WORKING PAPER

Please do not cite or circulate without permission. Comments welcome at jwshim@jwslawyers.com.

Word Count: 15,434

THE TOKENIZED SITUS: CONTROL AS THE NEW CONFLICTS PARADIGM FOR CROSS-BORDER COLLATERALIZATION

JASON W. SHIM

* Attorney, Los Angeles, California.

ABSTRACT

This Article introduces the "tokenized situs"—a conflicts-of-law framework that replaces territorial location with cryptographic control. Traditional property law depends on lex situs: the law where property is located governs property rights. But digital assets on a blockchain have no physical location. They exist everywhere the network operates and nowhere in particular. Tokenization does not merely create new assets requiring new rules; it collapses the foundational premise of conflicts jurisprudence—that property can be located in space—and demands a paradigm shift.

The Article makes three claims. First, UCC Article 12's concept of "control" provides the doctrinal foundation: control becomes the new situs, the connecting factor determining which law governs digital assets. Second, blockchain networks create "synthetic jurisdiction"—computational sovereignty operating alongside territorial sovereignty. The key insight is the distinction between *constitutive* jurisdiction (what the blockchain records) and *regulative* jurisdiction (what legal consequences follow). Third, core conflicts concepts require reconceptualization: the tokenized situs replaces physical location; the controller's law replaces lex situs; network consensus provides legal infrastructure transcending national boundaries.

Drawing on €25 trillion in global collateral markets and the BlackRock-Barclays-JPMorgan blockchain settlement, the Article develops this framework's practical implications. Control as the new situs is a fundamental reconception of how property law operates in computational space.

TABLE OF CONTENTS

INTRODUCTION

Where is a bitcoin? The question seems simple, but it exposes a fault line running through the foundations of property law. A bitcoin is not in any particular place. It exists as an entry on a distributed ledger replicated across thousands of nodes worldwide. It is everywhere those nodes operate and nowhere in particular. Ask which nation's law governs property rights in that bitcoin, and you have asked a question that traditional conflicts doctrine cannot answer.

This is not merely a technical puzzle for specialists. The global collateral market exceeds €25 trillion.[1] Cross-border lending represents trillions more. As these markets migrate to blockchain infrastructure—a process already underway at the world's largest financial institutions—the question of which law governs digital assets becomes central to commercial practice. In October 2023, BlackRock tokenized shares in a money market fund, transferred them to Barclays as collateral for an OTC derivatives trade, and settled the entire transaction in one second.[2] That transaction raises a question traditional doctrine cannot resolve: where was that collateral located during the one second it moved between parties across the Atlantic?

This Article provides an answer. It introduces the concept of the "tokenized situs"—a new conflicts-of-law framework that replaces territorial location with cryptographic control. The central claim is that tokenization does not merely create new assets requiring doctrinal adjustment; it collapses the foundational premise of conflicts jurisprudence and demands a paradigm shift.

[1] Finadium, *Collateral Market Tops €25 Trillion, Expanding the Argument for DLT Solutions* (Aug. 28, 2024).

[2] Press Release, J.P. Morgan, BlackRock and Barclays Execute First Collateral Settlement on TCN (Oct. 11, 2023).

Traditional property law depends on lex situs: the law of the place where property is located determines property rights. Joseph Beale stated the principle categorically: "[P]roperty can have no legal situs other than that of the state where it is."[3] The First Restatement codified it: "The validity and effect of a conveyance of an interest in land is determined by the law of the state where the land is."[4] For tangible property, this rule has governed for centuries.

But the rule always rested on a premise: that property *can* be located. Remove that premise and the rule collapses. Digital assets on a blockchain remove that premise. They are not located anywhere in the sense that land is located in Kansas or a painting is located in Paris. They exist as computational states distributed across a global network. The territorial predicate of lex situs—that every thing has a place—fails.

This Article argues that "control" provides the replacement concept. The 2022 amendments to the Uniform Commercial Code created Article 12, which establishes that a person has "control" of a digital asset if the system in which the asset is recorded enables that person to enjoy substantially all the benefit from the asset, transfer the asset, and prevent others from enjoying the benefit or transferring it.[5] This definition of control does not depend on location. It depends on the *functional capacity* to exercise property rights—capacity determined by cryptographic keys, network protocols, and smart contract code.

Control as the new situs produces a framework I call the "tokenized situs." In this framework, the applicable law is not the law of the place where the asset is located (because there is no such place), but the law agreed upon by the parties or, in the absence of agreement, the law with which the controller has the closest connection. The UNIDROIT

[3] Joseph H. Beale, *A Treatise on the Conflict of Laws* § 5.1 (1935) ("[P]roperty can have no legal situs other than that of the state where it is.").

[4] Restatement (First) of Conflict of Laws § 208 (Am. L. Inst. 1934) ("The validity and effect of a conveyance of an interest in land is determined by the law of the state where the land is.").

[5] U.C.C. § 12-102(A)(4); U.C.C. § 12-105.

Principles on Digital Assets adopt precisely this approach: "The law applicable to proprietary issues in respect of a digital asset is the law chosen by the parties."[6] Party autonomy replaces territorial fixity.

This theoretical contribution has three components. Part II develops the framework systematically, showing how lex situs fails for digital assets, how control provides the replacement concept, and how blockchain networks create what I term "synthetic jurisdiction"—a form of computational sovereignty that operates alongside territorial sovereignty. Part III surveys the legal frameworks emerging across jurisdictions to address these challenges, including the emerging case law from English, Singaporean, New Zealand, and U.S. courts that is building the jurisprudential foundation for digital asset property rights. Part IV analyzes landmark transactions. Parts V and VI address smart contracts and risks. Part VII develops implications and recommendations.

A note on scope. The tokenized situs framework operates at the conflicts level—it determines *which* jurisdiction's property law applies. It does not harmonize the substantive answers that different jurisdictions give. Civil law systems operating under *numerus clausus* may classify digital assets differently than common law systems comfortable with the bundle-of-rights conception. German law's requirement that *Sachen* be corporeal objects, Korean civil law's enumerated *mulkwŏn*, Japanese law's *bukken* categories—all present doctrinal challenges that control-based conflicts rules do not resolve. The tokenized situs provides the interface through which these diverse systems interact; substantive property law remains territorial.

The stakes are substantial. Jurisdictions that fail to adapt their conflicts frameworks will find their courts unable to resolve disputes over the most dynamic asset class in global finance. Those that embrace the tokenized situs will position themselves at the center of

[6] UNIDROIT, *Principles on Digital Assets and Private Law* (2023).

cross-border commerce in digital assets. The paradigm shift is coming whether doctrine accommodates it or not.

I. THE ARCHITECTURE OF CROSS-BORDER COLLATERALIZATION

A. Traditional Systems and Their Failures

Cross-border collateralization under traditional systems is an exercise in managing the consequences of territorial sovereignty over property. When a New York bank accepts Korean real estate as collateral for a loan, it must navigate Korean property law to create a valid security interest, Korean registration systems to perfect it, and Korean courts to enforce it. Each step requires local expertise, local infrastructure, and local time.[7]

The scale of cross-border collateral markets makes these frictions economically significant. The International Capital Market Association estimates the global repo market at approximately $15 trillion outstanding. The derivatives market—much of which is collateralized—exceeds $700 trillion in notional value. Securities lending transactions add trillions more. In each market, collateral must cross borders: a London hedge fund pledges Singapore government bonds to a Tokyo bank; a Frankfurt pension fund accepts New York corporate bonds from a Sydney counterparty. Each transaction requires resolution of conflicts questions that traditional doctrine struggles to answer.

The costs are staggering. Creating a cross-border security interest in real property typically requires eight to sixteen weeks and $500,000 or more in transaction costs: local counsel, title searches, due diligence, registration fees, and coordination across time zones and legal systems.[8] Enforcement is worse. Foreclosing on Korean property from New York means Korean proceedings, Korean procedural rules, and one to three years to judgment—assuming no appeals. These frictions are not bugs in the system; they are features. They reflect the foundational principle that property rights are territorial: Korean property is subject to Korean law because it is in Korea.

[7] U.C.C. § 9-102(A)(2); U.C.C. § 9-105.

[8] Juliet M. Moringiello & William L. Reynold, *The New Emergence of the Secured Creditor*, 18 DUKE J. COMP. & INT'L L. 255, 280–95 (2008).

