UCC ARTICLE 12 AND THE GOVERNANCE-TOKEN GAP:

Why Commercial Law Needs to Accommodate Decentralized Finance

November, 2025

This document is a working paper made publicly available for early readership and professional feedback.

Jason W. Shim, Esq.*

** California-licensed attorney focused on cross-border capital markets and digital asset regulation.*

ABSTRACT

The 2022 Amendments to the Uniform Commercial Code created Article 12, a new framework governing "controllable electronic records" that promised to bring digital assets within commercial law's protective umbrella. Article 12 established clear rules for transferring interests in Bitcoin, NFTs, and other electronic records, providing the take-free rules and priority structures that sophisticated markets require. But Article 12 has a gap—a significant one. The framework's central concept of "control" assumes that digital assets are managed by identifiable individuals with exclusive authority to enjoy, exclude, and transfer. This paradigm fails for the fastest-growing segment of digital assets: governance tokens that operate through decentralized autonomous organizations (DAOs), where control is distributed across thousands of participants who act through collective voting rather than individual decision-making.

This Article identifies and analyzes Article 12's "governance-token gap." Drawing on detailed examination of DAO governance mechanisms—including token voting, multi-signature wallets, timelocks, and guardian contracts—it demonstrates why Article 12's control concept cannot accommodate real-world decentralized finance structures. The Article surveys recent DAO litigation, state legislative responses, federal proposals, and international approaches, revealing a global convergence on control-based frameworks that share Article 12's blind spot. It then proposes specific amendments to expand Article 12's reach: new definitions for governance tokens, alternative tests for "distributed control," and safe-harbor provisions for DAO treasury assets.

INTRODUCTION

In July 2022, the Uniform Law Commission and American Law Institute approved the most significant amendment to the Uniform Commercial Code in a generation.[1] The 2022 Amendments, centered on a new Article 12 governing "Controllable Electronic Records," represent American commercial law's response to the emergence of cryptocurrency, non-fungible tokens, and other digital assets. By November 2025, over thirty states had enacted some version of Article 12, establishing a new commercial-law framework for digital-asset transactions across much of the country.[2]

Article 12 accomplishes much. It defines a new category of personal property—the "controllable electronic record" or CER—and provides clear rules for transferring interests in CERs.[3] It establishes a "take-free" rule that allows good-faith purchasers to acquire CERs free of competing property claims, promoting market liquidity.[4] It integrates with Article 9 to enable security interests in digital assets, with control-based perfection providing priority over interests perfected merely by filing.[5] For digital assets that fit Article 12's paradigm—Bitcoin in a single-owner wallet, an NFT transferred between individual collectors—the framework provides welcome certainty to a market long plagued by legal ambiguity.

But Article 12 has a gap—a significant one. The framework is built on a concept of "control" that assumes an identifiable individual or entity holds the relevant powers over a digital asset: the power to enjoy the asset's benefits, the exclusive power to prevent others from benefiting, and the exclusive power to transfer.[6] This paradigm reflects the mental model of cryptocurrency's early years, when Bitcoin and similar assets were held in individual wallets controlled by single private keys.[7]

Decentralized finance has evolved beyond that model. Today, billions of dollars in digital assets are managed not by individuals but by decentralized autonomous

[1] See Uniform Law Commission, UCC Amendments (2022) Prefatory Note.
[2] See Miller Nash LLP, UCC Article 12: Perfection of Security Interests in Controllable Electronic Records (Mar. 5, 2025); Willkie Farr & Gallagher, UCC Article 12, Controllable Electronic Records (Aug. 2024).
[3] U.C.C. § 12-102(a)(1) (2022).
[4] U.C.C. § 12-104(e) (2022).
[5] U.C.C. § 9-326A(a) (2022).
[6] U.C.C. § 12-105(a) (2022).
[7] See U.C.C. § 12-105 cmt. 3 (2022).

organizations—DAOs—that govern through collective voting.[8] MakerDAO, which administers over $5 billion in collateral backing the DAI stablecoin, makes governance decisions through MKR token voting.[9] Uniswap, the largest decentralized exchange, is governed by UNI token holders who vote on protocol parameters and treasury allocations.[10] Lido, which controls nearly 30% of all staked Ethereum, operates through a DAO structure where governance participants include major venture capital firms like Andreessen Horowitz and Paradigm.[11]

These governance tokens do not fit Article 12's control paradigm. No individual MKR holder "controls" MakerDAO's treasury; control is distributed across thousands of token holders who must achieve consensus through voting. No single person has "exclusive" power to transfer protocol assets; transfers require governance approval that aggregates many participants' preferences. The concept of "control" that structures Article 12 assumes a world of individual actors; DeFi operates through collective governance that Article 12 cannot accommodate.

The consequences of this gap are not merely academic. Courts are beginning to address DAO liability with troubling results for governance participants. In *CFTC v. Ooki DAO*, a federal court held that a DAO could be sued as an unincorporated association, with token holders who voted potentially liable for the organization's violations.[12] In *Sarcuni v. bZx DAO*, another court allowed claims that all governance token holders might be partners with unlimited liability.[13] And in *Samuels v. Lido DAO*, a court held that venture capital firms that participated in DAO governance could face personal liability alongside other DAO participants.[14]

Meanwhile, secured transactions in governance tokens operate in legal uncertainty. A lender that takes MKR tokens as collateral cannot perfect by "control" because no individual can satisfy Article 12's control test. Filing a financing statement provides some protection,

[8]See Gail Weinstein, Steven Lofchie & Jason Schwartz, A Primer on DAOs, Harv. L. Sch. F. on Corp. Governance (Sept. 17, 2022).
[9]See MakerDAO, The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System, https://makerdao.com.
[10]See Uniswap, Governance, https://uniswap.org/governance.
[11]See Samuels v. Lido DAO, No. 23-cv-06492-VC, 2024 WL 5155342, at *2-3 (N.D. Cal. Nov. 18, 2024).
[12]CFTC v. Ooki DAO, No. 22-cv-05416-WHO, 2023 WL 3945824 (N.D. Cal. June 8, 2023).
[13]Sarcuni v. bZx DAO, No. 22-cv-00618-TWR-DEB, 2023 WL 2657633, at *4-5 (S.D. Cal. Mar. 27, 2023).
[14]Samuels, 2024 WL 5155342, at *8-10.

but without control-based perfection, the lender lacks priority over a subsequent party that does obtain control. The very structure that makes DeFi innovative—distributed governance—makes it incompatible with Article 12's commercial-law protections.

Why Governance Tokens Belong in Article 12

Before proceeding, this Article must address a threshold question: why should governance tokens be treated as CERs at all, rather than as investment property under Article 8 or as some entirely new category? The answer lies in the functional characteristics of governance tokens and the policy purposes that Article 12 was designed to serve.

First, governance tokens are not "securities" in the traditional sense that Article 8 contemplates. Article 8's framework was designed for shares of stock, bonds, and similar instruments—assets that represent claims against an identifiable issuer and that are held through a centralized system of securities intermediaries.[15] Governance tokens lack these characteristics. There is no identifiable issuer in a sufficiently decentralized protocol; the protocol itself is the "issuer," but it is not a legal entity capable of owing obligations. And governance tokens are typically held directly in user wallets, not through securities intermediaries. Article 8's indirect-holding system—designed for a world of brokers, custodians, and clearing corporations—is a poor fit for assets that users hold and transfer directly on public blockchains.

Second, even if some governance tokens might satisfy the *Howey* test for federal securities-law purposes, that classification does not compel Article 8 treatment under state commercial law. The UCC's definition of "security" in Article 8 is distinct from the federal securities laws' definition.[16] A token might be a "security" for SEC registration purposes without being a "security" under Article 8—particularly if it is not "dealt in or traded on securities exchanges or securities markets" as Article 8 requires.[17] The classification questions are independent, and commercial law need not defer to federal securities classification in determining how property rights in tokens should be governed.

Third, governance tokens possess all the functional characteristics that motivated Article 12's creation. They are electronic records stored on distributed ledgers. They can be

[15] See U.C.C. § 8-102 (defining "security" and "securities intermediary").
[16] Compare U.C.C. § 8-102(a)(15) (defining "security" for UCC purposes), with Securities Act of 1933 § 2(a)(1), 15 U.S.C. § 77b(a)(1) (defining "security" for federal purposes).
[17] U.C.C. § 8-102(a)(15)(iii).

transferred through cryptographic transactions. They have value—often substantial value—that parties wish to buy, sell, and pledge as collateral. They circulate in markets that would benefit from clear take-free rules and priority structures. Article 12 was designed precisely for such assets. The governance-token gap arises not because governance tokens are categorically different from other CERs, but because Article 12's control test was drafted with individual holders in mind.

Fourth, excluding governance tokens from Article 12 would leave them in a commercial-law vacuum. If governance tokens are neither CERs (because no individual can satisfy the control test) nor investment property (because they are not held through securities intermediaries), then no UCC article provides clear rules for their transfer, perfection of security interests, or priority among competing claimants. This vacuum serves no policy purpose. Commercial law exists to facilitate commerce; leaving a significant category of commercial assets outside any coherent framework frustrates that purpose.

The better approach is to amend Article 12 to accommodate governance tokens' distinctive characteristics—to extend the CER framework rather than abandon it. The tokens themselves are electronic records capable of being controlled; the challenge is that control is distributed rather than individual. The proposed amendments address this challenge by expanding Article 12's control concept, not by creating an entirely new property category. This approach preserves Article 12's benefits—take-free rules, control-based perfection, integration with Article 9—while extending them to the governance structures that currently fall outside the framework.

This Article argues that Article 12 requires amendment to accommodate decentralized governance. The argument proceeds in six parts.

Part I examines Article 12's architecture in detail, tracing its intellectual genealogy from Article 8's indirect-holding system and Article 9's control-based perfection. It shows how Article 12's control test—requiring "exclusive" powers over digital assets—creates a framework well-suited to individual-holder scenarios but structurally incompatible with distributed governance.

Part II explores the governance-token gap with technical precision. Drawing on detailed analysis of DAO governance mechanisms—including token voting, multi-signature wallets, timelocks, and guardian contracts—it demonstrates why Article 12's control concept

fails to accommodate real-world DeFi structures. The Part examines MakerDAO's governance architecture as a case study, showing how continuous approval voting, executive spells, and the Governance Security Module create a system where "control" is distributed, contingent, and perpetually contested.

Part III surveys recent legal developments. It examines the emerging jurisprudence of DAO liability—*Ooki DAO*, *Sarcuni*, and *Lido*—and considers the implications of these decisions for Article 12. It analyzes state legislative responses, particularly Wyoming's Decentralized Unincorporated Nonprofit Association Act, and federal proposals like FIT21 that would establish a regulatory framework distinguishing decentralized from centralized digital-asset systems.[18] It also tracks Article 12's adoption across states, noting non-uniform amendments and the continuing patchwork of enactment.

Part IV offers comparative perspectives. It examines how other jurisdictions are addressing digital-asset property rights: the United Kingdom's "third category" of personal property,[19] Switzerland's ledger-based securities regime,[20] the European Union's Markets in Crypto-Assets Regulation,[21] and UNIDROIT's Principles on Digital Assets and Private Law.[22] A striking pattern emerges: jurisdictions worldwide have converged on "control" as the organizing concept for digital-asset property, and none has adequately addressed distributed governance. The governance-token gap is global.

Part V proposes specific amendments to Article 12. Three sets of changes would expand Article 12's reach to encompass decentralized governance. First, a new definition of "governance token" would establish this category within Article 12's scope. Second, amendments to Section 12-105 would create rules for "distributed control," addressing multi-signature arrangements, token-voting governance, and veto powers. Third, a new Section 12-110 would provide workable rules for DAO treasury assets, including multiple perfection mechanisms suited to collective ownership structures.

Part VI concludes by situating the proposed reforms within the broader trajectory of commercial-law development. The UCC has always evolved to accommodate new

[18]Financial Innovation and Technology for the 21st Century Act, H.R. 4763, 118th Cong. (2024).
[19]Law Commission, Digital Assets: Final Report (Law Com No 412, 2023).
[20]Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act) (Sept. 25, 2020) (Switz.).
[21]Regulation (EU) 2023/1114 (MiCA).
[22]UNIDROIT, Principles on Digital Assets and Private Law (2023).

commercial practices—from the original Code's response to mid-century commerce, through Article 2A's lease provisions, to Article 4A's wire-transfer rules. Article 12 was itself an evolution, extending commercial law to digital assets. The proposed amendments continue this tradition, adapting Article 12 to the decentralized structures that increasingly characterize digital-asset markets.

The stakes are significant. Decentralized finance represents a genuine innovation in financial infrastructure—one that enables permissionless participation, programmable transactions, and governance structures impossible in traditional finance. But innovation requires legal infrastructure. Without clear property rights, secure transfer mechanisms, and workable priority rules, DeFi will remain a frontier market, limited to participants willing to accept legal uncertainty. Article 12 reform can provide the legal infrastructure that DeFi needs to mature.

The Uniform Law Commission has an opportunity to lead. Other jurisdictions are grappling with the same challenges, and none has found adequate solutions. The United States—through Article 12 and the ULC's tradition of commercial-law innovation—can chart a path forward. This Article offers a roadmap.

