKING

The core purpose of decentralized governance is to coordinate decision making in a transparent, rule-based manner among participants who may be globally distributed, anonymous, or pseudonymous. DAOs may govern key decision making in a variety of ways, from allowing proposals from the community to cover any range of topics, to constraining proposals to narrow, clearly defined decisions. Smart contracts can automate the execution of these decisions, ensuring that treasury spending, token issuance, protocol upgrades, or resource transfers occur exactly as approved. This shifts the concept of traditionally contractual, off-chain processes into verifiable, on-chain actions.



RESOURCE ALLOCATION & TREASURY MANAGEMENT

One key subset of decision making focuses on mechanisms to allocate shared resources, held as treasury assets, in ways intended to reflect the priorities of token holders rather than the preferences of a centralized operator. Many DeFi protocols hold large on-chain treasuries funded by token issuance, fees, or liquidity incentives. Governance ensures that these resources are allocated transparently and in line with community priorities (e.g., funding audits, grants, protocol upgrades, partnerships, and emergency interventions).



ADAPTABILITY

Another subset of decision making supports protocol evolution and adaptability, as DeFi protocols must update smart contracts, risk parameters, yield strategies, oracle sources, and incentive mechanisms in accordance with changes in markets. DAO governance provides a structured, transparent mechanism for making these adjustments. Protocols must evolve as circumstances change, responding to security risks, changing market conditions, and technological advances. Governance provides embedded mechanisms for iteration, upgrades, and meta-governance (e.g., changing the rules of governance itself). This adaptability is crucial for long-term sustainability.

DAO governance also serves to legitimize outcomes by providing mechanisms for accountability. Voting, delegation, proposal templates, and quorum thresholds are tools meant to ensure that decisions arise from agreed-upon community rules rather than arbitrary authority. Clear governance processes give legitimacy to protocol decisions (e.g., upgrades, parameter changes, reward distribution, or partnerships). Transparent decision making increases user confidence and reduces the perception of insider control.

Ultimately, DAO governance is meant to ensure proper and trustworthy decentralization, ensuring reliability while preventing control by a single actor. DAOs are supposed to allow protocols to distribute decision making power across token holders or stakeholders, rather than concentrating it in founders or a central company (although this is not always the case in reality, reflecting how the space still needs to mature). When carried out appropriately, decentralization increases resilience against censorship, capture, corporate failure, or insider abuse.

Decentralization provides resilience. By distributing authority across many participants, DAOs reduce reliance on any single leader or jurisdiction. This makes them harder to censor, co-opt, or shut down. In essence, the purpose of decentralized governance is to empower communities to organize, allocate resources, and evolve collectively in a transparent, accountable, and sustainable manner in the long term.



5.1) DAO GOVERNANCE MECHANISMS

Research shows that DAO governance, through a variety of mechanisms, reflects many of the behavioral, psychological, and political dynamics that are manifested in direct democracies, adapted to the blockchain context. DAO governance structures produce a system that blends political theory, economics, software engineering, and social psychology to create a new form of digital, democratic coordination tailored to blockchain ecosystems.

DAO governance enables new economic and organizational models, which can be beneficial for a variety of organizations.

- Nonprofits and think tanks can find monetization opportunities through tokens
- Communities can fund real world projects such as buildings or carbon credit markets
- Tokenized assets can be governed in ways analogous to managing physical resources

Below are the key decentralized mechanisms employed by DAOs to carry out wide range of decentralized governance functions in the DeFi ecosystem, often powered by governance tokens.