Financial institutions have developed workarounds: collateral transformation (converting hard-to-use assets into more fungible forms), tri-party arrangements (using intermediaries to manage collateral logistics), and legal opinions (obtaining comfort letters from local counsel on enforceability). But these workarounds add costs without eliminating uncertainty. When Lehman Brothers collapsed in 2008, the complexity of its cross-border collateral arrangements contributed to years of litigation and billions in losses.

The operational complexity is staggering. A typical cross-border collateral arrangement involves multiple legal systems for perfection, each with its own formalities: UCC-1 financing statements in the United States, registration on the Charges Register in England, *Pfandrecht* registration in Germany, hypothecation entries in Hong Kong. Title must be verified in each jurisdiction. Priority must be determined against competing claimants under each system. Enforcement procedures differ radically—summary proceedings in some jurisdictions, years of litigation in others. The net result is that high-quality collateral sits unused because the costs of mobilizing it across borders exceed the benefits.

Consider a concrete example. A Korean conglomerate wishes to use its Tokyo real estate holdings as collateral for a dollar-denominated loan from a Singapore bank. The transaction requires: Japanese law opinions on the validity of the security interest under Japanese property law; registration at the Tokyo Legal Affairs Bureau; subordination agreements with existing Japanese creditors; Korean regulatory approvals for cross-border lending; Singapore banking regulatory compliance; U.S. law opinions on the dollar documentation; and coordination among at least six law firms across four time zones. Settlement takes weeks. Fees approach seven figures. And at the end, the Singapore bank still faces uncertainty about enforcement: if the borrower defaults, how long will it take to realize on Tokyo real estate from Singapore?

This territorial principle has deep roots. Lex situs emerged from the practical reality that only the sovereign with physical control over territory could effectively vindicate property rights within it. If a dispute arose over Kansas land, Kansas law applied because Kansas courts were the only courts that could order the sheriff to enforce a judgment. The rule was not mere doctrine; it was recognition of the limits of sovereign power.[9]

The emergence of intangible property complicated this picture. Where is a debt "located"? A share of stock? An intellectual property right? Courts and scholars developed various approaches: the debtor's domicile, the place of incorporation, the place of registration. But these were always fictions—attempts to assign location to things that have no location in the physical sense. The Hague Securities Convention's "PRIMA" approach (Place of the Relevant Intermediary Approach) acknowledged this by locating intermediated securities at the intermediary's jurisdiction—a functional location rather than a physical one.[10]

B. The Tokenization Paradigm

Tokenization represents the next evolution—and it breaks the mold entirely. When real estate is tokenized, a Korean property is placed in a trust or SPV that issues tokens representing fractional interests. These tokens exist on a blockchain—a distributed ledger replicated across nodes worldwide. The token is not in Korea. It is not in any single place. It is a computational state maintained by network consensus.[11]

This is not merely a change in form. It is a change in ontology. Traditional property exists in physical space and can be located there. Tokenized property exists in computational space and cannot be located anywhere in the traditional sense. The token representing Korean

[9] Brainerd Currie, *Selected Essays on the Conflict of Laws* 77–127 (1963).

[10] Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary, July 5, 2006, 46 I.L.M. 649, art. 4(1) [hereinafter Hague Securities Convention] (adopting "PRIMA"—Place of the Relevant Intermediary Approach).

[11] R. Tamara de Silva, *Blockchain and Tokenization: The Future of Collateral Management* 22–45 (2025).

real estate interests has no more location than a number has location. It is information, and information is not somewhere.

The distinction between the token and the underlying asset is critical. The Korean property remains in Korea, subject to Korean property law. But the token—the digital representation that can serve as collateral—exists in a different realm. Transferring the token does not transfer the property; it transfers a contractual right to the economic benefits of ownership. That right exists wherever the blockchain exists, which is to say nowhere in particular and everywhere at once.

This layered structure creates both opportunities and complexities. The opportunity is collateral mobility: the token representing Korean real estate can be pledged to a Singapore lender, repledged to a London bank, and settled instantly on a global blockchain—all while the underlying property remains immovably in Korea. The complexity is legal layering: the Korean property remains subject to Korean property law, but the token's property characteristics are governed by whatever law applies to the blockchain transaction. The tokenized situs framework addresses this second layer—the property law of the token itself.

The economic implications are substantial. Boston Consulting Group estimates that tokenization could unlock $16 trillion in previously illiquid assets by 2030. McKinsey projects that tokenized assets could represent 10% of global GDP by 2027. These projections may prove optimistic, but the direction is clear: significant capital is migrating from traditional to tokenized form. The legal infrastructure for this migration—conflicts rules, property classification, enforcement mechanisms—must develop in parallel or risk becoming a bottleneck.

C. Blockchain as Commercial Infrastructure

Blockchain technology provides the infrastructure for this new form of property. A blockchain is a distributed ledger: a database replicated across multiple nodes, with transactions validated through consensus mechanisms rather than central authority. The technology provides three capabilities essential for commerce: immutability (transactions cannot be altered once recorded), transparency (authorized parties can verify the current state), and programmability (smart contracts can automate conditional transfers).[12]

For conflicts purposes, the critical feature is that blockchain operates outside territorial boundaries. A Bitcoin transaction validated by nodes in Japan, Germany, and Brazil is equally valid regardless of where the parties are located. The network does not ask permission from any sovereign. It enforces its rules through mathematics rather than courts. Lawrence Lessig's insight that "code is law" applies with particular force: the protocol rules determine what transfers are possible, and those rules operate globally.[13]

This creates what De Filippi and Wright call "lex cryptographia"—a body of rules embedded in code that governs transactions on the network.[14] But lex cryptographia is not a replacement for law; it is a new stratum of legal infrastructure that interacts with territorial law in complex ways. A smart contract can execute a transfer that violates the law of every jurisdiction whose nodes participate in validating it. The transfer is valid on the blockchain—and potentially void under every applicable legal system. This disjunction between computational validity and legal validity is the central challenge that the tokenized situs framework addresses.

D. Market Transformation in Progress

The migration from traditional to blockchain-based collateral is not hypothetical—it is underway at the world's largest financial institutions. The numbers tell the story. JPMorgan's Tokenized Collateral Network has processed over $300 billion in repo transactions since its

[12] Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).

[13] Lawrence Lessig, *Code and Other Laws of Cyberspace* 6 (1999) ("Code is law.").

[14] Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (Mar. 2015).

launch. Goldman Sachs's digital asset platform tokenized €100 million in European Investment Bank bonds in its first month of operation. BlackRock's tokenized money market fund reached $1 billion in assets within months of launch.

The efficiency gains are dramatic. Traditional repo transactions settle in T+2—two business days after trade date. Blockchain-based repo settles in seconds. Traditional collateral substitution requires manual coordination and often takes a full business day. On-chain substitution is atomic—old collateral out and new collateral in within a single block. Traditional margin calls require human intervention; smart contracts can auto-liquidate in milliseconds if collateral ratios breach thresholds.

But these efficiency gains create new legal questions. When settlement takes seconds rather than days, which moment determines the applicable law? When collateral substitution is atomic, who bears the risk during the infinitesimal interval between transactions? When liquidation is automatic, what procedural protections remain? The tokenized situs framework provides the conflicts infrastructure for answering these questions—but the questions themselves are new, products of technological capabilities that traditional doctrine never contemplated.

The regulatory response has been fragmented. The United States moved first on commercial law, with UCC Article 12 providing the statutory foundation. The European Union moved first on regulatory law, with MiCA establishing comprehensive rules for crypto-asset service providers. Asia has seen mixed approaches: Singapore emphasizing regulatory clarity, Korea emphasizing investor protection, Japan emphasizing systemic risk after Mt. Gox. No jurisdiction has comprehensively addressed both the commercial law questions (what property rights exist in digital assets?) and the regulatory law questions (how should digital asset businesses be supervised?). The tokenized situs framework focuses on the former; it assumes regulatory compliance but does not resolve regulatory classification.