A word on methodology: This Article draws on technical documentation from major DeFi protocols, including MakerDAO, Uniswap, Aave, and Compound. It examines governance mechanisms as they actually operate—not as idealized abstractions—because Article 12's gaps become visible only when the statute confronts real-world complexity. The Article also engages extensively with the Official Comments to Articles 8, 9, and 12, which reveal the drafters' assumptions and help identify where those assumptions fail. Finally, the Article situates the proposed reforms within the broader context of commercial-law development, drawing on the UCC's history of adapting to new commercial practices.

I. THE ARCHITECTURE OF ARTICLE 12 AND ITS EMBEDDED ASSUMPTIONS

Article 12 represents the culmination of a three-year drafting effort by the Uniform Law Commission and the American Law Institute to integrate digital assets into the commercial-law framework.[23] The Joint Committee on Uniform Commercial Code and Emerging Technologies, which included over 300 observers from financial institutions, technology companies, law firms, and government agencies, sought to create what the Prefatory Note describes as "a legal regime that is meant to apply more broadly than to electronic (intangible) assets that are created using existing technologies such as distributed ledger technology (DLT), including blockchain technology."[24] More ambitiously, Article 12 "aspires to apply to electronic assets that may be created using technologies that have yet to be developed, or even imagined."[25]

This aspiration toward technological neutrality was laudable. But the drafters' determination to avoid technology-specific language created its own difficulties. By defining digital assets through the functional concept of "control" rather than through their technological substrate, Article 12 embedded certain assumptions about how digital assets operate—assumptions that may not hold across all asset types and governance structures. Understanding these assumptions is essential to identifying where Article 12 succeeds and where it falls short.

A. The Controllable Electronic Record: A New Category of Personal Property

Article 12's foundational concept is the "controllable electronic record" or CER. Section 12-102(a)(1) defines a CER as "a record stored in an electronic medium that can be subjected to control under Section 12-105."[26] This definition is notable for what it does not say: there is no reference to blockchain, distributed ledger technology, cryptographic keys, or any other technological mechanism. The drafters deliberately adopted this "technology-neutral" approach to ensure that Article 12 would remain applicable as digital-asset technology evolves.[27]

---

[23] See Uniform Law Commission, UCC Amendments (2022) Prefatory Note.

[24] 2022 U.C.C. Amendments, Prefatory Note to Article 12, at 229.

[25] Id.

[26] U.C.C. § 12-102(a)(1) (2022).

[27] See 2022 U.C.C. Amendments, Prefatory Note to Article 12, at 229; see also Cleary Gottlieb, UCC Digital Asset Amendments Finalized (July 21, 2022).

The definition establishes CERs as a residual category—encompassing electronic records that can be controlled but that do not fall into other, more specific UCC categories. Section 12-102(a)(1) expressly excludes from the CER definition: controllable accounts, controllable payment intangibles, deposit accounts, electronic copies of records evidencing chattel paper, electronic documents of title, electronic money, investment property, and transferable records under UETA or E-SIGN.[28] These exclusions preserve the application of existing UCC articles and federal law to assets already covered by those regimes.

The exclusion of "investment property" is particularly significant for this Article's analysis. Under Article 8, investment property includes securities, security entitlements, securities accounts, and commodity contracts.[29] By excluding investment property from the CER definition, Article 12 channels such assets into Article 8's framework for indirect holding through securities intermediaries. This channeling function works well for traditional securities held through a centralized clearing system. But as Part II will demonstrate, it creates acute difficulties for governance tokens that may or may not qualify as securities and that are typically not held through intermediaries.

The residual-category structure has important implications. Because CERs are defined negatively—as controllable electronic records that are *not* something else—the scope of Article 12 depends on the scope of the exclusions. If the SEC were to determine that all governance tokens are securities, they would become investment property and fall outside Article 12 entirely. If, instead, governance tokens are not securities, they might qualify as CERs—but only if they can be "subjected to control" under Section 12-105. The interaction between federal securities law, state property law, and Article 12's control test creates a classification thicket that Part II will explore in detail.

B. Control as the Organizing Concept

If the CER is Article 12's foundational concept, then "control" is its organizing principle. Section 12-105(a) provides that a person has control of a CER if four conditions are satisfied.[30]

[28] U.C.C. § 12-102(a)(1) (2022).
[29] See U.C.C. § 9-102(a)(49) (defining "investment property").
[30] U.C.C. § 12-105(a) (2022).

First, the electronic record, or a record attached to or logically associated with it, or the system in which it is recorded, must give the person "the power to avail itself of substantially all the benefit from the electronic record."[31] This element captures the functional equivalent of possession's use value—the ability to enjoy whatever benefits the record confers.

Second, the person must have "exclusive power" to prevent others from availing themselves of substantially all the benefit from the electronic record.[32] This exclusivity requirement mirrors possession's exclusionary function—the ability to keep others out.

Third, the person must have "exclusive power" to transfer control of the electronic record to another person or to cause another person to obtain control of another controllable electronic record as a result of the transfer.[33] This transfer power ensures that CERs can circulate in commerce and, critically, that they can be pledged as collateral.

Fourth, the electronic record, attached record, or system must enable the person "readily to identify itself" as having the foregoing powers.[34] Identification may be "by name, identifying number, cryptographic key, office, or account number."[35]

The Official Comments explain that this control standard was designed as "a functional equivalent of possession of a tangible asset."[36] Just as possession of a negotiable instrument gives rise to holder-in-due-course status under Article 3, control of a CER gives rise to qualifying-purchaser status under Article 12. The analogy is elegant: control does for intangibles what possession does for tangibles.

But the analogy also reveals Article 12's embedded assumption: that control, like possession, is exercised by a single, identifiable person with exclusive authority over the asset. The paradigm case—expressly contemplated by the Official Comments—is "a person in possession of a private key"[37] to a cryptocurrency wallet. In this paradigm, control is

[31]U.C.C. § 12-105(a)(1)(A) (2022).
[32]U.C.C. § 12-105(a)(1)(B)(i) (2022).
[33]U.C.C. § 12-105(a)(1)(B)(ii) (2022).
[34]U.C.C. § 12-105(a)(2) (2022).
[35]Id.
[36]U.C.C. § 12-105 cmt. 2 (2022).
[37]U.C.C. § 12-105 cmt. 3 (2022).

binary (you either have the key or you don't), exclusive (only one person knows the key), and individual (that person can be identified).

The control concept also embeds assumptions about *how* digital assets are held and transferred. The paradigm contemplates a wallet—a software or hardware device that stores cryptographic keys—that belongs to an individual. Transfers occur when the keyholder signs a transaction authorizing movement of assets to another address. The transaction is atomic: it either succeeds completely or fails completely. There is no intermediate state, no partial transfer, no shared custody during execution.

These assumptions accurately describe many cryptocurrency transactions. But they do not describe all of them—and they particularly fail to describe the governance structures that have emerged in decentralized finance. The next sections examine how Article 12's control-centric framework interacts with the specific doctrines of commercial law: qualifying-purchaser status, security interests, and multi-party arrangements.

C. Qualifying Purchaser Status and the Take-Free Rule

Control matters because it determines eligibility for qualifying-purchaser status. Section 12-102(a)(2) defines a "qualifying purchaser" as "a purchaser of a controllable electronic record . . . that obtains control of the controllable electronic record for value, in good faith, and without notice of a claim of a property right in the controllable electronic record."[38] This definition closely tracks Article 3's holder-in-due-course standard, adapted for the CER context.

The payoff for qualifying purchasers comes in Section 12-104(e), which provides that a qualifying purchaser "acquires its rights in the controllable electronic record free of a claim of a property right in the controllable electronic record."[39] This is the "take-free" rule—the negotiability feature that makes CERs commercially useful. A qualifying purchaser need not worry about competing claims from prior owners, secured creditors, or other claimants. The purchaser's rights are clean.

[38]U.C.C. § 12-102(a)(2) (2022).
[39]U.C.C. § 12-104(e) (2022).

Professors David Frisch and Nicole Dalrymple have identified a significant drafting problem in this structure.[40] The qualifying-purchaser definition requires that the purchaser "obtains control," but the take-free rule protects a purchaser who "acquires" the CER. These are different things. A purchaser might acquire ownership rights without obtaining control (for example, if the seller agrees to transfer but hasn't yet delivered the cryptographic keys), or might obtain control without acquiring ownership (for example, if the transfer is voidable). The Frisch-Dalrymple critique highlights how Article 12's control-centric framework can create gaps when applied to transactions that don't fit the single-keyholder paradigm.

D. Security Interests and the Priority Structure

Article 12 dovetails with revised Article 9 to create a comprehensive framework for secured transactions in digital assets. The 2022 Amendments added new provisions to Article 9 addressing attachment, perfection, and priority of security interests in CERs.[41]

Under the amended Article 9, a security interest in a CER may be perfected either by filing a financing statement or by obtaining control.[42] The innovation lies in the priority rules. Section 9-326A provides that a security interest in a CER "held by a secured party having control of the collateral has priority over a conflicting security interest held by a secured party that does not have control."[43] This is the "super-priority" rule—control trumps filing.

The super-priority structure creates powerful incentives for secured parties to obtain control. A lender who merely files a financing statement against a borrower's cryptocurrency holdings remains vulnerable to a subsequent lender who obtains control. The subsequent lender jumps the queue. Rational lenders will therefore insist on control-based perfection, which typically means taking custody of the borrower's private keys or having the borrower transfer assets to a wallet controlled by the lender.

The priority framework mirrors existing UCC rules for deposit accounts and investment property, where control-based perfection similarly trumps filing.[44] The drafters' logic was straightforward: if the secured party actually controls the collateral, the secured

[40]See David Frisch & Nicole Dalrymple, Oops! The Unfortunate (but Basic) Error in the New UCC Article 12, 11 Tex. A&M L. Rev. 515 (2024).
[41]See U.C.C. §§ 9-105A, 9-107A, 9-314A, 9-326A, 9-331A (2022).
[42]See U.C.C. § 9-312(a) (2022).
[43]U.C.C. § 9-326A(a) (2022).
[44]See U.C.C. § 9-327 (priority rules for deposit accounts); U.C.C. § 9-328 (priority rules for investment property).

party's interest should prevail over a creditor who merely filed paperwork. Control provides assurance that the secured party can actually reach the collateral upon default.

This priority structure reflects a broader trend in commercial law toward favoring "actual" over "constructive" forms of security. A secured party with possession of goods has priority over one who merely filed; a secured party with control of a deposit account has priority over one with a security agreement alone. The 2022 Amendments extended this logic to digital assets, creating a new domain where control-based perfection provides super-priority.

The practical implications are significant. Under the super-priority rule, a later-in-time secured party who obtains control can "prime" an earlier-filed security interest. This creates risk for lenders who rely on filing alone: a subsequent lender who takes control of the collateral jumps ahead in priority, even if the first lender's interest was perfected years earlier. The risk is particularly acute for governance tokens, where control may shift through market transactions without notice to earlier-perfected creditors.

But this logic depends on control being achievable—and achievable exclusively. If control cannot be obtained (because the asset is managed through decentralized governance), or if control is necessarily shared (because the asset is held in a multi-signature arrangement), then the priority structure breaks down. Secured parties cannot obtain the super-priority that Article 12 promises because the prerequisite control is unavailable.

E. The Multi-Signature Accommodation—and Its Limits

The drafters were not entirely blind to the possibility of shared control. Section 12-105(c) provides that a person may have control even if "the power [to transfer control] is shared with another person."[45] Similarly, a person may have control even if "another person . . . has control of the controllable electronic record" or "can cause a change, including a transfer or loss of control."[46]

These provisions appear to contemplate multi-signature arrangements, where multiple keyholders must cooperate to transfer assets. The Official Comments confirm this reading,

[45]U.C.C. § 12-105(c)(1) (2022).
[46]U.C.C. § 12-105(c)(2)-(3) (2022).

noting that "shared authority to make modifications to a controllable electronic record is not inconsistent with 'control.'"[47]

But the accommodation is narrow. Section 12-105(c) addresses shared *powers*—the case where multiple people can cause a transfer. It does not address distributed *governance*—the case where no one person has the power to cause a transfer, and where decisions require collective action by a shifting population of token holders. In a 3-of-5 multi-signature wallet, each of the five keyholders arguably has "shared power" to transfer. But in a DAO governed by token-weighted voting, no individual token holder has any meaningful "power" to transfer the DAO's treasury assets. The individual's power is infinitesimal—one vote among thousands.

Section 12-105(c) also does not address who counts as having control when control is shared. If two people share the power to transfer, do both have control? Can both be qualifying purchasers? Can both have super-priority security interests? The statute does not say, and the comments provide no guidance.

F. The Investment-Property Exclusion and Classification Uncertainty

Perhaps Article 12's most consequential design choice is the exclusion of investment property from the CER definition.[48] This exclusion preserves Article 8's role as the governing framework for securities and security entitlements. But it also creates a boundary problem: how do we know which digital assets are "investment property" and therefore outside Article 12's scope?