DAO GOVERNANCE MECHANISMS

Mechanism	Function	Strengths	Weaknesses	Commentary
Voting	Token-based: 1 token 1 vote	• Simple, transparent, aligns influence with financial stake, and incentivizes holders to participate • Direct democracy, numerically fair	• Susceptible to plutocracy (wealth concentration = power concentration) • Can encourage short-term thinking • Vulnerable to vote buying	Wealthy people may buy a significant majority of the votes
	Quadratic	• Reduces influence of whales by increasing the cost of multiple votes • Amplifies minority voices	• Requires Sybil resistance (otherwise one actor can split wallets to game the system) • Complex to explain and implement • Can deter participation, and may deter people from collaborating as a group	More compelling option that combats the problem of buying votes with buying tokens, as incremental increase in voting authority is more expensive.
	Conviction	• Rewards long-term commitment, where weight increases the longer tokens are locked • Dampens speculative or hasty decision making	• Illiquid for participants (tokens locked up) • Slow responsiveness to urgent issues • Difficult for casual contributors to engage	May only reward people with enough stake to lock up for long term, leading to a preference for "HODLers" who "bought & forgot." This may not be the best measure of selecting participants to be involved in governance, so it may not be best to trust their vote especially for issues that are evolving.
	Reputation-based	• Decouples power from wealth • Aligns governance influence with proven contributions • Can reward long-term community trust	• Reputation systems are subjective and gameable • Difficult to reset if reputation distribution ossifies • Not always transparent	Reality may be detached from facts. People with big reputations are not always trustworthy. Reputation is not same as leadership, good work ethic. There is a need for non self-centered interests.

Mechanism	Function	Strengths	Weaknesses	Commentary
Proposals	Who can make proposals	Vetting participants	Potential for bias Lack of true decentralization	- Vetting participants is like pre-voting, which may limit breadth of what you can submit (pre-judging) - This can be in the form of thresholds, like holding a certain amount of tokens to be eligible to vote
	Kinds of proposals allowed	Vetting projects	May forego other good ideas that don't fit parameters of what's considered "acceptable" prior	Vetting participants is like pre-voting, which may limit breadth of what you can submit (pre-judging)
	Timelocks/grace periods	Gives community time to react to malicious or rushed proposals llows "emergency exits"	- Can delay urgent upgrades - Attackers may exploit a delay to front-run or prepare countermeasures	Makes the DAO less responsive to the needs of the community; cant respond fast if there's friction in proposal setting
	Quorum requirements	- Ensures broad participation - Prevents small cliques from passing impactful decisions	High quorum can lead to governance paralysis (decisions can't pass); low quorum risks capture by a small group	Quorum avoids individuals spamming the community with random proposals
	Templates/standards	- Improves clarity, comparability, and professionalism - Lowers barriers for new proposers	- May stifle creativity - Bureaucratic feel can discourage grassroots contributors	Promising tool to let people vote on what those templates/ standards are
Smart Contracts to Execute Decisions	Treasury controls	- Multi-sig or contract-based constraints reduce theft and misuse - Predictable disbursements	- Adds friction to funding decisions - May centralize control if few key signers	Assess whether controls clash w/decentralized nature of DAO. Many DAOs are not fully so, for different reasons. There can be excess voting influence - one aspect of this can be treasury control
	On-chain execution	- Transparent and automated - Eliminates trusted intermediaries - Tamper-resistant once executed	"Code is law" rigidity, where bugs or unforeseen scenarios can cause catastrophic failures - Difficult to reverse	There needs to be significant amount of information given to participants before it happen. Need for clear disclosures and education of participants before they put assets at risk. Don't change model/limit on chain execution (off chain destroys the point), but need people appraised on what's happening. (ex -when voting to make a major purchase, funds are allocated and sent as soon as everyone votes yes).
	Emergency functions	- Safety valve for hacks or governance attacks - Builds confidence in early DAOs	- Centralization risk: who controls the emergency lever? - Potential abuse undermines decentralization	Can be effective to stop exploits quickly before permanent fix is deployed, which may rely on human intervention. This may require trust in a central entity to make this kind of decisions

Mechanism	Function	Strengths	Weaknesses	Commentary
Delegation	Participants delegating voting to others	- Increases participation by allowing passive token holders to delegate to active stewards - Concentrates expertise	- Risk of entrenched power blocs - May recreate representative politics rather than true decentralization	Increases participation and informed decision making but can lead to delegate misbehavior and "window dressing" concerns where early investors/founders still hold the majority of power. This double edged sword requires accountability mechanisms and careful structural design.
Governance Tokens	Mechanism for users to vote and participate in decision making	- Clear unit of governance power - Liquid and tradable - Can align incentives via ownership	- Markets for tokens invite speculation; governance power can be bought - May diverge from user/community interests	Foundational element for DeFi governance, but main challenges consist in plutocracy (whale domination), voter apathy, and a lack of legal enforcement. There is a need for robust mechanisms to counter wealth concentration and encourage broader and meaningful participation
Governance Updates	Meta-governance to change major governance aspects (e.g., voting mechanisms, modify smart contracts, etc.)	Allows adaptation as DAOs evolve Critical for resilience in a fast changing ecosystem	- Updating governance itself can be contentious or slow - Risk of capture if upgrade processes are unclear	Unprecedented transparency and adaptability to change, but may encounter difficulties when it comes to security, speed, and concentrated power structures. AI-based automated governance mechanisms are being experimented to address these challenges.