This fragmentation has costs. An institution wishing to offer tokenized collateral services globally must obtain licenses in multiple jurisdictions, comply with divergent custody requirements, and navigate conflicting property law frameworks. The result is regulatory arbitrage: institutions locate in jurisdictions with favorable rules and structure transactions to minimize unfavorable law. Whether this arbitrage is salutary (regulatory competition driving efficient rules) or harmful (a race to the bottom undermining investor protection) depends on one's priors about market discipline and regulatory competence. The tokenized situs framework enables this arbitrage by providing the choice-of-law infrastructure; it does not resolve whether the arbitrage is desirable.

II. THE TOKENIZED SITUS: A THEORETICAL FRAMEWORK

A. Lex Situs and Its Discontents

The lex situs rule—that the law of the place where property is located governs property rights—rests on three justifications: practical necessity, party expectations, and sovereign interest.[15] Each justification fails when applied to digital assets on blockchain.

The practical necessity argument holds that only the territorial sovereign can effectively enforce property judgments. Kansas courts apply Kansas law to Kansas land because only Kansas can compel the sheriff to execute the judgment. This argument assumes a connection between sovereign territory and the asset—a connection that digital assets sever entirely. No sovereign "contains" a digital asset in the way Kansas contains Kansas land. Blockchain assets exist on a network that spans jurisdictions. Enforcement must proceed against the person who controls the asset, not against the asset itself. And that person may be anywhere.

The party expectations argument holds that parties dealing with property expect the law of its location to govern. When buying Kansas land, parties reasonably expect Kansas law to determine their rights. But what expectations do parties have regarding digital assets with no location? Survey data suggest that sophisticated parties expect their contractual choice of law to govern, or the law of the platform operator's jurisdiction, or no particular territorial law at all.[16] Parties transacting on a global blockchain do not expect Idaho law to govern because a validator node happens to operate in Boise.

The sovereign interest argument holds that states have legitimate interests in controlling property within their borders. This interest is powerful for land and natural resources, weaker for movables, and largely illusory for digital assets. Korea has a genuine

[15] Symeon C. Symeonides, *The American Choice-of-Law Revolution: Past, Present and Future* 85–120 (2006).

[16] Kelvin F.K. Low & Eliza Mik, *Pause the Blockchain Legal Revolution*, 69 INT'L & COMP. L.Q. 135, 150–60 (2020).

sovereign interest in Korean land. It has a much attenuated interest in a token representing contractual rights to the economic benefit of Korean land—a token that can be created, transferred, and extinguished entirely outside Korean territory. The token is not *in* Korea in any meaningful sense.

The failure of these justifications does not mean that no law governs digital assets—lawlessness is not the alternative to lex situs. It means that the connecting factor must be something other than location. Conflicts scholars have long recognized that different connecting factors serve different policy goals.[17] The question is which connecting factor best serves the policies that property law advances when the traditional factor—location—is unavailable.

Comparative perspective illuminates the options. The Hague Securities Convention addressed the analogous problem for intermediated securities by adopting PRIMA—the Place of the Relevant Intermediary Approach. The intermediary's location provides a functional substitute for asset location: securities are "located" where they are held. This approach works for the intermediated system it was designed for, but it presupposes that an intermediary exists. For non-custodial digital assets—where the user holds private keys directly—there is no intermediary whose location could provide the connecting factor.

The UNIDROIT Principles on Digital Assets chart a different course. They adopt control as the functional equivalent of possession, and they permit party autonomy for choice of law. This combination—control as the organizing concept, party choice as the primary connecting factor—provides the foundation for the tokenized situs framework that this Article develops. The innovation is not in the individual components but in their synthesis: recognizing that control provides the determinable, administrable, commercially sensible connecting factor that digital assets require.

[17] Ralf Michaels, *The New European Choice-of-Law Revolution*, 82 TUL. L. REV. 1607 (2008).

B. The Collapse of Territorial Property

Property theory has long grappled with the relationship between property rights and the things to which they attach. Hohfeld's analysis decomposed property into jural relations—rights, duties, privileges, immunities—that exist between persons, not between persons and things.[18] Penner's exclusion thesis argued that property's essence is the right to exclude, not the physical thing excluded.[19] Merrill and Smith's work on the property/contract interface showed how property rights can exist across a spectrum from in rem (binding the world) to in personam (binding particular persons).[20]

These theoretical developments anticipated the possibility of property detached from physical things. If property is fundamentally about relations between persons with respect to resources—rather than about the resources themselves—then property can exist in computational space as readily as in physical space. The question is how to structure those relations when the traditional organizing principles—possession, location, registration in territorial systems—are unavailable.

Henry Smith's influential account of property emphasizes the "law of things" and the role of physical boundaries in reducing information costs.[21] Physical boundaries communicate property rights to the world: the fence says "keep out" without requiring investigation of the owner's identity or the scope of their rights. This boundary-setting function reduces transaction costs by providing standardized signals.[22]

Blockchain provides a new mechanism for this boundary-setting function. Cryptographic keys determine who can transfer an asset. The blockchain record shows who

[18] Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 26 YALE L.J. 710 (1917).
[19] J.E. Penner, *The Idea of Property in Law* 71–105 (1997).
[20] Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 790–800 (2001).
[21] Henry E. Smith, *Property as the Law of Things*, 125 HARV. L. REV. 1691, 1695 (2012).
[22] *Id.* at 1700–10.

currently holds the keys. Smart contracts define the conditions under which transfers can occur. These are not physical boundaries, but they serve the same function: they communicate to the world who has rights with respect to the asset and what those rights are. The information costs that physical boundaries reduce in the tangible world are reduced in the computational world by cryptographic and protocol-level boundaries.

The collapse of territorial property, then, is not a collapse into lawlessness but a transition to a different organizing principle. Property rights in digital assets are not unstructured; they are structured by code rather than by geography. The task for conflicts doctrine is to recognize and accommodate this new structure.

C. Control as the New Situs

UCC Article 12 provides the doctrinal foundation for the new paradigm. The concept of "control" in Article 12 captures the functional essence of property in digital assets: the capacity to enjoy the asset's benefits, transfer it, and exclude others from it.[23] This tripartite definition maps onto the traditional incidents of property ownership but defines them functionally rather than territorially.

A person has control of a controllable electronic record if the record is issued to them, or if they have the power to avail themselves of substantially all the benefit of the record, the exclusive power to transfer control to another person, and the ability to readily identify themselves as the person having such powers.[24] Critically, this definition does not refer to location. Control is determined by the relationship between the person and the technological system, not by where either is situated geographically.

[23] U.C.C. § 12-105 (DEFINING "CONTROL" OF CONTROLLABLE ELECTRONIC RECORD); *see also id.* § 12-104 (defining controllable electronic record).

[24] *Id.* § 12-104(a).

This Article argues that control should become the connecting factor for choice of law—the tokenized situs. Where traditional lex situs asks "where is the property?", the tokenized situs asks "who controls the property and under what legal framework?" The applicable law would be determined by: (1) the parties' choice of law, where they have agreed; (2) in the absence of choice, the law of the jurisdiction with which the controller has the closest connection; (3) subsidiarily, the law of the jurisdiction whose rules the technological system implements.

This approach has several virtues. First, it is determinable: parties can identify the applicable law ex ante by examining the control structure. Second, it respects party autonomy: sophisticated parties transacting in digital assets can select the legal framework that best suits their needs, just as they do for contracts.[25] Third, it is administrable: courts can assess control by examining the cryptographic and protocol-level facts, which are publicly verifiable on transparent blockchains.

The UNIDROIT Principles on Digital Assets adopt essentially this approach. Principle 6 provides that control is the functional equivalent of possession, and Principle 9 allows party autonomy in choice of law for proprietary issues.[26] The Hague Securities Convention's PRIMA approach is a precedent: it locates intermediated securities at the place of the relevant intermediary—a functional rather than physical location.[27] But PRIMA is an inadequate model for digital assets, and the tokenized situs is superior for three reasons.

First, PRIMA presupposes intermediation.[28] The Hague Securities Convention applies to "securities held with an intermediary"—it was designed for a world where investors hold

[25] U.C.C. § 12-107 CMT. 2 (DESCRIBING THE POLICY RATIONALE FOR CONTROL-BASED CHOICE OF LAW).

[26] UNIDROIT, *Principles on Digital Assets and Private Law*, princ. 6 cmt. (2023) ("The concept of control serves as the functional equivalent of possession for digital assets.").

[27] Christoph Bernasconi, *The Hague Convention on Indirectly Held Securities* 22–45 (2006).