Article 8 defines "security" to include an obligation of an issuer or a share or other interest in property or an enterprise that is (i) represented by a certificate, (ii) one of a class or series, (iii) divisible, and (iv) traded on securities exchanges or markets.[49] Many governance tokens satisfy these criteria: they are divisible, fungible, traded on exchanges, and issued by identifiable protocols.

But securities classification under Article 8 does not automatically follow from securities classification under federal law. The SEC applies the *Howey* test to determine

[47]U.C.C. § 12-105 cmt. 4 (2022).
[48]U.C.C. § 12-102(a)(1) (2022).
[49]See U.C.C. § 8-102(a)(15) (2022).

whether an instrument is an "investment contract" subject to the Securities Act.[50] The UCC's Article 8 uses a different definition. An asset might be a "security" for SEC purposes but not for Article 8 purposes, or vice versa.

This disjunction creates classification uncertainty. If a governance token is a security under *Howey* (because purchasers expect profits from the efforts of others), it is subject to SEC registration requirements. But it may or may not be "investment property" under Article 9, which would trigger Article 8's rules rather than Article 12's. The token's commercial-law treatment depends on a classification question that Article 12 does not resolve.

The practical consequence is a legal no-man's-land. Governance tokens that arguably qualify as securities cannot confidently be treated as CERs (because of the investment-property exclusion), but they also cannot confidently be treated as Article 8 securities (because they lack a centralized issuer and are not held through securities intermediaries). Parties transacting in these tokens face irreducible uncertainty about which rules apply.

G. Summary: The Single-Controller Paradigm

Article 12's architecture reflects what might be called the "single-controller paradigm." The framework assumes that a CER is controlled by an identifiable person who has exclusive authority to enjoy, exclude, and transfer. Control can be readily verified by reference to the person's cryptographic key or other identifier. Transfers occur between discrete parties, each of whom can be identified. Shared control is exceptional and involves a small, defined group of keyholders.

These assumptions draw on the historical development of commercial law's treatment of intangible property. Article 8's framework for securities originally contemplated paper certificates held in physical form; the indirect-holding system adapted that framework to dematerialized securities held through intermediaries. Article 9's treatment of deposit accounts assumed a relationship between a depositor and a bank—two identified parties with clear roles. Article 12 extends this tradition to digital assets, with "control" playing the role that possession played for goods and that control-through-intermediary played for securities.

The single-controller paradigm holds for many digital assets. Bitcoin held in a single-signature wallet fits perfectly: the keyholder has exclusive authority over the asset, can

[50] SEC v. W.J. Howey Co., 328 U.S. 293 (1946).

transfer it at will, and can be identified by their public address. NFTs minted to an individual address work similarly. Even tokenized securities custodied by a registered broker fit the paradigm, with the broker exercising control on behalf of identified customers.

For these assets, Article 12 provides welcome legal clarity. The framework establishes clear rules for transfers, priority, and perfection—rules that sophisticated commercial parties have long sought. The take-free rule promotes market liquidity by protecting good-faith purchasers. Control-based perfection enables secured lending. Integration with Article 9 situates digital assets within the familiar architecture of commercial law.

But the single-controller paradigm does not describe the fastest-growing segment of the digital-asset ecosystem: decentralized finance protocols and their governance tokens. The next Part examines why Article 12's framework breaks down when applied to these structures.

II. THE DEFI AND DAO GAP

Part I demonstrated that Article 12 rests on a single-controller paradigm—the assumption that digital assets are controlled by identifiable individuals with exclusive authority to enjoy, exclude, and transfer. This Part examines why that paradigm fails when applied to decentralized finance protocols and decentralized autonomous organizations. The failure is not merely technical; it reflects a fundamental mismatch between Article 12's conceptual architecture and the governance structures that now dominate the digital-asset ecosystem.

The mismatch has practical consequences. As of late 2025, decentralized finance protocols manage hundreds of billions of dollars in digital assets. Uniswap processes more trading volume than many traditional exchanges. Aave and Compound facilitate billions of dollars in loans. MakerDAO's DAI stablecoin circulates as a medium of exchange across the cryptocurrency ecosystem. These protocols are not toys or experiments; they are financial infrastructure serving sophisticated users with significant capital at stake.

Yet Article 12 cannot accommodate them. The governance tokens that control these protocols—UNI, AAVE, COMP, MKR—do not fit the single-controller paradigm. No individual holder can exercise the "exclusive" powers that Section 12-105 requires. The protocols' treasury assets are managed through collective governance, not individual authority. The smart contracts that execute protocol operations act autonomously, without human control. Article 12's framework, designed for a world of individual keyholders, cannot describe this collective, algorithmic reality.

A. The Architecture of Decentralized Governance

To understand why Article 12 fails for DAOs, one must first understand how DAOs actually operate. A DAO is not simply a group of people who happen to own the same token. It is a governance structure embedded in smart contracts, where collective decisions are made through formalized voting mechanisms and executed automatically on-chain.

1. On-Chain vs. Off-Chain Governance

DAO governance operates through two primary modalities: on-chain and off-chain voting.[51]

On-chain governance records votes directly on the blockchain and executes outcomes automatically through smart contracts. When a proposal passes, the smart contract immediately implements the specified changes—adjusting protocol parameters, transferring funds, or upgrading code. No human intermediary is required. Platforms like Compound Governor, Tally, and Aragon provide on-chain governance infrastructure.[52]

Off-chain governance, by contrast, conducts voting through external platforms and relies on trusted actors to implement results. Snapshot, the dominant off-chain voting platform, is used by approximately 96% of DAOs, including protocols like Aave and Lido.[53] Snapshot allows token holders to cast votes without paying gas fees by signing messages off-chain, with votes weighted according to token holdings at a specified block height.

Most mature DAOs employ *hybrid governance*, combining off-chain deliberation and signaling with on-chain execution. A proposal might be discussed in forums, subjected to a non-binding Snapshot vote to gauge community sentiment, and then—if it achieves sufficient support—submitted to an on-chain Governor contract for binding execution.[54] This layered structure creates multiple venues where "decisions" are made, none of which corresponds to Article 12's conception of individual control.

2. Voting Mechanisms and Power Distribution

DAO voting power is typically proportional to token holdings: one token equals one vote. But this simple formula obscures significant complexity in how voting power is calculated, delegated, and exercised.

Token-weighted voting is the baseline model. A holder of 1,000 governance tokens has 1,000 votes; a holder of 1 million tokens has 1 million votes. This creates plutocratic

[51]See Frontiers in Blockchain, Delegated Voting in Decentralized Autonomous Organizations: A Scoping Review (2025).
[52]See Compound Finance, Compound Governance (describing the Governor Bravo system).
[53]CoinDesk, Snapshot, Popular DAO Voting Platform, Finally Moves On-Chain, Atop Starknet (Sept. 9, 2024).
[54]See Aragon, Governance I - How to Set Your DAO Governance.

governance—those with more capital have more power—which critics argue replicates the inequalities of traditional finance.[55]

Quadratic voting attempts to mitigate plutocracy by making voting power proportional to the square root of token holdings. Under quadratic voting, 1,000 tokens yield approximately 31 votes, while 1 million tokens yield approximately 1,000 votes.[56]

Delegated voting allows token holders to transfer their voting power to designated representatives—often called "delegates"—who vote on their behalf.[57] Delegation addresses low voter turnout but also raises centralization concerns: research indicates that the top three MKR holders control over 78% of MakerDAO's voting power.[58]

Time-weighted voting increases voting power based on how long tokens have been held, rewarding long-term commitment over short-term speculation. Curve Finance pioneered this approach with its "vote-escrowed" CRV tokens: users lock CRV for up to four years to receive veCRV, which confers voting rights proportional to the lock duration.[59]

Conviction voting takes time-weighting further by accumulating voting power over time as tokens remain staked on a particular proposal. The longer tokens support a proposal, the more voting power they contribute—preventing last-minute voting swings and encouraging sustained community support.[60]

Each mechanism produces a different distribution of "control" over the DAO's assets and operations. Article 12's binary conception—either you control the asset or you don't—cannot capture these gradations of influence. A token holder with 51% of voting power has meaningful control over governance outcomes; a holder with 0.1% has almost none. But Article 12 makes no distinction: either the holder satisfies the control test or they don't.

3. Timelocks, Guardians, and Emergency Mechanisms

DAO governance includes safeguards that further complicate the control analysis. *Timelocks* impose mandatory waiting periods between proposal approval and execution—

[55]See Sirio Aramonte et al., DeFi and the Decentralisation Illusion, BIS Q. Rev. (Dec. 2021).
[56]Gitcoin Grants employs quadratic voting to allocate funding. See Gitcoin, Quadratic Funding.
[57]See Frontiers in Blockchain, supra.
[58]See BlockApps, Understanding the MakerDAO Governance Process for Stablecoins (Dec. 2024).
[59]See Curve Finance, Vote Escrowed CRV.
[60]See 1Hive, Conviction Voting.

typically 24 to 72 hours—during which the community can detect and respond to malicious proposals.[61] During the timelock period, who "controls" the DAO's assets? The proposal has been approved but not executed; the tokens remain in the treasury but are committed to a pending transaction. The approved proposal represents the collective will of governance participants, but that will has not yet been effectuated.

The timelock creates a window of vulnerability—and a window of opportunity. A malicious proposal might pass through governance (perhaps through vote manipulation, bribing, or exploiting low turnout), but the timelock allows the community to organize a response. Concerned participants can withdraw their assets, the protocol can activate emergency procedures, or—in some protocols—the timelock can be extended or the proposal cancelled by designated guardians.

Guardian or *veto* mechanisms allow designated addresses (often multisigs controlled by core team members) to block or pause governance actions in emergencies.[62] The Guardian's veto power creates a form of negative control—the ability to prevent action—that exists alongside the DAO's collective positive control. Optimism's DAO, for example, includes a "Security Council" with authority to veto malicious proposals during the timelock period.[63]

Emergency shutdown mechanisms allow rapid response to critical vulnerabilities. MakerDAO's Emergency Shutdown Module can halt all protocol operations if sufficient MKR is deposited—a fail-safe that overrides normal governance.[64] When triggered, the Emergency Shutdown terminates all collateral auctions, allows vault owners to withdraw collateral, and winds down the protocol in an orderly fashion. The mechanism has never been used, but its existence demonstrates the layered nature of DAO "control": normal governance can be superseded by emergency governance, which itself requires collective action (depositing MKR) rather than individual authority.

[61] See OpenZeppelin, TimelockController.
[62] See MakerDAO, Governance Module.
[63] See Optimism, Security Council.
[64] See MakerDAO, Emergency Shutdown Module.

B. MakerDAO: A Case Study in Distributed Control

MakerDAO illustrates the control problem in concrete terms. MakerDAO governs the Maker Protocol, which issues the DAI stablecoin—one of the largest decentralized stablecoins with a market capitalization exceeding $5 billion.[65]

1. The MKR Token and Voting Power

MKR is MakerDAO's governance token. MKR holders can vote on all aspects of the Maker Protocol, including: adding or removing collateral types, setting risk parameters (debt ceilings, liquidation ratios, stability fees), adjusting the DAI Savings Rate, approving protocol upgrades, and allocating treasury funds.[66]

Voting occurs through the *Chief* contract, which implements continuous approval voting.[67] Users lock their MKR in the Chief contract and receive IOU tokens in return. The locked MKR is then allocated to "slates"—sets of candidates (typically smart contract addresses representing proposed actions). The slate with the most MKR support becomes the "hat" and gains authority to execute protocol changes.

The Chief contract's continuous voting mechanism means that control is always in flux. A proposal that has the "hat" today may lose it tomorrow if MKR holders reallocate their votes. There is no moment at which any individual "has control" in the Article 12 sense; there is only a constantly shifting equilibrium of collective voting power.

2. Executive Spells and Protocol Modification

When MakerDAO governance approves a change, that change is encoded in an "Executive Spell"—a smart contract that performs one or more atomic actions on the protocol.[68] The spell might adjust the DAI Savings Rate, onboard a new collateral type, or transfer funds from the protocol surplus.

Executive Spells are deployed before voting begins, so voters know exactly what code will execute if the proposal passes. Once a spell receives sufficient MKR support and the timelock expires, anyone can call the cast() function to execute the spell. The execution is

[65] See MakerDAO, The Maker Protocol.
[66] See MakerDAO Governance Portal, https://vote.makerdao.com.
[67] See MakerDAO, Chief - Detailed Documentation.
[68] See MakerDAO, Executive Spell Documentation.

permissionless—no individual "controls" the decision to execute; the smart contract simply implements what governance has approved.

The spell mechanism has important implications for Article 12's control concept. During the period between spell deployment and execution, who "controls" the protocol assets that the spell will affect? The spell's deployer has no special authority—they merely wrote the code. The MKR voters who supported the spell have collective authority, but no individual voter can unilaterally prevent execution. The timelock guardian can block execution, but cannot redirect the assets. Control is distributed across multiple actors, each with partial authority, none with complete authority.

This architecture inverts traditional control relationships. In Article 12's paradigm, the person who controls an asset decides what happens to it. In MakerDAO, the collective decides what will happen, and the smart contracts execute that decision automatically. Control flows from governance to code, not from individual to asset.