5.2) DAO GOVERNANCE VS. CORPORATE GOVERNANCE

With no centralized control, DAOs operate very differently from traditional corporations. For a corporate setting, the main purpose of governance is to act on behalf of shareholders. Directors are expected to act in accordance with this purpose, even as US regulations have allowed boards and management teams to have certain veto rights over proposals.

On the other hand, DeFi protocols carry out many of the equivalent governance processes by means of DAOs and governance tokens. These decentralized mechanisms replace the role traditionally filled by corporate boards, executives, or foundation stewards. The entire lens of governance shifts because in peer-to-peer networks, there are no shareholders to act on behalf of in the same way. The users and token holders themselves can have the opportunity to directly participate in decision making

Below is a comparison of key governance aspects for corporations and DAOs:

Governance Mechanism	Corporate Governance	DAO Governance
Purpose	Alignment of management with shareholder interests, generally by maximizing firm value, and ensuring compliance with law and fiduciary duties.	- Coordination of a decentralized community to collectively manage, fund, and evolve a protocol. - Preserve decentralization and ensure decisions reflect the community rather than a central authority.
Decision Making	Centralized: a board of directors and executives make strategic and operational decisions on behalf of shareholders.	Decentralized: decisions are proposed and voted on by token holders as direct participants in a network, or designated delegates. This is often executed automatically via smart contracts.
Accountability	Directors and officers face legal and fiduciary accountability, with regulators enforcing compliance and reporting obligations.	Accountability is embedded into transparent on-chain voting, open-source code, community oversight, and reputational incentives, with enforcement being more social and technical rather than legal (which may evolve with regulatory developments for DeFi).
Adaptability	Adaptation takes place through management initiatives, board resolutions, and occasional shareholder votes (considered infrequent or slow).	Highly adaptable, where protocols can evolve continuously through proposals, parameter changes, and upgradeable smart contracts. Governance processes can be iterated and redesigned over time.
Ownership & Control	Shares represent economic and voting rights, where voting power is usually proportional to investment. Retail shareholders are generally passive.	Tokens may represent voting power, governance rights, or utility. Participation can be open to anyone, and power can be more widely distributed, though large token holders can dominate.
Transparency	Financial and strategic disclosures are provided periodically through regulated reporting (e.g., quarterly filings).	Full transparency, where treasury balances, votes, proposals, and upgrades are visible on-chain in real time.
Execution of Decisions	Decisions are executed by management and operational staff, with off-chain implementation that is subject to discretion.	Decisions can be executed automatically through smart contracts, reducing discretion and increasing determinism.
Participation	Limited, where only shareholders vote, and most retail shareholders do not participate.	Broad, global, permissionless participation, where token holders, contributors, and delegates can engage directly in governance.
Regulatory Structure	Well defined legal frameworks provide clear fiduciary duties, liability standards, and corporate reporting requirements.	Emerging and uncertain legal frameworks, where DAOs often operate without clear jurisdictional rules and rely on technological rather than legal compliance mechanisms. This may evolve with regulatory developments.
Resilience & Continuity	Continuity depends on the firm's solvency, leadership stability, and compliance with legal obligations.	Protocols can be resilient and durable through decentralization. Governance continues even if individual contributors or teams exit the network.
Resilience & Continuity	Continuity depends on the firm's solvency, leadership stability, and compliance with legal obligations.	Protocols can be resilient and durable through decentralization. Governance continues even if individual contributors or teams exit the network.

5.3) DAO GOVERNANCE GAPS

There exist clear governance gaps between DAOs and traditional corporations that reflect the immaturity of decentralized governance frameworks relative to long-established corporate structures. Although DAOs offer radical on-chain transparency, this information is not always easy for participants to interpret, unlike curated corporate disclosures designed for investor comprehension. Taken together, these gaps highlight the need for more robust governance design, legal integration, and regulatory clarity for DAOs to achieve the reliability, accountability, and strategic coherence expected of mature financial systems.