[28] Hague Securities Convention, *supra* note 10, art. 4(1). The PRIMA rule applies only to "securities held with an intermediary" and expressly excludes directly-held securities. *Id.* art. 1(1)(f).

securities through banks, brokers, and central depositories. Digital assets on blockchain fundamentally challenge this assumption.[29] A user holding Bitcoin in a non-custodial wallet has no intermediary. The asset exists on the blockchain, controlled by private keys that only the user possesses. Extending PRIMA to digital assets would require treating wallet providers or even software developers as "intermediaries"—a conceptual stretch that distorts both the technology and the legal framework.[30]

Second, even for custodial arrangements, PRIMA's logic fails. When a custodian "holds" digital assets for clients, it holds private keys—not the assets themselves. The blockchain remains the authoritative record of title. The custodian's internal books are derivative, not constitutive. Locating property rights at the custodian's jurisdiction mistakes the key-holder for the record-keeper.[31] Control-based analysis correctly focuses on who can execute transfers on the authoritative ledger, regardless of where ancillary service providers are located.

Third, PRIMA was designed to provide certainty for a specific institutional structure—the tiered holding systems of global securities markets.[32] Digital assets operate through different institutional structures—or no institutional structures at all. The tokenized situs framework is native to this new architecture. It does not retrofit concepts designed for intermediated systems onto disintermediated ones; it builds from the foundational reality of cryptographic control.

[29] The fundamental innovation of Bitcoin and subsequent cryptocurrencies is the elimination of intermediaries through cryptographic proof. *See* Nakamoto, *supra* note 12, at 1 ("What is needed is an electronic payment system based on cryptographic proof instead of trust.").

[30] Consider a non-custodial wallet: the user holds the private keys directly. There is no intermediary. Applying PRIMA would require identifying a "place" for the wallet software—an absurdity when the same wallet can be accessed from any jurisdiction.

[31] Even for tokens held through custodians, treating the custodian as an "intermediary" under PRIMA creates a category error: the custodian holds keys, not the asset itself. The blockchain, not the custodian's books, remains the authoritative record of title.

[32] *See* Christoph Bernasconi & Harry C. Sigman, *Myths About the Hague Convention Debunked*, INT'L FIN. L. REV., Nov. 2005, at 31, 33 (acknowledging that PRIMA was designed for a world of intermediated holding systems).

Control as the new situs is not merely a technical adjustment. It reflects a fundamental reconception of property's relationship to sovereignty. Traditional property law assumed that property existed within territorial space and was therefore subject to territorial sovereignty. Digital property exists in computational space—a space that is not nowhere but everywhere, not outside sovereignty but alongside it. The tokenized situs framework recognizes this new topology and provides the conflicts infrastructure to navigate it.

A clarification is essential. This Article's argument is normative, not merely descriptive.[33] UCC Article 12 has adopted control-based property concepts as a matter of positive law in American jurisdictions. But the claim here is not that control *is* the connecting factor because Article 12 says so. The claim is that control *should be* the connecting factor because it is functionally superior to alternatives—and Article 12's adoption provides evidence of that superiority, not its source.

The normative case for control rests on four pillars. First, *epistemic accessibility*: control can be determined by examining publicly verifiable facts. The blockchain records who holds private keys and who can sign transactions. A court in any jurisdiction can verify control by inspecting the same technical evidence. By contrast, "location" of a digital asset cannot be determined because there is nothing to locate. Control provides the connecting factor that location cannot.[34]

Second, *functional alignment*: control tracks the functional reality of property in digital assets. Property rights matter because they determine who can use an asset, transfer it, and exclude others. In digital asset systems, these capacities flow from cryptographic control.

[33] The normative case for control-based conflicts rules is independent of their positive adoption in any jurisdiction. Even if no legislature had enacted Article 12, the functional superiority of control as a connecting factor would remain.

[34] On the general theory of connecting factors in private international law, *see* Alex Mills, *The Confluence of Public and Private International Law* 230–45 (2009).

The person who holds the keys can do these things; the person without keys cannot. A conflicts rule that tracks control tracks what actually matters.

Third, *commercial efficiency*: control-based rules reduce transaction costs. Parties can structure transactions to achieve desired legal outcomes by arranging control structures. They can select their preferred legal framework through choice-of-law agreements, with control providing the fallback rule. The BlackRock-Barclays transaction demonstrates this efficiency: one-second settlement was possible because the legal framework aligned with the technical reality of instantaneous control transfer.

Fourth, *theoretical coherence*: control-based rules fit within established property theory. The Hohfeldian analysis of property as relations between persons, the exclusion thesis's focus on the right to exclude, and Smith's information-cost theory all support control as the organizing concept. Control is not a novel invention; it is the recognition that property's traditional functions—use, transfer, exclusion—can be performed through cryptographic means as effectively as through physical possession.

This normative case is independent of any legislature's adoption. If no jurisdiction had enacted Article 12, the functional superiority of control would remain. Article 12's significance is that it demonstrates workability: a major commercial law jurisdiction has translated these concepts into statutory form, providing a template for international adoption. The UNIDROIT Principles and emerging Hague Conference work confirm that this is not merely American exceptionalism but reflects a developing international consensus.

The Three-Factor Control Test

For courts confronting disputes over digital assets, the tokenized situs framework requires a method for determining control. This Article proposes a three-factor test, drawing on the functional analysis of property developed in the possession literature.[35]

First, *technical control*: who holds the private keys that can authorize transactions on the blockchain? Technical control is verifiable through blockchain analysis—forensic tools can trace transaction histories and identify which addresses control which assets at any given time.[36] For non-custodial holdings, technical control is typically determinative: the person with the keys controls the asset. For custodial arrangements, the custodian holds technical control, but this raises the second factor.

Second, *legal control*: who has the legal right to direct the asset's disposition? Legal control may diverge from technical control where contractual arrangements, trusts, or agency relationships create claims superior to those of the key-holder.[37] The *Celsius* bankruptcy illustrates this divergence: the exchange held technical control, but legal control depended on the terms of service—whether customers had transferred title or merely created a bailment.

Third, *effective control*: can the controller actually exercise control without interference? This factor becomes acute when private keys are shared, subject to multi-signature requirements, or held in contested arrangements.[38] A party with legal rights but no

[35] This tripartite framework draws on the functional analysis of property developed in the possession literature. *See generally* Carol M. Rose, *Possession as the Origin of Property*, 52 U. CHI. L. REV. 73 (1985).

[36] Technical control is verifiable through blockchain analysis: forensic tools can trace transaction histories and identify which addresses control which assets at any given time. *See* Chainalysis, *The 2024 Crypto Crime Report* 12–18 (2024) (describing blockchain forensics capabilities).

[37] Legal control may diverge from technical control where contractual arrangements, trusts, or agency relationships create claims superior to those of the key-holder. *Cf.* Restatement (Third) of Agency § 8.12 (Am. L. Inst. 2006) (agent's duty to account for property received in course of agency).

[38] Effective control asks whether the technical controller can actually exercise control without interference—a question that becomes acute when private keys are shared, subject to multi-signature requirements, or held in contested custodial arrangements.

effective ability to exercise them—because a custodian refuses access or keys have been lost—lacks control in the sense that matters for conflicts purposes.

The three factors interact hierarchically. Technical control establishes a presumption. Legal control can rebut that presumption where contractual or fiduciary relationships allocate rights differently from key-holding. Effective control serves as a reality check: legal rights without practical ability to exercise them do not establish the connection that conflicts doctrine requires.[39]

This framework gives courts concrete tools for digital asset disputes. When asked "which law governs property rights in this Bitcoin?", the court should ask: (1) Who holds the keys? (2) Do legal arrangements allocate control differently? (3) Can the legal controller actually exercise control? The answers determine who "controls" the asset for choice-of-law purposes—and thus which jurisdiction's property law applies.[40]

D. Synthetic Jurisdiction and Computational Sovereignty

The tokenized situs framework implies a further theoretical claim: blockchain networks create a form of "synthetic jurisdiction" that operates alongside territorial jurisdiction. This is not the discredited cyberspace-exceptionalism of early internet scholarship—the claim that the internet is a separate place outside sovereign control.[41] It is a more modest but more defensible claim: that blockchain consensus mechanisms create a system of rules, adjudication, and enforcement that functions as a quasi-legal order within the network.