3. The GSM and Negative Control

MakerDAO's Governance Security Module (GSM) introduces yet another layer of complexity. The GSM imposes a 48-hour delay between governance approval and execution.[69] During this period, authorized parties can cancel the pending action.

The GSM creates a form of "negative control"—the power to prevent action—that coexists with the DAO's collective positive control. A minority of MKR holders can block execution of a spell that the majority has approved, provided they coordinate quickly enough. This negative control is not exclusive (any sufficient coalition can exercise it) and is not identified with any individual.

Consider the GSM from Article 12's perspective. The collective MKR voters have "control" in the sense that they can approve protocol changes. But the GSM Guardian has "control" in the sense that it can veto those changes. Neither has exclusive control in Article 12's sense; authority is divided between an initiating power and a blocking power.

Article 12 has no framework for negative control. Section 12-105's control test asks whether a person has the power to enjoy benefits, prevent others from enjoying benefits, and

[69] See MakerDAO, Governance Module (describing the GSM Pause Delay).

transfer control. It does not address the power to prevent the collective from taking action—a distinct form of authority that is central to DAO governance.

C. The Multi-Signature Problem

Beyond token-voting governance, DAOs rely extensively on multi-signature ("multisig") wallets for treasury management and operational security. The dominant multisig solution is Safe (formerly Gnosis Safe), which secures over $100 billion in assets across the Web3 ecosystem.[70]

1. How Multisigs Work

A multisig wallet is a smart contract that requires multiple private keys to authorize transactions. The standard configuration is "M-of-N": any M signers from a set of N authorized addresses must approve a transaction before it executes. Common configurations include 2-of-3, 3-of-5, and 4-of-7.[71]

When a transaction is proposed, signers review it and approve by cryptographically signing. Once M signatures are collected, anyone can submit the transaction for execution. The process can take hours or days, depending on signer availability.

Major DeFi protocols rely on multisigs for critical operations. Uniswap's DAO manages over $2 billion through a 4-of-7 Safe wallet.[72] Compound's timelock is ultimately controlled by a multisig of community delegates. Even protocols with on-chain governance often use multisigs for emergency interventions.

2. The Control Attribution Problem

Who "controls" assets in a 3-of-5 multisig? Article 12 provides no clear answer.

Option 1: No one has control. No individual signer can unilaterally transfer the assets, so no individual satisfies Section 12-105(a)'s requirement of "exclusive power." Under this reading, multisig assets fall outside Article 12 entirely.

[70] See Safe, https://safe.global.
[71] See Safe Documentation, Multi-Signature Security.
[72] See Bitbond, Safe(Wallet) Multisig Guide for Projects (Sept. 2025).

Option 2: All five signers jointly have control. The five signers together can exercise all the powers in Section 12-105(a). But this conflicts with the "exclusive power" requirement—any three of five can act, so no subset has truly exclusive authority.

Option 3: Any three signers have control. Since any three signers can authorize a transaction, any coalition of three satisfies the control test. But this produces absurd results: the same asset would be simultaneously "controlled" by multiple overlapping groups.

Option 4: Section 12-105(c) resolves the problem. But Section 12-105(c) says that sharing power does not negate control—it does not say who has control when power is shared.

3. Implications for Secured Transactions

The control attribution problem has immediate practical consequences for secured lending. Under revised Article 9, a security interest in a CER can be perfected by control, and control-based perfection yields super-priority.[73]

Suppose a DeFi protocol wants to borrow against treasury assets held in a 3-of-5 multisig. How does the lender perfect by control? The lender cannot unilaterally control the assets. The lender might become one of the five signers, but one signer cannot satisfy the control test. The lender might insist on becoming three of the five signers—but then the borrower loses meaningful control over its own treasury.

The practical result is that multisig assets may be effectively unsecurable—or securable only through awkward workarounds that undermine the multisig's security benefits. This is a significant impediment to DeFi lending markets.

D. Governance-Token Classification Uncertainty

The difficulties described above assume that governance tokens are CERs subject to Article 12. But this assumption is itself uncertain. Governance tokens occupy a classification gray zone between Article 8 (investment securities) and Article 12 (controllable electronic records).

[73] U.C.C. § 9-326A (2022).

1. The Three-Way Taxonomy

Market participants and regulators typically distinguish three categories of digital tokens:[74]

Utility tokens provide access to products, services, or features within a blockchain ecosystem. They function like prepaid credits—valuable within their native platform but not inherently investment vehicles.

Security tokens represent ownership interests in external assets or enterprises. They function like traditional securities—entitling holders to profits, dividends, or appreciation.

Governance tokens grant voting rights over protocol parameters and treasury allocation. They do not directly represent ownership of an enterprise, but they confer economic benefits indirectly through protocol appreciation.

Governance tokens fit uneasily into this taxonomy. They have utility (voting rights), but that utility is tied to an expectation of economic benefit. They resemble securities (holders expect profits), but the "enterprise" is a smart contract without traditional issuer-investor relationships.[75]

2. The Howey Analysis

Whether governance tokens are "securities" for federal law purposes depends on the *Howey* test: an instrument is a security if it involves (1) an investment of money (2) in a common enterprise (3) with an expectation of profits (4) derived from the efforts of others.[76]

Governance tokens arguably satisfy all four prongs. But counterarguments exist for each. Governance tokens may be acquired through "liquidity mining" rather than investment. The "common enterprise" is debatable when the protocol is fully decentralized. Holders may acquire tokens for governance participation rather than profit. And in a sufficiently decentralized protocol, there is no identifiable "other" whose efforts drive returns.

The SEC has signaled that governance tokens may be securities—Commissioner Crenshaw stated that "the SEC has indicated that DAO-issued tokens usually will be

[74]See Ledger Academy, Crypto Tokens: Utility, Governance and Security Tokens Explained (Oct. 2023).
[75]See Cardozo Law Review, Separating Governance Tokens from Securities.
[76]SEC v. W.J. Howey Co., 328 U.S. 293 (1946).

considered 'securities.'"[77] But the Commission has not issued formal guidance, and the SEC's decision to close investigations of Uniswap and other DeFi protocols without action further clouds the analysis.[78]

3. The UCC Classification Cascade

Even if governance tokens are securities under *Howey*, they may or may not be "investment property" under the UCC. Article 9 defines investment property to include "security," "security entitlement," "securities account," and "commodity contract."[79] "Security" is defined in Article 8, which requires that the instrument be, among other things, "of a type dealt in or traded on securities exchanges or securities markets."[80]

Governance tokens are traded on exchanges—but cryptocurrency exchanges, not traditional securities exchanges. Whether trading on Uniswap (a decentralized exchange), Coinbase (a centralized exchange), or Binance (an offshore exchange) satisfies Article 8's "securities exchange or market" requirement is unclear. The UCC does not define these terms, and the Official Comments do not address cryptocurrency markets.

The result is classification uncertainty at multiple levels: Is the governance token a security under *Howey*? (Unclear.) If so, is it a "security" under Article 8? (Unclear.) If so, is it "investment property" excluded from Article 12? (Unclear.) This multi-layered uncertainty defeats Article 12's purpose of providing commercial-law clarity.

Parties cannot confidently structure transactions when the governing legal regime is uncertain. A lender considering a loan secured by governance tokens cannot know whether to perfect under Article 8 (control through a securities intermediary), Article 9 (filing or control), or Article 12 (control as a CER). Different perfection methods yield different priority results. The classification cascade creates irreducible legal risk that sophisticated parties may find unacceptable.

This uncertainty also affects secondary-market purchasers. A buyer of governance tokens on a cryptocurrency exchange cannot know whether they are acquiring a "security" (potentially subject to registration requirements and resale restrictions) or a CER (freely

[77]Statement on DeFi Risks, Comm'r Caroline A. Crenshaw, SEC (Nov. 9, 2021).
[78]See CLS Blue Sky Blog, Uniswap's Reprieve Reveals the Uncertainty of DeFi Regulation (Apr. 2025).
[79]U.C.C. § 9-102(a)(49) (2022).
[80]U.C.C. § 8-102(a)(15) (2022).

transferable under Article 12's take-free rule). The buyer's rights—and potential liabilities—depend on a classification question that may not be resolved until years after the purchase.

E. Algorithmic Control and Smart Contract Execution

A final gap in Article 12's framework concerns algorithmic or automated control. DeFi protocols routinely execute transactions without human intervention.

1. Smart Contract Automation

In DeFi lending protocols like Aave and Compound, collateral liquidation is fully automated.[81] When a borrower's collateral value falls below the liquidation threshold, any user can trigger the liquidation by calling a smart contract function. No human at Aave or Compound approves the liquidation.

Who "controls" the collateral during the period between deposit and liquidation? The borrower deposited it but cannot withdraw without repaying. The protocol holds it but cannot dispose of it except according to its rules. Article 12's control test assumes a person with unified authority. DeFi protocols fragment that authority across multiple actors and embed it in code.

2. The "Robot Problem"

When a smart contract has the power to transfer assets, does the smart contract "control" those assets? The question sounds absurd—smart contracts are code, not persons—but it identifies a real gap in Article 12's framework.

Section 12-105(a) asks whether "the electronic record, a record attached to or logically associated with the electronic record, or a system in which the electronic record is recorded" gives "a person" certain powers. The statute clearly contemplates persons exercising control, not algorithms. But in DeFi, algorithms exercise the powers that Article 12 attributes to persons.

Consider a yield-farming protocol that automatically moves assets between lending pools to maximize returns. The protocol has the power to "avail itself of substantially all the benefit" of the deposited assets (it earns yield), the power to "prevent others from availing themselves" (depositors cannot withdraw until they interact with the protocol), and the power

[81] See Aave Documentation, Liquidations.

to "transfer control" (it moves assets between pools). But the protocol is not a "person"—it is a smart contract without legal personality.

One might argue that the depositor retains control because the depositor can withdraw at any time by calling the appropriate function. But this conflates control with the right to terminate a relationship. A person who deposits money in a bank retains the right to withdraw, but we do not say the depositor "controls" the money while it sits in the bank—the bank controls it, subject to the depositor's contractual rights. The same logic should apply to DeFi: the protocol controls the assets, subject to the depositor's right to withdraw.

Another response might attribute control to the protocol's developers or governance participants. But in a sufficiently decentralized protocol, there may be no identifiable developers with ongoing authority, and governance participants control only the protocol's parameters—not the individual asset movements that the protocol executes automatically. The "robot problem" is not easily resolved.

F. Summary: The Scope of the Gap

Article 12's gaps are not peripheral; they go to the heart of the DeFi ecosystem:

Governance voting creates collective control that no individual exercises. Tens of billions of dollars are governed by DAO structures where Article 12's control test cannot identify a controller.

Multi-signature arrangements distribute authority among multiple keyholders in ways that Section 12-105 does not address.

Governance tokens face classification uncertainty that prevents parties from knowing which UCC article applies.

Smart contract automation executes transactions without human control, fragmenting authority in ways that Article 12 cannot accommodate.

These gaps affect real commercial transactions: secured lending against DAO treasuries, acquisitions of governance tokens, priority disputes among creditors, and the structuring of DeFi protocols themselves. Consider the practical difficulties:

A venture capital firm wants to lend $50 million to a DeFi protocol, secured by the protocol's governance token holdings. How does the lender perfect its security interest? Filing

provides some protection, but without control-based perfection, the lender lacks priority over a subsequent creditor who obtains control. But can anyone obtain control of tokens managed through DAO governance? If not, control-based perfection is unavailable—and so is the super-priority that sophisticated lenders expect.

A cryptocurrency fund wants to acquire a 20% stake in a protocol's governance tokens. The fund needs assurance that it will receive clean title—free of prior security interests or ownership claims. Article 12's take-free rule provides that assurance for qualifying purchasers. But can the fund be a qualifying purchaser if it cannot obtain "control" of the tokens? If control requires exclusive power to transfer, and governance tokens can only be transferred through the fund's individual wallet (not through protocol governance), perhaps the fund has control. But what about tokens held in the protocol's treasury? Can the fund become a qualifying purchaser of treasury tokens that no individual controls?

These are not hypothetical concerns. As institutional capital flows into DeFi, sophisticated parties need answers that Article 12 does not provide. Until Article 12 addresses decentralized governance, it will remain incomplete—a framework for yesterday's digital assets rather than tomorrow's.

III. RECENT LEGAL AND REGULATORY DEVELOPMENTS

Article 12 entered into force against a backdrop of rapidly evolving litigation, enforcement, and legislative activity. Courts are only beginning to grapple with DAOs' legal status, Congress is considering comprehensive digital-asset legislation, states are experimenting with DAO-specific entity forms, and Article 12 itself is spreading through the states at variable pace.

A. The Emerging Jurisprudence of DAO Liability

Three recent cases have begun to define the legal status of DAOs and their participants. Each case addresses a different theory of DAO liability, and together they create significant uncertainty—and significant risk—for governance-token holders.