Gap 1: Accountability – Structures for accountability are much more developed for traditional corporations, leading to greater trust and scale.

- Corporations benefit from clear legal accountability. Directors and officers have fiduciary duties, can be held liable, and operate under strong regulatory oversight.
 - DAOs, on the other hand, rely mostly on social, reputational, or technical accountability, with no consistent legal recourse when governance decisions go wrong.
-

Gap 2: Participation & Strategic Vision - Participation differs significantly, in ways that can significantly undermine the quality of decision making for DAOs: a major gap where DAOs may not operate as intended. Strategic coherence is also harder to achieve in DAOs, where decentralized voting can produce inconsistent or reactive governance rather than a unified long-term vision.

- Corporate governance is centralized and stable, with boards acting on behalf of shareholders. Corporate boards consist of experienced professionals who deliberate strategically on key priorities.
 - DAOs allow broad, permissionless participation but often suffer from voter apathy, governance capture by large token holders, and unrepresentative decision-making. DAO voters may lack the technical or financial expertise needed to evaluate complex proposals, leading to fragmented or short-term choices.
-

Gap 3: Execution Challenges - Execution and enforcement may be unclear for DAOs in the context of their structure.

- Corporations have employees and managers who carry out decisions, with expertise and nuance required to address complex issues and unexpected problems.
 - DAOs rely on smart contracts or loosely coordinated contributors, making execution either rigid (when coded) or uncertain (when human). Smart contracts are only programmed to execute based on predetermined conditions, which will not include the possibilities of unintended outcomes that eventually may occur.
-

Gap 4: Regulatory clarity (or lack thereof) – Regulatory developments for blockchain and digital assets are still underway, leading to a series of regulatory gray areas for DeFi and DAO governance in specific.

- Corporations operate within well-defined legal frameworks, reporting rules, and compliance standards.
 - DAOs often exist in legal gray areas with uncertain tax treatment, liability, and compliance obligations.
-

Gap 5: Ownership and control divergences – In traditional contexts, those who own a company may be different than those who control it by making key decisions, with clear and established roles. DAO structures may bring together ownership and control in a way that better aligns interests, but the need for better safeguards remains.

- Corporate ownership structures are stable and legally registered.
 - DAO token ownership is fluid and anonymous, creating risks of governance attacks or sudden shifts in control.
-



VI) CONCLUSION

DeFi introduces a series of structural changes that fundamentally reshape how financial markets operate, especially if adopted at scale. By reducing reliance on intermediaries and enabling peer-to-peer interactions, DeFi creates more efficient markets with broader participation, in contrast to traditional systems where large institutions dominate profitable activities (e.g., syndicated lending among top banks) while leaving smaller participants remain excluded.

Moreover, DeFi's open, global infrastructure allows anyone with an internet connection to access market-rate borrowing, lending, and trading opportunities across borders. This expands the universe of available interest rates and financial products, enabling individuals and institutions to seek opportunities globally rather than being bound by domestic market constraints. For example, where one country may experience zero interest rates and another high rates, DeFi enables capital to flow to where it is most productive, fostering more competitive and efficient pricing.

Although technology serves as the tool enabling this transformation, human relationships, trust, and responsible practices (e.g., including whitelisting, compliance mechanisms, and adherence to securities laws when relevant) remain important as DeFi integrates with regulated environments. If scaled, DeFi could significantly expand global capital flows, shift markets toward a unified global cost of capital rather than fragmented national ones, and increase access and efficiency across the financial ecosystem while preserving pathways for regulated participation.

If regulators adopt such an adequate approach to DeFi as discussed throughout this paper, the implications for DeFi and the broader crypto ecosystem could be transformative: greater regulatory clarity, reduced legal risk, more institutional participation, deeper liquidity, and broader use of tokenized assets, all while keeping the core benefits of decentralization and blockchain-native infrastructure.

If DAOs at the same time also evolve decentralized governance strategies, DeFi protocols will be able to operate more safely, transparently, and sustainably at scale. This ensures that decisions are made collectively rather than controlled by a single actor, increasing resilience and trust in the system. Effective governance also improves risk management, responsible resource allocation, and can guide the DeFi protocols' long-term strategy. By embedding accountability, clear processes, and community participation, strong DAO governance attracts users and institutional partners, reduces vulnerability to manipulation or governance capture, and supports continuous innovation. Ultimately, effective DAO governance can transform DeFi protocols from a set of smart contracts into a stable, credible, and self-sustaining ecosystem.