[39] *Compare* THE ANALOGOUS THREE-PART TEST FOR "POSSESSION" UNDER ARTICLE 9 OF THE UCC: (1) ACTUAL PHYSICAL CONTROL, (2) AUTHORITY TO DISPOSE, AND (3) INTENTION TO POSSESS. U.C.C. § 9-313 CMT. 3.

[40] The problem of competing claims to control parallels traditional property disputes over possession. *See* Richard A. Epstein, *Possession as the Root of Title*, 13 GA. L. REV. 1221 (1979).

[41] Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

Consider how blockchain networks operate. Protocol rules determine what transactions are valid. Consensus mechanisms determine which valid transactions become part of the authoritative record. Smart contracts execute predetermined consequences when conditions are met. Disputes over protocol interpretation are resolved through governance mechanisms—sometimes on-chain voting, sometimes off-chain social consensus, sometimes hard forks that split the network.[42] These are the functional equivalents of legislation, adjudication, and enforcement—the basic machinery of legal order.

Synthetic jurisdiction is "synthetic" because it is constructed rather than inherited, computational rather than territorial, voluntary rather than compulsory.[43] Participants opt into network rules by choosing to transact on the network. The network's "jurisdiction" extends to all transactions on that network, regardless of where participants are physically located. Exit is possible—participants can leave the network—but while participating, they are subject to its rules.[44]

This synthetic jurisdiction does not displace territorial jurisdiction; it layers over it. A transaction on Ethereum is simultaneously subject to Ethereum protocol rules (synthetic jurisdiction) and to the laws of every territorial jurisdiction that claims authority over it (territorial jurisdiction). When these layers conflict—when the protocol permits a transaction that territorial law prohibits—the question becomes which layer prevails. Within the network,

[42] Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies* 27–65 (2016).

[43] "Voluntary" here refers to the initial decision to acquire assets on the network and transact through its protocols—not necessarily to every subsequent transaction affecting those assets. A hack victim whose assets are transferred without authorization did not consent to that specific transaction, but the victim (or the victim's predecessor in interest) did choose to hold assets on a network whose protocol rules permit such transfers. The remedy lies in territorial jurisdiction—criminal prosecution of the hacker, civil claims for conversion—not in synthetic jurisdiction, which simply records what the cryptographic keys authorized. This is the division of labor between constitutive and regulative jurisdiction: the network records the transfer; the court addresses its wrongfulness.

[44] This term builds on De Filippi and Wright's concept of "lex cryptographia." *See* De Filippi & Wright, *supra* note 14, at 193–95.

protocol rules are self-executing; territorial law must be enforced externally, against persons rather than against the network itself.

The limits of synthetic jurisdiction require explicit definition. Traditional jurisdictional analysis distinguishes between in rem jurisdiction—authority over things—and in personam jurisdiction—authority over persons.[45] Synthetic jurisdiction operates primarily in the in rem register: it determines the state of the ledger, which records who controls which assets. When the network validates a transfer, it exercises a form of in rem authority—it changes the record of title that binds all network participants.[46]

But synthetic jurisdiction cannot and does not attempt to exercise in personam authority in the traditional sense. It cannot compel testimony, impose fines, or order imprisonment. When a smart contract liquidates collateral, it does not adjudicate the debtor's rights; it executes a predetermined protocol. The debtor remains free to seek relief in territorial courts—to argue that the liquidation violated applicable law, that the smart contract was defective, or that the counterparty acted in bad faith. Territorial courts retain exclusive authority over these in personam claims.

This division of labor is not anomalous. It mirrors other contexts where private ordering governs certain matters while public courts retain residual authority. Arbitration clauses commit disputes to private resolution, but courts enforce awards and police procedural fairness. Industry self-regulation governs conduct within domains, but regulatory agencies and courts maintain oversight.[47] Synthetic jurisdiction governs the state of the

[45] The distinction between in rem and in personam jurisdiction traces to Pennoyer v. Neff, 95 U.S. 714, 722–23 (1878). For modern treatment, *see* Shaffer v. Heitner, 433 U.S. 186, 199–206 (1977).

[46] *See* Restatement (Second) of Conflict of Laws § 56 cmt. b (Am. L. Inst. 1971) (distinguishing adjudicatory jurisdiction over things from jurisdiction over persons).

[47] Ooki DAO, No. 3:22-cv-05416, slip op. at 12–15 (N.D. Cal. Dec. 20, 2022) (holding that service on a DAO through a forum post satisfied due process where the protocol's governance structure created constructive notice).

ledger; territorial jurisdiction governs the rights and obligations of persons who interact with it.

A theoretical objection demands response: if the state holds a monopoly on legitimate violence, how can synthetic jurisdiction be "jurisdiction" at all? Max Weber defined the state as the entity that "successfully claims the monopoly of the legitimate use of physical force within a given territory."[48] Thomas Hobbes argued that without sovereign enforcement, property rights dissolve into the "war of all against all."[49] If a territorial court orders reversal of a blockchain transaction—and the blockchain cannot comply—has synthetic jurisdiction not failed?

The objection confuses two distinct functions. Synthetic jurisdiction is *constitutive*: it determines what the ledger says. Territorial jurisdiction is *regulative*: it determines what consequences follow from what the ledger says.[50] When a court orders a transaction reversed, it does not change the blockchain—it creates obligations for persons. The defendant must transfer equivalent assets, pay damages, or face contempt. The ledger remains as the network wrote it; the court operates on the person who interacted with it.

This is not a failure of synthetic jurisdiction; it is the division of labor working as designed. The blockchain provides the authoritative record of what happened—who transferred what to whom, when, under what conditions. The court provides the normative assessment of whether that transfer was lawful and what remedies follow if it was not. Neither can do the other's job. The court cannot rewrite the blockchain; the blockchain cannot imprison a fraudster. But together they provide the infrastructure for property rights in

[48] Max Weber, *Politics as a Vocation* (1919), *reprinted in* From Max Weber: Essays in Sociology 77, 78 (H.H. Gerth & C. Wright Mills eds., 1946) ("[A] state is a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory.").

[49] For the classic statement, *see* Thomas Hobbes, *Leviathan* ch. 13 (1651) (describing the state of nature as "war of all against all" absent sovereign enforcement).

[50] On the distinction between constitutive and regulative rules, *see* John R. Searle, *The Construction of Social Reality* 27–29 (1995).

computational space: the network determines the state of the world, and the court determines what to do about it.[51]

The comparison to arbitration is apt but incomplete.[52] Arbitration awards bind parties but require state enforcement. Blockchain transactions are self-enforcing within the network but cannot reach beyond it. The key insight is that enforcement is always against persons, never against things. A court enforcing an arbitral award seizes the defendant's bank account; it does not rewrite the arbitrator's reasoning. A court reversing a blockchain transfer seizes the defendant's other assets or holds them in contempt; it does not and cannot rewrite the ledger. The state's monopoly on violence operates at the level of persons; synthetic jurisdiction operates at the level of records.

Property scholars have long recognized that property norms can emerge and be enforced through mechanisms other than state violence.[53] The medieval lex mercatoria provided transnational commercial law enforced through reputation and exclusion from trade networks.[54] ICANN governs the domain name system through contractual arrangements cascading from registry to registrar to registrant.[55] Blockchain networks are the latest entry in this tradition of private ordering—distinguished by their technical sophistication and global reach, but not by their conceptual novelty. Synthetic jurisdiction is not an attempt to escape

[51] *See* Florian Möslein & Sebastian Omlor, *The Enforcement Problem in Crypto-Asset Transactions* (draft 2024) (analyzing the gap between on-chain and off-chain enforcement).

[52] *Compare* the enforcement mechanism in international arbitration: arbitral awards bind parties through contract, but enforcement requires state action under the New York Convention. Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 38.

[53] *See* Robert C. Ellickson, *Order Without Law: How Neighbors Settle Disputes* 123–36 (1991) (demonstrating that property norms can emerge and be enforced without state involvement).

[54] *See generally* Leon E. Trakman, *The Law Merchant: The Evolution of Commercial Law* (1983) (tracing the development of lex mercatoria as transnational commercial law).