1. CFTC v. Ooki DAO: DAOs as Unincorporated Associations

The Commodity Futures Trading Commission's enforcement action against Ooki DAO marked the first federal court ruling that a DAO can be sued as a legal entity.[82]

Ooki DAO operated the bZx Protocol, a decentralized trading platform. The CFTC alleged that Ooki DAO violated the Commodity Exchange Act by operating an unregistered futures commission merchant.[83] Critically, the CFTC alleged that the founders converted bZeroX into a DAO structure specifically "to insulate the . . . protocol from regulatory oversight."[84]

Judge William Orrick rejected arguments that Ooki DAO was merely autonomous software incapable of being sued. The court found that the CFTC had "sufficiently pleaded facts showing that Ooki DAO is an unincorporated association."[85] Crucially, the CFTC defined the association as comprised of "Ooki Token holders who have voted those tokens to govern the Ooki Protocol."[86]

[82]CFTC v. Ooki DAO, No. 22-cv-05416 (N.D. Cal. June 8, 2023).
[83]See CFTC Press Release No. 8715-23 (June 9, 2023).
[84]Id.
[85]CFTC v. Ooki DAO, 2022 WL 17822445, at *5-8 (N.D. Cal. Dec. 20, 2022).
[86]Id. at *4.

Ooki DAO adopted a strategy of "strategic nonparticipation," declining to appear. The court entered a default judgment imposing $643,542 in penalties.[87] The CFTC's Enforcement Director declared the ruling "a precedent-setting decision."[88]

2. Sarcuni v. bZx DAO: Partners All the Way Down

In *Sarcuni v. bZx DAO*, plaintiffs sued to recover losses from a hack of the bZx Protocol, arguing that all DAO token holders were liable as general partners.[89]

The Southern District of California denied the DAO's motion to dismiss, holding that plaintiffs had plausibly alleged that *all* governance-token holders could be partners subject to unlimited personal liability.[90] Unlike *Ooki DAO*, which defined the association narrowly as those who actually voted, *Sarcuni* suggested that mere token ownership could suffice for partnership liability.

3. Samuels v. Lido DAO: Venture Capital Meets Unlimited Liability

The most significant DAO litigation to date is *Samuels v. Lido DAO*, a securities class action in the Northern District of California.[91]

Lido DAO operates a "staking-as-a-service" protocol. Plaintiff Andrew Samuels purchased LDO tokens on a secondary market and sued under Section 12(a)(1) of the Securities Act.[92]

The defendants—including Andreessen Horowitz, Paradigm, and Dragonfly—argued that Lido DAO was "just autonomous software."[93] Judge Vince Chhabria rejected this, observing that Lido's actions "are not those of an autonomous software program—they are the actions of an entity run by people."[94]

On partnership liability, Judge Chhabria held that the VC defendants were partners because they "meaningfully participated" in governance.[95] The decision sent "tremors

[87]Ooki DAO Order at 11-12.
[88]CFTC Press Release No. 8715-23.
[89]Sarcuni v. bZx DAO, 2023 WL 2657633 (S.D. Cal. Mar. 27, 2023).
[90]Id. at *4-5.
[91]Samuels v. Lido DAO, No. 23-cv-06492 (N.D. Cal. Nov. 18, 2024).
[92]See Davis Wright Tremaine, Samuels v. Lido DAO: A Potential New Frontier for Liability (Jan. 2025).
[93]Samuels Order at 5-6.
[94]Id. at 6.
[95]Id. at 8-10.

through the DAO community."[96] Myles Jennings, general counsel of a16z Crypto, declared that "a California judge dealt a huge blow to decentralized governance."[97]

4. Implications for Article 12

These cases have immediate implications for Article 12's governance-token gap. If governance-token holders are partners or association members, then the tokens represent membership interests in an unincorporated entity. That raises classification questions: are membership interests "investment property" under Article 9, triggering Article 8's framework? Or are the tokens themselves CERs, separate from the membership interests they confer?

The cases also complicate the control analysis. In *Ooki DAO*, liability attached to token holders who *voted*—those who exercised governance rights. In *Sarcuni*, liability potentially extends to all token holders regardless of voting activity. If mere ownership creates partnership liability, then the token holder's "control" over governance is irrelevant to their legal exposure. But if only active voters face liability, then the distinction between holding and exercising governance rights becomes critical—a distinction Article 12 does not recognize.

The *Lido* case adds another dimension. The venture capital defendants were not merely passive token holders; they "meaningfully participated" in governance by voting on proposals and serving on committees. Their participation exposed them to unlimited personal liability—a result that may chill sophisticated investors' engagement with DAO governance. If the legal consequence of participating in governance is personal liability, rational actors will avoid participation, concentrating control in the hands of those willing to accept the risk.

This chilling effect is particularly significant for Article 12's governance-token gap. Part of the argument for extending Article 12 to governance tokens is that such tokens represent valuable assets deserving commercial-law protection. But if holding governance tokens creates potential partnership liability, the tokens' value may be diminished—rational buyers will discount for legal risk. And if participating in governance creates additional liability, the value of governance rights specifically (as opposed to any economic rights the token confers) becomes negative: the right to vote is also a risk of liability.

[96]Cointelegraph, Lawsuits Could Be Catastrophic for DAOs If Denied 'Limited Liability' (Nov. 27, 2024).
[97]Id.

The DAO liability cases also complicate the secured-lending analysis. A lender considering a loan secured by governance tokens must consider not only the token's commercial value, but the legal exposure that accompanies token ownership. If the borrower defaults and the lender forecloses on the governance tokens, does the lender become a partner in the DAO? Does the lender inherit liability for the DAO's past misconduct? These questions—unanswered by current law—add risk to secured transactions in governance tokens.

5. Doctrinal Synthesis: The Liability Taxonomy

The three cases establish a preliminary taxonomy of DAO participant liability. At one end, *Ooki DAO* imposes liability on participants who *actively vote* on governance proposals—those who manifest consent to associate through affirmative participation. At the other end, *Sarcuni* suggests that *mere token ownership* may suffice for partnership status—the capacity to participate, even if unexercised, creates the requisite co-ownership relationship. In the middle, *Lido* focuses on *meaningful participation*—a standard between active voting and mere ownership that captures engagement beyond passive holding.

This taxonomy creates strategic dilemmas for governance-token holders. Under *Ooki DAO*'s narrower standard, a holder who abstains from voting might avoid association liability—but abstention undermines the governance participation that makes decentralized protocols function. Under *Sarcuni*'s broader standard, even abstention provides no protection—the holder's mere ownership of governance rights creates partnership exposure. Under *Lido*'s intermediate standard, holders must calibrate their engagement to avoid crossing the "meaningful participation" threshold—but without clear guidance on where that threshold lies.

The doctrinal uncertainty is compounded by the lack of appellate guidance. All three cases were decided at the district court level, and none has been reviewed by a circuit court. The Ninth Circuit, which covers California (the jurisdiction for all three cases), has not addressed DAO liability. Until appellate courts provide clarity, district courts will continue developing the doctrine case by case, potentially reaching inconsistent conclusions about when and how DAO participants face liability.

6. Policy Implications: The Case for Reform

The emerging DAO liability jurisprudence strengthens the case for Article 12 reform. If governance-token holders face potential unlimited liability under current law, clear commercial-law rules become even more important. Parties need to know not only whether they can take security interests in governance tokens, but also what legal exposure accompanies token ownership and how that exposure affects the tokens' commercial value.

More fundamentally, the liability cases reveal a mismatch between existing legal categories and decentralized governance structures. Partnership law developed for small businesses with identifiable partners who share profits and management responsibilities. Unincorporated association law developed for clubs, churches, and voluntary organizations. Neither framework contemplates thousands of pseudonymous participants coordinating through smart contracts to manage billions of dollars in assets.

Article 12 reform can contribute to resolving this mismatch. By providing clear rules for governance-token property rights, the amendments would establish that governance tokens are a distinct category of commercial asset—not merely membership interests in a partnership or association. This characterization would not eliminate liability concerns (which depend on entity law, not commercial law), but it would provide transactional certainty for parties dealing with governance tokens as collateral, as traded assets, or as components of more complex financial arrangements.

7. The Legal Opinion Liability Crisis

The governance-token gap creates acute liability exposure not only for lenders and DAO participants, but for the law firms advising them. Every secured transaction involving governance tokens requires legal opinions—and the opinions being issued today rest on foundations of sand.

In a typical secured lending transaction, the lender's counsel issues a "perfection opinion" confirming that the security interest has been properly perfected and will have priority over competing claims. For traditional collateral, these opinions are routine: counsel confirms that a financing statement was filed in the correct jurisdiction, or that the secured party has possession of certificated securities. The legal analysis is well-established; the risk of error is minimal.

Governance-token collateral is different. When counsel opines that a lender has "control" of governance tokens under Article 12, counsel is making a legal conclusion that no court has validated. The opinion asserts that the lender satisfies Section 12-105(a)'s requirements—exclusive power to enjoy benefits, exclusive power to prevent others from benefiting, exclusive power to transfer control. But when the collateral is held in a multi-signature wallet, when voting rights are distributed across token holders, when smart contracts impose constraints on transfer—can any individual truly satisfy the "exclusive" power requirements?

The honest answer is: we do not know. And that uncertainty creates malpractice exposure for every law firm issuing perfection opinions on governance-token collateral.

Consider the scenario that will inevitably arise. A lender extends $50 million secured by governance tokens, relying on counsel's opinion that the security interest is perfected by control. The borrower defaults. The lender attempts to foreclose—but discovers that another creditor claims priority, arguing that the lender never had "control" under Article 12 because the multi-signature arrangement meant no individual had exclusive transfer authority. The lender loses its priority position and suffers a $30 million loss.

The lender will sue its law firm. The complaint will allege that counsel negligently opined that the lender had control when, under a proper reading of Article 12, the distributed custody arrangement precluded any individual from satisfying the control test. The law firm will defend by arguing that its interpretation was reasonable—but "reasonable" is cold comfort when the opinion proved wrong and the client lost millions.[98]

The professional-responsibility implications extend further. Legal opinions in secured transactions are often addressed to multiple parties—the lender, participants in a syndicated facility, assignees who may later acquire the loan. Opinion recipients rely on counsel's conclusions; that reliance is the opinion's purpose. When the opinion proves incorrect, *all* recipients have potential claims against the opining firm.[99]

Law firms currently issuing perfection opinions on DAO collateral face strict professional standards. An opinion that a lender "has control" under Article 12 is an assertion

[98]See Restatement (Third) of the Law Governing Lawyers § 51 (liability to client for negligent legal opinion).
[99]See ABA Comm. on Legal Opinions, Legal Opinion Principles, 53 Bus. Law. 831 (1998) (discussing reliance by opinion recipients).

of legal fact. If the assertion is wrong—if a court later holds that multi-signature arrangements preclude control, or that distributed governance defeats exclusivity—the opinion was negligent when issued, regardless of whether the error was foreseeable.

Every opinion letter signed today without a technical audit is a potential malpractice claim waiting for a market crash. When token prices decline and defaults spike, lenders will scrutinize their collateral positions. Those who discover their "perfected" security interests were never properly perfected will seek recovery from their advisors. The law firms that issued confident opinions on uncertain legal questions will bear the consequences.

The prudent response is not to stop issuing opinions—clients need legal guidance, and refusing to opine serves no one. The prudent response is to issue opinions that accurately reflect the legal uncertainty: qualified opinions that disclaim conclusions on unsettled questions, opinions that condition control conclusions on technical audits confirming custody arrangements, opinions that explicitly note the absence of judicial guidance on distributed control. Such opinions may be less satisfying to clients, but they are honest—and honesty is the best protection against malpractice liability.

The legal opinion crisis underscores the urgency of market solutions. Until the law clarifies, law firms need standardized frameworks for analyzing control in distributed arrangements. The constructive-control mechanisms discussed in Part V—qualified custody, smart-contract escrow, technical verification—provide the foundation for opinions that can withstand scrutiny. A law firm opining that a lender has control through a qualified custodian, supported by a smart-contract audit and proof-of-reserves attestation, stands on far firmer ground than a firm opining on raw multi-signature arrangements without technical verification.

The ultimate solution is *insured verification*: technical analysis of smart contract control, backed by insurance coverage. If the verification is wrong and collateral is compromised, the policy pays—shifting liability from the law firm's malpractice carrier to a purpose-built insurance product. This model mirrors title insurance in real estate: the title company verifies ownership, and the policy covers errors in that verification. Digital asset lending needs the same infrastructure. The law firm that conditions its control opinions on insured verification certificates protects both its client and itself—and positions its practice for the institutional market that demands such protections.

B. State DAO Legislation: Wyoming's DUNA

Wyoming's Decentralized Unincorporated Nonprofit Association Act (DUNA), signed March 2024 and effective July 1, 2024, represents the most ambitious state-level attempt to provide legal infrastructure for DAOs.[100]

A DUNA is a legal entity separate from its members that provides limited liability for participants.[101] Unlike general partnerships or unincorporated associations, DUNA members are not personally liable for the entity's debts.[102]

DUNAs must have at least one hundred members and must be organized for nonprofit purposes.[103] However, the statute permits DUNAs to engage in for-profit activities and pay "reasonable compensation" to members.[104]

The statute contemplates that membership can be acquired automatically through token ownership—the governing principles can be embedded in smart contracts.[105]

Limits of the DUNA Solution

While innovative, the DUNA does not solve Article 12's governance-token problem. DUNAs require affirmative adoption—a DAO that has not organized as a Wyoming DUNA remains an unincorporated association or general partnership under default law. The vast majority of existing DAOs have not adopted any legal wrapper.[106]

The DUNA structure may also be incompatible with certain DeFi activities. The nonprofit requirement—no distribution of profits to members—may conflict with protocols that distribute fees or revenues to governance-token holders.[107] Many DeFi protocols share trading fees, lending revenue, or other economic benefits with token holders. These distributions might violate the nonprofit constraint, making the DUNA unavailable for the protocols that most need legal clarity.