RECOMMENDATIONS

The following recommendations for DeFi governance outline a practical path forward.

A roadmap for a hybrid, pragmatic regulatory regime should:

- Recognize new digital-native tokens and define a category for them (protocol tokens) rather than forcing them into traditional securities definitions.
- Update custody, exchange, and intermediary rules in a technology-neutral way to allow blockchain-native trading & settlement.
- Permit tokenization of traditional assets (equities, funds, debt), all treated as securities, but allow them to live on blockchains with smart-contract enforcement of transfer restrictions and compliance.
- Ensure disclosure, AML/KYC, and investor protections roughly analogous to what exists now, but adapted to digital realities.
- Provide transitional or safe-harbor regimes to let innovation continue while regulation catches up.

If regulators adopt such an approach, the implications for DeFi and the broader crypto ecosystem could be transformative: greater regulatory clarity, reduced legal risk, more institutional participation, deeper liquidity, and broader use of tokenized assets, all while keeping the core benefits of decentralization and blockchain-native infrastructure.

1. Establish a Clear and Harmonized Regulatory Framework

- Adopt a functional, technology-neutral regulatory model that follows the activity over the technology. Oversight should focus on actors (e.g., custodians, exchanges, brokers, and revenue-generating intermediaries), not protocol developers or validators.
- Recognize new digital-native tokens, such as “protocol tokens” that perform network functions (e.g., gas, staking, validation, governance), which should not be forced into traditional securities definitions.
- Permit tokenization of traditional assets (equities, funds, debt), all treated as securities, and allow them to operate on blockchains with smart contract enforcement of transfer restrictions and compliance.
- Provide tailored disclosure and registration pathways, with proportional disclosures for DeFi (e.g., tokens, governance structure, token supply, admin key risks, and upgradeability).
- Implement safe harbor regimes to let innovation continue while regulation catches up. For early stage protocols, this would provide DeFi projects space to decentralize before facing full regulatory obligations. This should require baseline disclosures, anti-fraud protections, and decentralization milestones.

2. Define Standards for Decentralization and Control, with measurable criteria for decentralization

- Clarify what counts as “sufficiently decentralized,” using metrics such as token distribution, governance participation dispersion, or operational independence from founders.
- Clarify treatment of sequencers, relayers, and validators. Roles essential to network operations should not be automatically treated as regulated intermediaries unless they perform discretionary or revenue-generating functions comparable to traditional financial actors.

3. Adapt Custody, Settlement, and Exchange Rules

- Update custody rules to recognize smart contract and self-custody models.
- Permit blockchain-based settlement for both securities and non-securities tokens.
- Create tailored rules for non-custodial trading venues, such as DEXs and automated market makers (AMMs), allowing them to operate under a framework distinct from centralized exchanges that can recognize code-based matching, automated liquidity, and the absence of discretionary brokers.
- Update custody, exchange, and intermediary rules in a technology-neutral way to allow blockchain-native trading & settlement.

4. Strengthen Private Law Foundations for Digital Assets

- Harmonize property law treatment of digital assets, drawing on principles such as UCC Article 12 or UNIDROIT to define digital asset ownership, transfer, custody, and creditor rights.
- Support legal recognition of blockchain ledgers as valid property registries.
- Develop clearer legal treatment for tokenized RWAs.

5. Improve DAO Governance Structures and Accountability

- Adopt governance designs that increase participation and reduce capture, using delegation, reputation systems, quadratic or alternative voting models, and incentive structures to avoid plutocratic control.
- Formalize governance processes and transparency, requiring proposal templates, disclosure of conflicts, voting thresholds, and risk assessments to strengthen decision-making quality.
- Clarify execution responsibilities, especially for situations where smart contracts cannot handle unexpected complexity. DAOs should designate teams, stewards, and service providers responsible for operational execution with clear mandates.