[55] On ICANN as private governance, *see* A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17 (2000).

the Westphalian order; it is private ordering with unprecedented coordination capacity, operating within and alongside territorial sovereignty.[56]

The concept of synthetic jurisdiction illuminates why control works as a connecting factor. Control is what links participants to the synthetic jurisdiction of the network. The person who holds the private keys—who can sign transactions that the network will validate—is the person subject to network rules with respect to that asset. Control determines both what is possible (the protocol's permissions) and what is permissible (the law that governs the controller's actions). The tokenized situs uses control to connect synthetic jurisdiction to territorial jurisdiction, providing the interface between code-based rules and court-enforced law.

Gillian Hadfield's work on "rules for a flat world" anticipated this development. She argues that global commerce requires legal infrastructure that transcends national boundaries—and that such infrastructure can emerge from private ordering as well as public law.[57] Blockchain networks are precisely such private ordering at global scale. They provide the infrastructure for property rights in digital assets: the record of title (the blockchain), the mechanism of transfer (cryptographic signing), and the enforcement of conditions (smart contracts). The tokenized situs framework provides the conflicts rules that connect this private infrastructure to public legal systems.

E. The Civil Law Challenge: Numerus Clausus and Control

The tokenized situs framework presents distinctive challenges for civil law jurisdictions. Common law systems, comfortable with the "bundle of rights" conception of

[56] The argument here parallels Lon Fuller's analysis of private ordering. *See* Lon L. Fuller, *The Morality of Law* 207–13 (rev. ed. 1969).

[57] Gillian K. Hadfield, *Rules for a Flat World: Why Humans Invented Law and How to Reinvent It for a Complex Global Economy* 250–80 (2017).

property, can accommodate control-based property rights with relative ease.[58] The common law tradition treats property as a collection of rights—to use, exclude, transfer, encumber—that can be divided, recombined, and held by different parties. Control, in this framework, is simply another way of describing who holds which sticks in the bundle.

Civil law systems operate from a fundamentally different premise. The concept of *numerus clausus*—the closed number of property rights—holds that property rights exist only in forms recognized by law.[59] German law conceives of ownership (*Eigentum*) as absolute dominion over a thing, not as a divisible bundle of rights.[60] Korean and Japanese civil codes follow similar structures, restricting the creation of real rights (*mulkwŏn* / *bukkenken*) to those enumerated in statute.[61]

This structural difference creates friction with control-based property concepts. When the UCC defines "control" as a functional capacity rather than a formal legal category, it assumes the common law's flexible approach to property. Civil law jurisdictions must ask: is control a new property right, and if so, does it require legislative creation? Can control be perfected against third parties without registration in traditional land or movable property registers? How does control interact with existing categories of real rights?[62]

The German Law Commission has acknowledged these difficulties, noting that traditional property categories map poorly onto digital assets.[63] The Korean FSC's STO guidelines attempt to work within existing trust law structures rather than creating new

[58] For the foundational analysis of property as a "bundle of rights," *see* Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16 (1913).

[59] Sjef van Erp, *A Numerus Quasi-Clausus of Property Rights as a Constitutive Element of a Future European Property Law?*, 7.2 ELEC. J. COMP. L. 1, 8–12 (2003).

[60] *See* Bürgerliches Gesetzbuch [BGB] [Civil Code], § 903, translation at https://www.gesetze-im-internet.de/englisch_bgb/ (Ger.) (defining ownership as absolute dominion subject only to statutory limits).

[61] Minpŏp [Civil Act], Act No. 471, Feb. 22, 1958, art. 185 (S. Kor.) ("No real right can be created other than by this Act or other Acts."). *See also* Minpō [Civil Code], Law No. 89 of 1896, art. 175 (Japan) (similar provision).

[62] Eva-Maria Kieninger, *Security Rights in Movable Property in European Private Law* 34–52 (2004).

[63] The German Law Commission has acknowledged the difficulty of applying traditional property categories to digital assets. *See* Bundesministerium der Justiz, *Eckpunkte für die regulatorische Behandlung von Kryptowerten* 12–15 (2019).

property categories—a pragmatic accommodation that preserves *numerus clausus* while enabling token-based transactions.[64] France has enacted specific legislation to enable blockchain-based securities, creating a sui generis regime that sits alongside traditional property categories.[65]

The tokenized situs framework does not resolve these doctrinal tensions—it operates at the conflicts level, not the substantive property level. But it provides a framework within which diverse property systems can interact. The applicable law—determined by control and party choice—will specify whether control constitutes a property right, how that right is perfected, and what protections it receives against third parties. Civil law jurisdictions can maintain their [66]*numerus clausus* while recognizing that other jurisdictions may structure property rights differently. The tokenized situs provides the interface; substantive property law remains territorial.

The insolvency context crystallizes these challenges. Under German law, creditors with *dingliche Rechte* (real rights) may invoke *Aussonderung*—separation of their assets from the insolvency estate under Insolvenzordnung § 47.[67] But if crypto-assets cannot

[64] Financial Services Commission (S. Kor.), Guidelines for Security Token Offerings (Feb. 2023).

[65] France's approach illustrates the civil law adaptation. *See* Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers, JORF n°0287 (Dec. 9, 2017) (creating special regime for blockchain-based securities).

[66] A critical doctrinal point warrants elaboration: the tokenized situs framework assumes that the chosen law has a mechanism to recognize the transfer. In civil law systems, the distinction between *titulus* (the underlying contract creating the obligation to transfer) and *modus* (the mode of transfer that actually passes title) presents a threshold question: does a blockchain update constitute the *modus* sufficient to transfer title? German law (BGB §§ 929–931) generally requires physical delivery for movables or registration for immovables. If a token is classified as neither, and the Civil Code lacks a mechanism recognizing blockchain entry as a valid mode of transfer, title may fail to pass entirely under local law—even if the tokenized situs points to that jurisdiction. France addressed this gap through its 2017 Ordinance No. 2017-1674, which created a *sui generis* regime whereby a “dispositif d’enregistrement électronique partagé” (shared electronic recording device, i.e., blockchain) constitutes the legal register for certain unlisted securities, satisfying the *modus* requirement legislatively. *See* Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l’utilisation d’un dispositif d’enregistrement électronique partagé pour la représentation et la transmission de titres financiers; Code monétaire et financier, art. L. 211-3. This legislative approach validates the tokenized situs framework’s path for civil law reform, discussed *infra* Part III.B.

[67] Insolvenzordnung [InsO] [Insolvency Statute], Oct. 5, 1994, BGBl. I at 2866, § 47 (Ger.) (providing for separation of assets not belonging to insolvency estate); *see also id.* § 51 (providing for preferential satisfaction of secured creditors).

constitute *Sachen* under BGB § 90, customers whose crypto was held by an insolvent custodian may be relegated to unsecured claims.[68] The Mt. Gox proceedings in Japan reached precisely this result: Bitcoin depositors were treated as unsecured creditors, not proprietary claimants.[69]

Korea's Virtual Asset User Protection Act of 2024 responds to this problem through regulatory rather than property-law mechanisms.[70] The Act requires segregation of customer assets and establishes deposit insurance—protections that operate through trust structures rather than by recognizing proprietary rights in the assets themselves.[71] Japanese law similarly defines crypto-assets functionally under the Payment Services Act—as "property values" capable of electronic transfer—without resolving their classification under the Minpō's property categories.[72]

The contrast with common law jurisdictions is instructive. In *Ruscoe v. Cryptopia*, the New Zealand court held that crypto-assets constituted property held on trust for customers—giving them priority over unsecured creditors.[73] The U.S. bankruptcy courts' analysis in *Celsius* turned on contractual interpretation: whether the terms of service transferred title or created a bailment. Common law's flexible property categories allowed courts to reach results driven by functional analysis rather than formal categorization.

[68] The *Aussonderung* (separation) right under InsO § 47 requires that the claimant demonstrate a *dingliches Recht* (real right) or ownership. If crypto-assets cannot constitute *Sachen* under BGB § 90, claimants are relegated to unsecured claims. *See* Bürgerliches Gesetzbuch [BGB] [Civil Code], § 90, translation at https://www.gesetze-im-internet.de/englisch_bgb/ (Ger.).

[69] Japanese courts have not definitively resolved whether crypto-assets constitute *bukken* (real rights) under the Minpō. The Mt. Gox bankruptcy proceedings treated Bitcoin as property of the estate, not customer property. *See* Tokyo District Court, Aug. 5, 2015 (Mt. Gox ruling).