---

[100] Wyo. Stat. §§ 17-32-101 to -129 (2024).
[101] Wyo. Stat. § 17-32-108(a).
[102] See a16z Crypto, The DUNA: An Oasis for DAOs (Mar. 8, 2024).
[103] Wyo. Stat. § 17-32-103(a).
[104] Wyo. Stat. § 17-32-105(b).
[105] Wyo. Stat. § 17-32-106(a).
[106] See Winston & Strawn, DAOs Watch Out (Dec. 2024).
[107] See Preston Byrne, The Wyoming DUNA Act, Section-by-Section (Mar. 8, 2024).

Third, and most relevant for Article 12, the DUNA does not clarify how commercial law should treat DUNA interests or DUNA-controlled assets. If a DUNA issues governance tokens that represent membership interests, are those tokens "securities" under Article 8 (as membership interests in an organization)? Are they CERs under Article 12? If the DUNA holds treasury assets, can a creditor perfect a security interest in those assets by control—and if so, who has control?

Wyoming has pioneered DAO-specific entity legislation, and other states may follow. But commercial law has not kept pace. Article 12 was drafted without DUNAs in mind, and the interaction between entity-law innovations and UCC rules remains uncharted territory.

C. Federal Legislation: FIT21

The Financial Innovation and Technology for the 21st Century Act (FIT21) passed the House in May 2024 with bipartisan support (279-136).[108]

FIT21 would divide digital-asset regulation between the SEC and CFTC based on whether a digital asset is "decentralized." An asset qualifies as decentralized if no person has "unilateral authority" to control the blockchain and no person has controlled 20% or more of the voting power.[109]

FIT21 passed the House but stalled in the Senate during the 118th Congress. Prospects have brightened in 2025, with House Financial Services Chairman French Hill stating intent to present FIT21 for President Trump's signature.[110] The bill's bipartisan support in the House—71 Democrats joined all but three Republicans in voting for passage—suggests that comprehensive digital-asset legislation may be achievable in the current Congress.

FIT21's approach differs from Article 12's in a significant respect. FIT21 treats decentralization as a binary classification: either an asset is on a "decentralized" blockchain (and regulated as a commodity) or it is not (and regulated as a security). Article 12, by contrast, requires individual-level control regardless of the underlying blockchain's

[108]See King & Spalding, House Passes FIT21 (May 2024).
[109]H.R. 4763 § 101.
[110]See Jones Day, Regulating Digital Assets: FIT21 Seems to Fit the Bill (Feb. 2025).

decentralization status. A governance token on the most decentralized blockchain still requires a "person" with "exclusive" powers under Section 12-105.

This distinction matters because FIT21's decentralization test focuses on the *system*, while Article 12's control test focuses on the *holder*. A blockchain can be decentralized (no person controls it) while individual tokens on that blockchain are controlled by individual holders. FIT21 would give such tokens favorable regulatory treatment; Article 12 would accommodate them through the existing control framework. But governance tokens held collectively through DAO mechanisms present a different case: the blockchain may be decentralized, *and* no individual controls the tokens. FIT21 would classify such tokens as commodities; Article 12 cannot accommodate them at all.

Implications for Article 12

If enacted, FIT21 would have complex interactions with Article 12. On one hand, FIT21's decentralization framework might help resolve classification uncertainty. On the other hand, FIT21 does not address commercial law—it allocates regulatory jurisdiction but does not specify treatment for secured transactions or priority rules.

Moreover, FIT21's decentralization test may conflict with Article 12's control requirement. FIT21 treats decentralization as a virtue; Article 12 treats control as the organizing concept. A governance token on a "decentralized" system (favored under FIT21) may be a token over which no person has control (problematic under Article 12). The two frameworks pull in opposite directions.

D. Article 12 Adoption: An Incomplete Patchwork

As of early 2025, Article 12 has been enacted in approximately 25 states and the District of Columbia.[111] Washington and California have both enacted the amendments, providing coverage for the two states with the most significant digital-asset activity. But the patchwork remains incomplete.

Several factors complicate adoption. First, some states have enacted *non-uniform* amendments—variations from the official text that may create conflicts when transactions span state lines. Texas and Tennessee, for example, have enacted versions with material

[111] See Miller Nash LLP, UCC Article 12 (Mar. 5, 2025).

deviations.[112] Second, transition periods in early-adopting states are expiring. Most states that enacted Article 12 in 2023 provided transition periods ending July 1, 2025, after which the new rules fully apply. Third, key states like New York have not yet enacted the amendments, creating uncertainty for transactions involving parties or assets in those jurisdictions.

The adoption patchwork has immediate practical consequences. A secured party seeking to perfect a security interest in governance tokens must determine which state's law governs and whether that state has enacted Article 12. If the state has enacted Article 12, the secured party must then navigate the control test—with all its difficulties for distributed governance structures. If the state has not enacted Article 12, the secured party faces even greater uncertainty: the older UCC provisions were not drafted with digital assets in mind, and courts may struggle to apply them.

The proposed amendments would add another layer to this complexity. States that have already enacted Article 12 would need to enact the amendments separately. States that have not yet enacted Article 12 might adopt the amendments simultaneously with the original provisions, or might enact Article 12 without the amendments. The result could be a three-tier system: states with original Article 12, states with amended Article 12, and states with neither. Careful drafting and coordinated enactment efforts will be essential to minimize the resulting fragmentation.

[112] See Willkie Farr & Gallagher, UCC Article 12 (Aug. 2024).

IV. COMPARATIVE PERSPECTIVES

Article 12's governance-token gap is not unique to the United States. Jurisdictions worldwide are grappling with the private-law treatment of digital assets.

A. United Kingdom: The Third Category of Personal Property

In June 2023, the UK Law Commission published its final report on digital assets, recommending statutory recognition of a "third category" of personal property.[113] English law traditionally recognizes two categories: "things in possession" and "things in action." Crypto-tokens fit neither comfortably.[114]

The Law Commission recommended legislation confirming that a thing "is not prevented from being the object of personal property rights merely because it is neither a thing in possession nor a thing in action."[115] The Property (Digital Assets etc) Bill was introduced in September 2024.[116]

Like Article 12, the UK framework centers on "control." But the Law Commission's treatment is more nuanced, identifying control as a "spectrum" rather than a fixed test.[117] The Commission recommended an expert panel to develop guidance on control in distributed arrangements—an acknowledgment that the control concept requires adaptation for decentralized structures.[118]

The UK approach differs from Article 12 in a significant respect: it does not make control the sole organizing principle for property rights. Instead, the Law Commission identifies control as one of several "indicia" of data objects that can be the subject of property rights, alongside uniqueness, rivalrousness, and divestibility.[119] This multi-factor approach may prove more adaptable to distributed governance structures than Article 12's control-centric framework.

---

[113]Law Commission, Digital Assets: Final Report (Law Com No 412, 2023).
[114]See id. at paras. 3.1-3.54.
[115]Id. at para. 4.43.
[116]Property (Digital Assets etc) Bill [HL], 2024-25, Bill 4.
[117]Law Commission, supra, at paras. 5.35, 5.48-5.62.
[118]Id. at para. 20.57.
[119]Id. at para. 5.15.

1. The Multi-Factor Alternative

The Law Commission's multi-factor framework deserves closer examination as a potential alternative to Article 12's control-centric approach. The Commission identified four characteristics that make data objects suitable for property rights:

Uniqueness refers to the object's distinctness from other data objects—its capacity to be singled out and identified. Governance tokens satisfy this criterion: each token on a blockchain has a unique identifier, and token balances are tracked with precision at the address level.

Rivalrousness means that use or consumption by one person necessarily limits use by others. Unlike information (which can be copied infinitely), digital assets on a blockchain are rivalrous: if Alice holds a governance token, Bob cannot simultaneously hold the same token. The blockchain's consensus mechanism enforces this rivalrousness.

Divestibility is the capacity to be transferred from one person to another. Governance tokens are readily divestible through blockchain transactions—indeed, their transferability is a defining feature.

Control in the UK framework is not a binary test but a "spectrum" reflecting varying degrees of practical authority over the asset. A person may have strong control (exclusive possession of a private key), weak control (one key among several in a multisig), or no control (a minority token holder who cannot influence governance outcomes). The Commission explicitly rejected the view that control must be "exclusive" to ground property rights.[120]

This multi-factor approach has significant advantages for distributed governance structures. A governance token clearly satisfies uniqueness, rivalrousness, and divestibility—even when no single person has exclusive control. Under Article 12, the absence of exclusive control potentially disqualifies the token from CER status. Under the UK framework, the token can still be the subject of property rights based on the other factors.

The multi-factor approach also provides more granular analysis of commercial transactions. A secured lender taking governance tokens as collateral can be understood as acquiring a property interest in assets that are unique, rivalrous, and divestible—even if the

[120]Law Commission, supra, at para. 5.52.

lender's "control" is limited by the distributed governance structure. The lender's rights attach to the tokens' property characteristics, not solely to a contested notion of control.

Article 12's drafters might have adopted a similar approach. Instead of making control definitional (a CER is a record that *can be subjected to control*), Article 12 might have defined CERs by their functional characteristics and then addressed control separately in the context of perfection and priority. This would have preserved control's role in secured transactions while avoiding the definitional problems that exclude distributed-governance assets from Article 12's scope entirely.

The UK approach is not without difficulties. A multi-factor test may be harder to apply than a single bright-line rule. Courts must weigh multiple considerations rather than asking a single yes-or-no question. But the flexibility may be worth the complexity—particularly for an asset class as varied as digital assets, where governance structures range from single-key wallets to sophisticated DAO mechanisms.

The proposed amendments in Part V take a different approach: they preserve Article 12's control-centric structure while expanding the control concept to accommodate distributed governance. This approach has the advantage of working within Article 12's existing framework, minimizing disruption to the provisions already enacted in over thirty states. But the UK's multi-factor alternative represents a road not taken—one that future revisions might consider if the control-centric approach proves unworkable in practice.

2. Beyond Control: Alternative Property Paradigms

The governance-token gap invites broader reflection on whether "control" should be the sole organizing concept for digital-asset property. Traditional property law employs multiple concepts—possession, title, ownership, use rights—that do not reduce to a single criterion. Digital-asset law might similarly benefit from conceptual pluralism.

Possession as factual control. In traditional property law, possession is a factual state rather than a legal conclusion. A person possesses land by occupying it; a person possesses chattels by holding them. Possession creates a presumption of ownership and grounds certain legal protections (adverse possession, possessory actions) even when the possessor is not the "true" owner. Digital assets might be analyzed similarly: a person who holds private keys to a wallet "possesses" the assets in that wallet, regardless of whether they satisfy Article 12's control test. This possessory approach would extend property protections to governance-

token holders based on their factual relationship to the tokens, not on contested questions of "exclusive" control.

Bundle-of-rights analysis. Property has long been conceptualized as a "bundle of rights"—the right to use, exclude, transfer, and destroy, among others.[121] Governance tokens confer specific rights (voting, proposing, delegating) that differ from the rights associated with traditional property or even with other digital assets like Bitcoin. A bundle-of-rights approach would analyze governance tokens by reference to the specific rights they confer, rather than forcing them into a control framework designed for assets with different characteristics. This approach might reveal that governance tokens warrant different commercial-law treatment than other CERs—perhaps different perfection rules, different priority structures, or different take-free provisions.

Relational property. Some property theorists have argued that property is fundamentally relational—it concerns relationships among persons with respect to things, not relationships between persons and things.[122] This relational perspective is particularly apt for governance tokens, which are valuable precisely because they establish relationships among token holders (through voting, delegation, and collective decision-making). A relational approach would analyze governance-token property rights by reference to the governance relationships the tokens create and maintain, rather than by reference to abstract control criteria.

Information-based property. Digital assets are, at their core, information—data recorded on distributed ledgers. Some scholars have argued that digital-asset property should be analyzed through the lens of information law, drawing on concepts like access, attribution, and integrity rather than possession and control.[123] Under this view, a governance-token holder's property interest might be understood as an interest in the information that the token represents (voting power, protocol rights) rather than as control over a thing. This reconceptualization could support property protections without requiring satisfaction of Article 12's control test.

---

[121] See Wesley Newcomb Hohfeld, Fundamental Legal Conceptions as Applied in Judicial Reasoning, 26 Yale L.J. 710 (1917).
[122] See Thomas W. Merrill & Henry E. Smith, The Morality of Property, 48 Wm. & Mary L. Rev. 1849 (2007).
[123] See Joshua A.T. Fairfield, BitProperty, 88 S. Cal. L. Rev. 805 (2015).