6. Embed Security, AML, and Privacy-Preserving Compliance into Protocol Design

- Shift from identity-first KYC to behavior-first AML, integrating blockchain analytics, behavioral monitoring, and pattern detection rather than relying solely on traditional identity collection.
- Adopt privacy-preserving compliance tools (e.g., zero-knowledge proofs), where users can prove they are not sanctioned or illicit without revealing sensitive data.
- Create interoperability layers for compliance, such as a global “green-check” verification standard to enable private, verifiable participation in DeFi.
- Encourage RegTech inside the protocol instead of around it, embedding compliance logic within smart contracts to reduce reliance on centralized intermediaries and facilitate institutional use.
- Ensure disclosure, AML/KYC, and investor protections roughly analogous to what exists now, but adapted to digital realities.

OPEN QUESTIONS

The following open questions remain to be addressed by the DeFi ecosystem in order to scale in a coordinated and compliant manner:

1. How should DeFi activities, protocol tokens, and decentralized systems be classified under law and regulation?
2. What constitutes “sufficient decentralization,” and how should accountability work in decentralized systems?
3. How should smart contracts be treated legally and operationally?
4. How should decentralized marketplace actors (e.g., DEXs, AMMs, composable protocols), be regulated without undermining decentralization?
5. Should decentralized exchanges (DEXs) or elements of DeFi protocols be treated as regulated intermediaries, and under what conditions may this treatment be considered?
6. How should digital assets be treated under property, custody, and bankruptcy law?
7. How should DAOs draw on traditional corporate governance structures to carry out governance activities?
8. How should existing weaknesses in DAO governance mechanisms be addressed in a harmonized way, such that the strengths of decentralized governance remain while ensuring user protections?
9. How should DeFi integrate compliance (KYC/AML) while preserving privacy and decentralization?
10. How should systemic risks be managed in a composable ecosystem where protocols may be significantly interconnected and dependent on one another on many levels?
11. What is the right balance between decentralization and centralized control if at all necessary?

ENDNOTES

DEFI

- 1 <https://www.sec.gov/about/crypto-task-force>
- 2 <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125>
- 3 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBolgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs__Crypto_Task_Force_Written_Submission.pdf; <https://www.sec.gov/files/ctf-written-input-digital-chamber-073125.pdf>
- 4 <https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf>
- 5 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBolgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs__Crypto_Task_Force_Written_Submission.pdf
- 6 <https://www.sec.gov/files/ctf-written-input-digital-chamber-073125.pdf>
- 7 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBolgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs__Crypto_Task_Force_Written_Submission.pdf
- 8 <https://www.sec.gov/files/ctf-written-input-securitize-050725.pdf>
- 9 <https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf>
- 10 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBolgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs__Crypto_Task_Force_Written_Submission.pdf
- 11 <https://www.sec.gov/files/ctf-written-input-digital-chamber-073125.pdf>
- 12 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBolgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs__Crypto_Task_Force_Written_Submission.pdf
- 13 <https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf>
- 14 <https://www.sec.gov/files/ctf-written-input-securitize-050725.pdf>
- 15 <https://www.sec.gov/files/ctf-written-input-digital-chamber-073125.pdf>
- 16 <https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf>
- 17 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBolgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs__Crypto_Task_Force_Written_Submission.pdf
- 18 <https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf>
- 19 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBolgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs__Crypto_Task_Force_Written_Submission.pdf
- 20 <https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf>

- 21 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBolgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs_Crypto_Task_Force_Written_Submission.pdf
- 22 <https://www.sec.gov/files/ctf-written-input-securitize-050725.pdf>
- 23 <https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf>
- 24 <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>
- 25 <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/>
- 26 <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125>
- 27 Some questions focus on traditional registered offerings, exchange-traded products, or investment companies, which are more relevant to tokenized securities than to permissionless DeFi protocols.
- 28 <https://www.owlexplains.com/en/podcast/ava-labs-x-cber-ep-2-governance-of-decentralized-autonomous-organizations/>
- 29 https://www.worldscientific.com/doi/10.1142/S281100482350001X?srsIid=AfmBOoofMXWxnJCQWdoW5WYe4_TL9XQdHrH_lwXlvPX_dEmCVRNhSWGm



GBBC

© 2025 Global Blockchain Business Council - Without permission, anyone may use, reproduce or distribute any material provided for noncommercial and educational use (i.e., other than for a fee or for commercial purposes) provided that the original source and the applicable copyright notice are cited. Systematic electronic or print reproduction, duplication or distribution of any material in this paper or modification of the content thereof are prohibited.