[70] Virtual Asset User Protection Act, Act No. 19597, July 18, 2023 (S. Kor.) (effective July 19, 2024) (requiring segregation of customer assets and establishing deposit insurance for virtual assets).

[71] The Korean Act creates regulatory protections but does not resolve the underlying property-law classification. Customer "separation" operates through trust structures rather than proprietary rights in the assets themselves. *See* Korean Financial Services Commission, *Virtual Asset User Protection Act Implementation Guidelines* 23–28 (2024).

[72] Shikin Kessai ni Kansuru Hōritsu [Payment Services Act], Law No. 59 of 2009, art. 2(5) (Japan) (defining "crypto-assets" as property values that can be used for payment and transferred electronically).

[73] Ruscoe v Cryptopia Ltd (in liq) [2020] NZHC 728 at [120] (holding that cryptocurrencies held by exchange were property held on trust for customers, not assets of the exchange).

For the tokenized situs framework, these differences matter at the choice-of-law stage. A German court applying German property law may deny separation rights that a New Zealand court would recognize. The tokenized situs provides the method for determining which law applies; it does not harmonize the substantive answers. Sophisticated parties will select applicable law with these insolvency consequences in mind—another dimension of the regulatory arbitrage that control-based choice of law enables.

III. LEGAL FOUNDATIONS ACROSS JURISDICTIONS

A. United States: UCC Article 12

The 2022 amendments to the Uniform Commercial Code created Article 12, which provides the most developed statutory framework for the tokenized situs concept. Article 12 introduces "Controllable Electronic Records" (CERs) and establishes control as the mechanism for acquiring property rights in them.

The definition of "controllable electronic record" is deliberately technology-neutral. A CER is an electronic record that is susceptible to control: it must be capable of being subject to control, meaning that the system in which it is recorded enables a person to enjoy substantially all the benefit from the record, exercise exclusive power to transfer control, and readily identify themselves as having such powers. This definition captures blockchain-based tokens but is not limited to them—it can apply to any technological system that enables cryptographic or equivalent control.

The control-based perfection rule is central. A security interest in a CER may be perfected by the secured party's obtaining control.[74] This replaces the traditional filing-based perfection for tangibles and establishes control as the gold standard for digital assets. Control-based perfection has priority over filing-based perfection—creating powerful incentives for lenders to structure transactions around control.

The priority regime reflects the informational properties of control. Traditional UCC priority depends on filing: the first to file generally wins, because filing provides constructive notice to subsequent creditors. Control provides a different kind of notice—actual, verifiable control of the asset. When a secured party has control, subsequent creditors can verify that the asset is already encumbered by examining the control structure. This is the information-

[74] U.C.C. § 12-104(A); § 12-105(A).

cost rationale for the control-based priority rule: control serves the notice function that filing serves for traditional collateral.

The take-free rule completes the framework. A qualifying purchaser who obtains control of a CER takes free of any property claim to the record.[75] This mirrors the holder-in-due-course protection for negotiable instruments and the purchaser-for-value protection for securities. It creates the transferability essential for liquid markets: purchasers can acquire digital assets with confidence that their title will not be defeated by prior claims they could not have discovered.

Article 12's choice-of-law provisions implement elements of the tokenized situs approach. Section 12-107 provides that the local law of the jurisdiction agreed upon by the parties governs questions relating to CERs. In the absence of agreement, the law of the jurisdiction in which the controller is located governs. This is control-based choice of law—precisely the framework this Article advocates.

As of mid-2024, approximately forty states have enacted versions of Article 12, with more adoptions expected. This rapid adoption reflects both the commercial need for clear rules governing digital assets and the success of the Uniform Law Commission's drafting process. For cross-border transactions, the pattern of adoption matters: parties will structure transactions to ensure that Article 12 law governs, selecting applicable law accordingly. The tokenized situs framework operates within this pattern—determining which jurisdiction's version of Article 12 (or equivalent law) applies.

B. European Union: MiCA and the DLT Pilot Regime

The European Union has approached digital assets through regulatory rather than commercial law frameworks. The Markets in Crypto-Assets Regulation (MiCA) establishes

[75] *Id.* § 12-105(a).

comprehensive rules for crypto-asset service providers, including custody, trading, and issuance.[76] The DLT Pilot Regime creates a sandbox for trading and settlement of tokenized securities.[77]

The EU approach differs fundamentally from the UCC model—and this difference matters for the tokenized situs framework. Article 12 operates at the level of property law: it creates a new category of personal property (controllable electronic records) and establishes rules for acquiring, transferring, and perfecting interests in that property. MiCA operates at the level of regulatory law: it governs the conduct of service providers without creating new property categories or modifying existing property concepts.[78]

This distinction creates a gap. MiCA tells a crypto-asset service provider how to obtain a license, what disclosures to make, and what capital to hold. It does not tell a German court whether a token is *Sache* (thing), *Forderung* (claim), or something else entirely—and that classification determines which property rules apply. The regulatory superstructure leaves the property law foundation unaddressed.

The German challenge is particularly acute. German property law (*Sachenrecht*) applies only to "things" (*Sachen*), defined in BGB § 90 as "corporeal objects" (*körperliche Gegenstände*).[79] Digital assets, lacking corporeality, cannot be "things" and therefore cannot be subject to property rights in the technical sense. This creates what German scholars call

[76] Regulation (EU) 2023/1114, of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, 2023 O.J. (L 150) 40 [hereinafter MiCA].

[77] Regulation (EU) 2022/858 (DLT Pilot Regime), 2022 O.J. (L 151) 1.

[78] For analysis of the regulatory versus property law distinction, *see* Philipp Paech, *The Governance of Blockchain Financial Networks*, 80 MOD. L. REV. 1073, 1095–1100 (2017).

[79] Bürgerliches Gesetzbuch [BGB] [Civil Code], § 90, translation at https://www.gesetze-im-internet.de/englisch_bgb/ (Ger.), defines "things" (*Sachen*) as "corporeal objects" (*körperliche Gegenstände*). Digital assets, lacking corporeality, cannot be "things" under German law and therefore cannot be subject to property rights (*Sachenrecht*). This creates the *Zuordnungsproblem*—the allocation problem.

the *Zuordnungsproblem*—the allocation problem: how to assign rights in assets that fit no established category.[80]

Germany has taken partial steps. The Electronic Securities Act (*Gesetz über elektronische Wertpapiere*, eWpG) of 2021 permits bearer bonds and certain fund units to exist in dematerialized form on electronic registers, including blockchain.[81] But this statute applies only to specific securities categories—it does not extend to crypto-assets generally, and it does not modify the fundamental property law categories that constrain German courts.[82]

How, then, might a German court accept "control" as a property concept? Three paths are possible. First, *legislative reform*: the Bundestag could amend the BGB to recognize a new category of property in digital assets, with control as the organizing concept. This is the cleanest path but requires political will and legislative bandwidth.

Second, *judicial development*: German courts have historically developed new categories to accommodate technological change. The concept of *sonstiges Recht* ("other right") under BGB § 823(1) emerged through case law to provide tort protection for interests that fit no established category.[83] Courts might similarly recognize control of digital assets as a protected interest, even without express legislative authorization. This path is slower and less certain but does not require legislative action.

Third, *obligational characterization*: German law might characterize digital asset rights as purely obligational (*schuldrechtlich*) rather than proprietary (*sachenrechtlich*). The

[80] *See* Matthias Lehmann, *Who Owns Bitcoin? Private Law Facing the Blockchain*, 21 MINN. J.L. SCI. & TECH. 193, 210–18 (2020) (analyzing German property law's application to crypto-assets).

[81] *See* Gesetz über elektronische Wertpapiere [eWpG] [Electronic Securities Act], June 3, 2021, BGBl I at 1423 (Ger.) (creating framework for electronic securities without physical certificates).

[82] The eWpG applies only to bearer bonds and certain fund units; it does not extend to crypto-assets generally. *See* Sebastian Omlor, *Digitales Eigentum an Kryptowerten* [Digital Ownership of Crypto-Values], JURISTENZEITUNG 2021, 1025.

[83] This path is analogous to how German courts developed *sonstiges Recht* ("other right") under BGB § 823(1) to provide tort protection for interests not fitting traditional property categories. *See* BGH, Feb. 26, 1954, 13 BGHZ 334 (extending protection to business operations).

token holder would have contractual claims against the issuer or network participants, not property rights in the token itself. This path avoids the Sachenrecht constraints but sacrifices the advantages of proprietary characterization, including priority in insolvency and availability of proprietary remedies.