These alternative paradigms are not mutually exclusive, and none provides a complete solution to the governance-token gap. But they illustrate that control-centric analysis is a choice, not a necessity. Article 12's drafters chose control as the organizing concept, influenced by the mental model of individual cryptocurrency holders with exclusive possession of private keys. The governance-token gap reveals the limitations of that choice. Future reforms—whether to Article 12 or to the broader framework of digital-asset property law—might draw on these alternative paradigms to develop more flexible approaches.

B. Switzerland: Ledger-Based Securities

Switzerland's DLT Act, enacted 2020-2021, created "ledger-based securities" (*Registerwertrechte*)—a new category that can be created, transferred, and pledged directly on a distributed ledger.[124]

However, ledger-based securities require an underlying contractual claim against an identifiable issuer.[125] Governance tokens that confer only voting rights may not qualify. And the framework requires a Swiss-incorporated entity with regulatory authorization—requirements that decentralized protocols cannot satisfy.[126]

The Swiss approach reflects a different philosophy than Article 12. Rather than creating a new category of property (the CER), Switzerland adapted existing categories (securities) to new technologies (distributed ledgers). This adaptation preserves the conceptual framework of traditional securities law—with its emphasis on issuers, intermediaries, and regulatory oversight—while enabling blockchain-based transactions. The approach works well for tokenized traditional securities but struggles with natively digital assets that have no issuer and no underlying claim.

C. European Union: Markets in Crypto-Assets (MiCA)

The EU's MiCA became fully applicable December 30, 2024.[127] MiCA classifies crypto-assets into three categories: asset-referenced tokens (stablecoins backed by multiple

[124]Swiss Code of Obligations arts. 973d-973i (as amended by DLT Act).
[125]See Global Legal Insights, Blockchain & Cryptocurrency Laws 2026: Switzerland.
[126]See IMD, New Tech Act in Switzerland (July 2023).
[127]Regulation (EU) 2023/1114 (MiCA).

assets), e-money tokens (stablecoins backed by single currency), and other crypto-assets (a catch-all including governance tokens).[128]

MiCA's treatment of governance tokens is notably light. Governance tokens typically fall into the "other crypto-assets" category, which has the least prescriptive requirements. Issuers must publish a "white paper" describing the token and its risks, but there is no authorization requirement.[129] Critically, MiCA does not address who "owns" governance tokens or how property rights in them transfer—the underlying property questions that Article 12 attempts to answer remain governed by member-state law.[130]

Importantly, MiCA provides that it does not apply to crypto-asset services that are "fully decentralized."[131] This exclusion creates a regulatory gap for the most decentralized structures—precisely the structures that Article 12 also struggles to accommodate. The EU has effectively acknowledged that its regulatory framework cannot reach truly decentralized protocols, while the underlying property-law questions remain unresolved.

D. UNIDROIT Principles on Digital Assets

The UNIDROIT Principles, adopted May 2023 and published October 2023, represent the most ambitious attempt to harmonize private-law rules for digital assets internationally.[132]

Like Article 12, the UNIDROIT Principles center on "control." Principle 8 requires: exclusive ability to prevent others from obtaining benefit; ability to obtain benefit; and exclusive ability to transfer control.[133] This definition closely parallels Article 12, reflecting the influence of American commercial law on international harmonization efforts.

The UNIDROIT Principles acknowledge the challenge of multi-party arrangements. Principle 8 Commentary notes that "control may be shared among multiple persons" and that "the determination of which person or persons have control of a digital asset is a factual

[128]See ESMA, Markets in Crypto-Assets Regulation.
[129]MiCA art. 4.
[130]See Norton Rose Fulbright, Regulating Crypto-Assets in Europe: Practical Guide to MiCA (Dec. 2024).
[131]MiCA, recital 22.
[132]UNIDROIT, Principles on Digital Assets and Private Law (2023).
[133]UNIDROIT Principles, Principle 8.

matter."[134] But this acknowledgment does not provide operational guidance for determining who has control in a multi-signature arrangement or token-voting governance structure.

Despite their sophistication, the UNIDROIT Principles suffer from the same governance gap as Article 12. The Principles' control definition—requiring "exclusive" ability—does not accommodate distributed governance. The Principles recognize that control may be "shared," but they do not specify how shared control should be attributed, perfected against, or prioritized among competing claimants. The governance-token gap is not merely American; it is embedded in the emerging international consensus on digital-asset property law.

E. Summary: A Global Governance Gap

The comparative survey reveals a striking pattern: jurisdictions worldwide have converged on "control" as the organizing concept for digital-asset property rights, and none has satisfactorily addressed distributed governance. The United Kingdom recognizes control as a "spectrum" but has not yet developed rules for multi-party arrangements. Switzerland requires identifiable issuers, excluding decentralized protocols. The European Union exempts "fully decentralized" services from its regulatory framework. UNIDROIT acknowledges shared control but provides no operational rules for attribution.

The convergence on control reflects the concept's intuitive appeal: just as possession anchors property rights in tangible goods, control anchors property rights in digital assets. But the convergence also means that the governance-token gap is global. A party seeking to perfect a security interest in governance tokens faces uncertainty not only under Article 12, but under virtually every developed jurisdiction's framework for digital-asset property.

This global gap creates an opportunity for American leadership. The Uniform Law Commission, with its tradition of commercial-law innovation and its influence on international harmonization, can develop solutions that other jurisdictions may adopt. Article 12 reform can position American law at the forefront of digital-asset property rights—providing a model for the UK's expert panel, informing the EU's eventual treatment of decentralized protocols, and shaping future revisions to the UNIDROIT Principles.

[134]UNIDROIT Principles, Principle 8 Commentary 8.5-8.11.

V. BRIDGING THE GAP: CONSTRUCTIVE CONTROL AND MARKET SOLUTIONS

The governance-token gap is real, and legislative reform would provide the clearest path to resolution. But lenders, investors, and market participants cannot wait for the Uniform Law Commission to draft amendments, for fifty state legislatures to enact them, and for courts to interpret them. That process could take five to ten years—an eternity in digital-asset markets. The market needs certainty today.

This Part proposes a practical bridge: a "Constructive Control" standard that enables secured lending against governance tokens *within* existing Article 12, supplemented by contractual mechanisms, technical verification, and risk-transfer products. This approach does not require legislative change. It requires market participants to develop standardized practices that courts can recognize as satisfying Article 12's control requirements—or that provide equivalent commercial certainty even if Article 12 technically does not apply.

A. The Constructive Control Framework

Article 12's control test requires that a person have (1) the power to enjoy substantially all the benefit of the CER, (2) the exclusive power to prevent others from enjoying substantially all the benefit, and (3) the exclusive power to transfer control.[135] For governance tokens held in distributed arrangements, no individual may satisfy this test literally. But the question is whether parties can *construct* arrangements that courts will recognize as satisfying the test—or that provide equivalent protection regardless of technical Article 12 compliance.

1. Custody-Based Constructive Control

The most straightforward path to constructive control is qualified custody. A lender taking governance tokens as collateral can require that the tokens be transferred to a custodian that (a) holds exclusive possession of the private keys, (b) acknowledges the lender's security interest, and (c) agrees to follow the lender's instructions upon default.

Under this arrangement, the *custodian* satisfies Article 12's control test: the custodian holds the keys, can prevent others from transferring the tokens, and can transfer control at the lender's direction. The lender perfects by obtaining the custodian's acknowledgment under

[135] U.C.C. § 12-105(a).

Section 12-105(e), which provides that control can be established through a "control agreement" with the person having control.[136]

Qualified custody resolves the distributed-control problem by interposing a controlled entity. The borrower deposits governance tokens with the custodian; the custodian holds them in a segregated wallet; the lender has contractual rights against the custodian. From Article 12's perspective, the custodian—not the distributed governance structure—is the relevant "person" with control.

Several qualified custodians now offer governance-token custody services specifically designed for secured lending. These custodians maintain regulatory licenses (state money-transmitter licenses or federal bank charters), carry insurance against theft and operational failure, and provide institutional-grade security. Anchorage Digital, BitGo, Coinbase Custody, and Fireblocks all offer such services.[137]

A critical distinction for insurance underwriting: even where full "initiative control" (the power to transfer) remains uncertain, **negative control**—the power to *block* unauthorized transfers—may be sufficient for coverage purposes. A multi-signature arrangement where the lender holds one of three required keys may not satisfy Article 12's exclusive-transfer requirement, but it demonstrably prevents theft: no transfer can occur without the lender's signature. Insurance carriers value this blocking power because it stops the loss, even if it does not give the lender unilateral initiative. This insight is foundational: verification insurance can underwrite negative control arrangements that Article 12 may not recognize, providing commercial certainty where legal certainty remains elusive.

2. Smart-Contract Escrow

For parties seeking to avoid third-party custodians, smart-contract escrow provides an alternative. The borrower deposits governance tokens into an escrow smart contract that enforces the security agreement's terms algorithmically. The contract is programmed to release tokens only upon satisfaction of specified conditions: repayment of the loan, or transfer to the lender upon verified default.

[136] U.C.C. § 12-105(e).

[137] See Coinbase Institutional, Digital Asset Custody for Institutions (2024); BitGo, Qualified Custody Solutions (2024).

Smart-contract escrow raises novel questions under Article 12. Does a smart contract "have" control? The contract holds the private keys (or controls the token balances), can prevent unauthorized transfers, and can transfer tokens according to its programming. But a smart contract is not a "person" in the traditional sense—it is code, not a legal entity.

The better analysis treats the smart contract as an agent of the parties who deployed it. The lender and borrower jointly create the escrow arrangement; the contract executes their agreed-upon terms. For control purposes, the relevant question is whether *the lender* can cause the contract to transfer control—and the answer is yes, upon satisfaction of the default conditions. This agency analysis supports a finding that the lender has constructive control through the smart-contract mechanism.[138]

Several protocols now offer standardized smart-contract escrow for secured lending. Aave and Compound enable overcollateralized borrowing with automatic liquidation upon undercollateralization. PWN Protocol provides peer-to-peer lending with customizable loan terms.[139] These protocols can be adapted for governance-token collateral, providing off-the-shelf infrastructure for constructive-control arrangements.

3. Contractual Control Agreements

Even where technical control is uncertain, contractual mechanisms can provide equivalent commercial protection. A comprehensive control agreement between lender and borrower can specify custody arrangements, voting rights during the loan term, distribution rights for airdrops or rewards, default triggers, remedies upon default, and dispute resolution mechanisms.

These contractual provisions operate independently of Article 12. Even if the lender lacks "control" under Section 12-105, the borrower's contractual obligations are enforceable. The lender can sue for breach of contract, obtain specific performance requiring token transfer, or pursue the borrower's other assets. The contract creates *in personam* rights against the borrower, supplementing any *in rem* rights the lender might have under Article 12.

Contractual control agreements also provide evidence of the parties' intent, which may be relevant to Article 12 analysis. Courts interpreting "control" in novel contexts will look to the parties' understanding. An agreement specifying that the lender "has control of the

[138]Cf. Restatement (Third) of Agency § 1.01 (agency relationship).
[139]See PWN Protocol Documentation, https://docs.pwn.xyz.

Collateral for purposes of Article 12 of the Uniform Commercial Code" may influence judicial interpretation—particularly where the agreement is industry-standard and reflects market consensus about control's meaning in distributed-governance contexts.

B. Technical Verification and Audit Standards

Constructive control requires not only legal arrangements but also technical verification. A lender claiming control must be able to demonstrate that the claimed control actually exists—that the custody arrangement is secure, that the smart contract functions as specified, that the borrower cannot unilaterally access the collateral.

1. Proof of Reserves and On-Chain Verification

Proof-of-reserves attestations, developed initially for cryptocurrency exchanges, can be adapted for governance-token collateral. A proof-of-reserves audit verifies that a custodian actually holds the assets it claims to hold, using cryptographic proofs that link on-chain balances to off-chain representations.[140]

Blockchain transparency enables continuous verification that would be impossible with traditional collateral. A lender can monitor the collateral wallet in real time, observing any transfers, governance votes, or other activity. Automated alerts can notify the lender if tokens are moved unexpectedly or if collateral value declines below agreed thresholds. Platforms like Nansen, Arkham, and Chainalysis provide wallet monitoring, transaction tracing, and risk scoring.

2. Smart-Contract Audits

For smart-contract escrow arrangements, code audits are essential. A reputable security auditor reviews the escrow contract's code, identifies vulnerabilities, and attests that the contract functions as specified. Leading auditors include Trail of Bits, OpenZeppelin, Consensys Diligence, and Certik.[141]

The audit report becomes part of the loan documentation, providing the lender with assurance that the technical infrastructure supports the claimed control. Audit scope should include access controls, token handling, upgrade mechanisms, and edge cases.

---

[140] See Nic Carter & Hasu, Proof of Reserves: A Guide to Crypto Reserve Attestations (2022).
[141] See OpenZeppelin, Smart Contract Security Audits (2024).

3. The Control Certificate: Mapping Code to Law

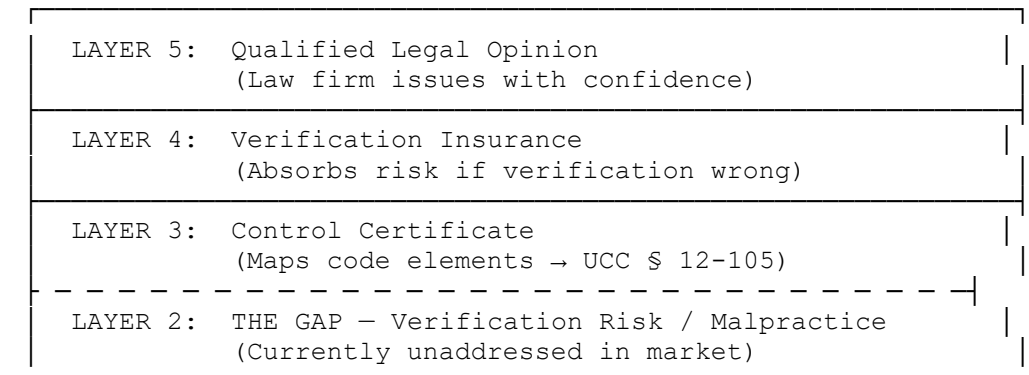
The market needs a standardized deliverable that bridges technical audit and legal opinion—a **Control Certificate** that maps specific smart contract elements to specific Article 12 requirements. No such standard currently exists.[142]

A comprehensive Control Certificate would document: (1) the specific wallet addresses or smart contract holding the collateral; (2) analysis of access controls—who holds private keys, what multi-signature requirements exist, whether admin keys or upgrade proxies could transfer tokens without the lender's consent; (3) explicit mapping of each control element to Section 12-105(a)'s requirements; and (4) ongoing monitoring commitments for the life of the loan.

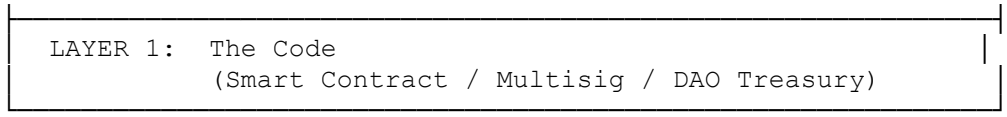
Such certificates could become standard deal documentation, analogous to title commitments in real estate transactions or representations and warranties in M&A. The lender receives not merely an opinion that control exists, but a verified, auditable analysis of *how* control exists—which code elements satisfy which legal requirements. This transparency supports both the legal opinion and the insurance underwriting that backs it.

The infrastructure to produce such certificates does not yet exist at scale. Building it requires integration of smart contract analysis (decompiling bytecode, identifying control patterns), legal framework mapping (translating code to UCC requirements across jurisdictions), and ongoing monitoring (alerting on state changes that could invalidate control). The firm or platform that standardizes this workflow will occupy a position analogous to title companies in real estate—essential infrastructure for every transaction.

Figure 1: The Liability Shield Architecture



[142]This gap creates both liability exposure and market opportunity. Law firms issue control opinions without standardized technical verification; when those opinions prove incorrect, the claim lands on the firm's malpractice policy—or nowhere.



The Control Certificate and Verification Insurance (Layers 3-4) bridge the gap between code and legal opinion, absorbing the malpractice risk that currently falls on law firms.

C. Risk Transfer: Insurance and Guarantees

Even robust constructive-control arrangements cannot eliminate all risk. The law may evolve adversely; courts may reject the constructive-control analysis; technical failures may compromise security arrangements. Risk-transfer mechanisms—insurance and guarantees—provide the final layer of protection and may ultimately prove the most important.

Every major asset class has verification insurance. Real estate has title insurance—a market exceeding $20 billion in annual premiums. M&A transactions have representations and warranties insurance—a market exceeding $3 billion. Digital asset lending has nothing: no standard verification protocol, no insurance coverage, no institutional backstop when collateral disappears through an undisclosed admin key or upgrade proxy.[143]

1. Custody and Title Insurance

Qualified custodians typically carry insurance against theft, hacking, and operational failure. Coverage limits vary—Coinbase Custody reportedly carries $320 million in crime insurance; BitGo offers up to $250 million—but policies increasingly cover digital-asset custody losses.[144]

Traditional title insurance is being adapted for digital assets. Several insurers now offer policies protecting against "chain of title" defects: risks that the purported owner did not have valid title, that prior liens encumber the asset, or that the asset was stolen or fraudulently transferred before the insured acquired it.

The deeper opportunity is *verification insurance*—coverage that protects against errors in the control analysis itself. If a Control Certificate incorrectly concludes that a lender has exclusive control, and collateral is subsequently transferred through an undisclosed admin key, verification insurance would cover the loss. This product does not yet exist at scale, but

[143]The title insurance parallel is instructive. Title insurance emerged because real property transactions required assurance that the seller actually owned what they purported to sell. Digital asset transactions present the same fundamental problem: does the borrower actually control what they claim to pledge?

[144]See Coinbase Custody, Insurance and Security (2024).

the underwriting logic is sound: smart contract verification is a quantifiable, bounded risk with documented loss history from prior exploits.

Just as title insurance became infrastructure for real estate transactions—no institutional lender closes without it—verification insurance could become infrastructure for digital asset lending. The carrier that commits to requiring standardized control verification as a condition of coverage will create a structural moat: verification becomes not merely best practice but a prerequisite for institutional participation.

2. Legal-Risk Insurance

The most novel risk-transfer mechanism addresses the legal uncertainty itself. Specialized insurers offer policies covering adverse legal developments—court decisions, regulatory actions, or legislative changes that impair the insured's expected legal position.[145]

For governance-token lending, legal-risk insurance could cover the risk that a court holds the lender does not have "control" under Article 12, that the governance tokens are reclassified as securities (triggering Article 8), or that the DAO is held to be a general partnership (exposing the lender to entity liability). These policies are expensive—premiums may range from 2% to 5% of coverage annually—but they provide certainty where the law does not.

D. Market Infrastructure and Standardization

Constructive control will become more effective as market infrastructure develops and standards emerge.

1. Industry Standards and Documentation

Trade associations and industry groups are developing standards for digital-asset custody, lending, and collateral management. The Chamber of Digital Commerce, the Blockchain Association, and the Digital Asset Markets Association have all published guidance on best practices.[146] These standards, while not legally binding, provide frameworks that courts may recognize as establishing industry custom.

[145] See Ondo Finance, Legal Risk Insurance for DeFi (2024).
[146] See Chamber of Digital Commerce, Digital Asset Custody Standards (2023).

Standardized documentation is equally important. Just as the Loan Syndications and Trading Association (LSTA) developed standardized documents for syndicated loans, industry groups are developing standardized documents for digital-asset lending. Standardized security agreements, control agreements, and custody terms reduce transaction costs and increase the predictability of judicial interpretation.

2. Specialized Lending Platforms

Institutional lending platforms are emerging that provide end-to-end infrastructure for governance-token secured lending. These platforms integrate custody, collateral monitoring, margin management, and liquidation into unified systems designed for institutional participants.

The next generation of platforms—including Maple Finance, Clearpool, and TrueFi—incorporates lessons from earlier failures, providing more robust collateral management, better risk disclosure, and improved governance.[147] These platforms can provide the infrastructure that individual lenders lack, making governance-token secured lending more accessible and more standardized.

E. From Bridge to Permanent Solution

The constructive-control framework is a bridge, not a destination. It enables market activity today, but it does not resolve the underlying legal uncertainty. A lender relying on constructive control is making a bet—a reasonable bet, supported by contractual protections and risk transfer, but a bet nonetheless—that courts will recognize the claimed control or that the contractual backstops will prove adequate.

The permanent solution remains legislative reform. The Uniform Law Commission should eventually amend Article 12 to explicitly address distributed control, multi-signature arrangements, and governance tokens. But legislative reform takes time—the ULC's drafting process is deliberate; state enactment is piecemeal; judicial interpretation is gradual.

In the interim, the market cannot wait. Constructive control provides the bridge—imperfect, improvised, but functional—that enables governance-token secured lending to proceed while the legislative process unfolds. The market's adoption of constructive-control practices may itself influence the legislative process. If courts recognize custody-based

[147] See Maple Finance, Institutional Lending Protocol (2024).

control, if smart-contract escrow becomes routine, if industry standards emerge and prove workable, legislators may codify what the market has developed.

By developing robust constructive-control mechanisms, market participants are not merely bridging a gap—they are helping to build the legal infrastructure that will eventually close it. The relationship between market practice and legal reform is iterative: practice informs law, and law shapes practice. The time to start building is now.

CONCLUSION

The 2022 Amendments to the Uniform Commercial Code represent a watershed in American commercial law's engagement with digital technology. Article 12 establishes, for the first time, a comprehensive framework for property rights in electronic records that can be subjected to control. The take-free rule promotes market liquidity; control-based perfection enables secured lending; and integration with Article 9 situates digital assets within the familiar architecture of commercial law.

But Article 12's achievements should not obscure its limitations. The control paradigm that structures Article 12 assumes a world of individual actors exercising exclusive authority over digital assets. Decentralized finance operates differently. Governance tokens distribute authority across thousands of participants who act through collective voting. Multi-signature wallets require coordination among multiple keyholders. Smart contracts execute transactions automatically, without human intervention. The "exclusive" control that Article 12 requires is precisely what DeFi structures are designed to avoid.

The proposed amendments do not abandon the control concept; they extend it. Governance tokens would become recognized CERs, with control defined by reference to the token itself rather than the protocol it governs. Multi-signature arrangements would have clear rules specifying when participants have collective control. DAO treasuries would have workable perfection mechanisms suited to collective ownership. And "negative control"—the power to block without the power to initiate—would receive limited recognition appropriate to its practical significance.

These reforms are urgent. Courts are imposing liability on DAO participants without adequate legal frameworks for understanding distributed governance. In *Ooki DAO*, token holders who voted faced liability as association members. In *Sarcuni*, all token holders potentially faced partnership liability. In *Lido*, venture capital firms that participated in governance confronted unlimited personal exposure. These cases create powerful disincentives for governance participation—disincentives that may concentrate control in fewer hands and undermine the decentralization that makes DeFi distinctive.

Meanwhile, legislatures are creating new organizational forms whose relationship to commercial law remains unclear. Wyoming's DUNA provides limited liability for DAO participants, but does not specify how DUNA interests interact with Article 12's framework.

Federal proposals like FIT21 would establish regulatory classifications for digital assets, but do not address the commercial-law questions of property rights, perfection, and priority. International bodies are converging on control-based principles for digital-asset law, but none has adequately addressed distributed governance. Article 12 reform should lead this evolution, not lag behind it.

The Uniform Law Commission has navigated similar transitions before. The original UCC itself was a response to changing commercial practices—a recognition that twentieth-century commerce required legal infrastructure that nineteenth-century doctrine could not provide. Article 4A's wire-transfer rules, Article 2A's lease provisions, and Article 8's indirect-holding system all extended commercial law to new practices. Each extension preserved the UCC's core concepts while adapting them to new commercial realities. Article 12 was the latest such extension, and the proposed amendments would continue the tradition.

The governance-token gap is not a flaw in Article 12's design; it reflects the genuinely novel characteristics of decentralized governance. No prior commercial practice required legal rules for distributed control, token voting, or collective treasury management. The drafters of Article 12 cannot be faulted for failing to anticipate structures that emerged after their work was largely complete. The 2022 Amendments were drafted primarily between 2019 and 2021, when the DeFi ecosystem was far smaller and less sophisticated than it is today.

But the gap must now be addressed. The market has evolved; commercial law must evolve with it. As of late 2025, decentralized finance protocols manage hundreds of billions of dollars in digital assets through governance mechanisms that Article 12 cannot accommodate. Sophisticated institutional investors—the venture capital firms named in *Lido*—are active participants in DAO governance. Major protocols like Uniswap and Lido have treasuries exceeding $2 billion. This is no longer an experimental corner of finance; it is a significant sector requiring legal infrastructure.

The proposed amendments offer a path forward—one that preserves Article 12's achievements while extending its reach to the decentralized structures that increasingly define digital-asset markets. The governance-token definition clarifies that these assets can qualify as CERs. The distributed-control provisions establish workable rules for multi-signature arrangements and token voting. The DAO-treasury provisions create perfection mechanisms

suited to collective ownership. Together, these amendments would bring Article 12 into alignment with contemporary DeFi practice.

American commercial law has always been an instrument of commercial development, providing the legal infrastructure that enables markets to function. The governance-token gap threatens to leave a significant portion of digital-asset markets outside that infrastructure—or worse, subject to legal rules (like general partnership liability) that impose unlimited exposure on participants. Article 12 reform can close the gap, provide legal certainty for market participants, and position American law to lead the global conversation about digital-asset property rights.

The Uniform Law Commission should act. The proposed amendments are technically sound, conceptually coherent, and practically necessary. They extend Article 12's reach without disrupting its architecture. They accommodate distributed governance without abandoning the control concept. And they provide a model that other jurisdictions—the United Kingdom, the European Union, UNIDROIT's member states—may follow as they develop their own approaches to digital-asset property.

The future of commercial law is digital. Article 12 was a crucial first step toward that future. The proposed amendments are the next step—and the time to take that step is now.