The European Law Institute has recommended harmonized approaches to blockchain property rights across EU member states.[84] Until such harmonization occurs, the tokenized situs framework operates at the conflicts level—determining which jurisdiction's property law applies—while leaving the substantive property law question to each member state. A German court applying German law to a token transaction would apply German property categories; a French court applying French law would apply the special blockchain regime created by the 2017 Ordonnance. The tokenized situs provides the interface; substantive property law remains territorial and diverse.

C. Asia-Pacific Developments

Singapore has positioned itself as a leader in digital asset regulation. The Payment Services Act and Securities and Futures Act provide licensing frameworks for digital asset businesses.[85] The Personal Property Securities Act enables security interests in digital assets through a registration system.[86] Singapore courts have shown receptivity to recognizing property rights in digital assets—most notably in *Quoine v. B2C2*, where the Court of Appeal held that algorithmically executed trades were binding contracts.[87]

[84] *See* European Law Institute, *Principles on Blockchain Technology, Smart Contracts, and Consumer Protection* 45–52 (2022) (recommending harmonized approach to blockchain property rights across EU member states).

[85] Payment Services Act 2019 (Sing.); Securities and Futures Act 2001 (Sing.).

[86] Personal Property Securities Act 2009 (Sing.).

[87] B2C2 Ltd. v. Quoine Pte Ltd. [2019] SGHC(I) 03 (Sing. Int'l Com. Ct.), *aff'd*, [2020] SGCA(I) 02 (Sing. Ct. App.).

South Korea presents a particularly dynamic case study. The Financial Services Commission issued comprehensive guidelines for security token offerings in 2023.[88] Market projections estimate the Korean STO market at 34 trillion won ($23 billion) by 2024, with annual growth exceeding 49%.[89] Platforms like Lucentblock have tokenized Korean real estate, demonstrating the commercial application of these frameworks.[90]

The Korean regulatory approach illustrates the tension between investor protection and property law classification. The Virtual Asset User Protection Act of 2024 requires segregation of customer assets and creates deposit insurance protections. But these protections operate through regulatory mandates rather than property recognition—customer "separation" works through trust structures, not through recognition of proprietary rights in the assets themselves. The underlying property classification under the Korean Civil Code's *numerus clausus* remains unresolved.

Japan's approach to digital assets evolved through crisis. The Mt. Gox collapse of 2014—at the time the world's largest Bitcoin exchange—exposed gaps in the regulatory and property law framework. Japanese courts treated Bitcoin depositors as unsecured creditors rather than proprietary claimants, leaving customers to compete with other creditors for a share of remaining assets. The result was catastrophic losses for users who believed they "owned" their Bitcoin.

Japan responded with regulatory reform. The Payment Services Act now defines crypto-assets as "property values" (*zaisan-teki kachi*) that can be used for payment and transferred electronically. This functional definition creates a regulatory category without resolving the property law question: are crypto-assets *bukken* (real rights) under the Minpō?

[88] Financial Services Commission (S. Kor.), Guidelines for Security Token Offerings (Feb. 2023).
[89] Samil PwC Business Research, *Korean STO Market Analysis 2024* (2024) (projecting Korean STO market at 34 trillion won in 2024).
[90] Lucentblock.io (documenting first Korean security token issuance).

Japanese scholars remain divided, and courts have not definitively resolved the question. The tokenized situs framework accommodates this uncertainty: Japanese law applies to property questions when Japanese parties control the relevant assets, but what that law provides remains a matter for Japanese courts to determine.

Hong Kong and Australia have taken different approaches. Hong Kong has positioned itself as a crypto-friendly jurisdiction through the Virtual Asset Service Provider licensing regime, attracting major exchanges. Australia has developed a token mapping framework that classifies tokens by function rather than form. Both approaches reflect the global trend toward functional regulation—governing digital assets based on what they do rather than what they are. But neither jurisdiction has definitively resolved the underlying property law questions that the tokenized situs framework addresses.

D. International Harmonization

Two international instruments are shaping the global framework. The UNIDROIT Principles on Digital Assets provide soft-law guidance on control, transfer, and innocent acquisition. The Principles adopt control as the functional equivalent of possession—the core insight of the tokenized situs framework.[91]

The UNIDROIT Principles merit detailed examination. Principle 6 establishes that "the law applicable to proprietary issues in respect of a digital asset is the law chosen by the parties." This is party autonomy as the primary connecting factor—precisely what the tokenized situs framework recommends. When parties have not chosen a law, Principle 7 provides fallback rules based on the "law of the State with which the digital asset is most closely connected," with control serving as the primary indicator of connection. The

[91] UNIDROIT, Principles on Digital Assets and Private Law, princ. 4 (2023).

Principles thus operationalize control as the default connecting factor when party choice is absent.

The Principles also address innocent acquisition—the bona fide purchaser problem translated to digital assets. Principle 8 provides that an innocent acquirer who obtains control of a digital asset in good faith, without knowledge of competing claims, takes free of prior interests. This rule parallels the shelter provision in UCC Article 12 and serves the same commercial function: protecting the integrity of transactions by enabling parties to rely on control as evidence of title. The convergence between the UNIDROIT Principles and UCC Article 12 on this point is striking—and supports the claim that control-based property concepts reflect functional necessity rather than jurisdictional idiosyncrasy.

The Hague Conference on Private International Law has undertaken complementary work on choice of law for digital assets, building on the Securities Convention's PRIMA approach. The emerging consensus favors party autonomy as the primary connecting factor, with control-based rules as the fallback.[92] The Hague work differs from UNIDROIT in focus: while UNIDROIT addresses substantive principles (when does control transfer? what rights does an innocent acquirer take?), the Hague work addresses conflicts principles (which jurisdiction's law answers these substantive questions?). Together, they provide the complete framework: Hague-style choice-of-law rules determine the applicable law, and UNIDROIT-style substantive principles—as adopted in domestic law—determine outcomes under that law.

This international convergence validates the tokenized situs framework. When UNIDROIT, the Hague Conference, and the Uniform Law Commission independently arrive at control as the organizing concept, the conclusion is not coincidence but recognition of

[92] Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary, July 5, 2006, 46 I.L.M. 649, art. 4 [hereinafter Hague Securities Convention].

functional reality. Digital assets require control-based property rules because control captures the functional essence of property in computational systems. This is the tokenized situs in international form—a framework emerging organically from the needs of global commerce rather than imposed from any single jurisdiction.

E. Emerging Jurisprudence: Courts Confront Digital Assets

While statutory frameworks develop, courts have begun confronting digital assets through common law reasoning. These decisions—from England, New Zealand, Singapore, and U.S. bankruptcy courts—provide the doctrinal grounding that the tokenized situs framework organizes and extends.

The English courts have led in recognizing crypto-assets as property. In *AA v. Persons Unknown*, the Commercial Court held that Bitcoin meets Lord Wilberforce's classic four-part definition of property: it is definable, identifiable by third parties, capable of assumption by third parties, and has some degree of permanence.[93] The court granted a proprietary injunction, treating Bitcoin as property capable of being traced and recovered.[94] Subsequent decisions in *Ion Science* and *Fetch.AI* extended this analysis, establishing that crypto-assets generally—not merely Bitcoin—constitute property under English law.[95]

The UK Law Commission codified and extended this jurisprudence, concluding that crypto-assets constitute a "third category" of personal property—distinct from both things in possession and things in action.[96] This third-category analysis aligns with the tokenized situs

[93] AA v Persons Unknown [2019] EWHC (Comm) 3556 [55] (Eng.) (recognizing Bitcoin as property capable of being subject to a proprietary injunction).

[94] *Id.* at [59] ("[C]rypto assets such as Bitcoin are property. They meet the four criteria set out in Lord Wilberforce's classic definition of property in *National Provincial Bank v. Ainsworth*.").

[95] Ion Science Ltd. v. Persons Unknown [2020] EWHC 1234 (Comm) (granting worldwide freezing order over Bitcoin); Fetch.AI Ltd. v. Persons Unknown [2021] EWHC 2254 (Comm) (extending proprietary analysis to other crypto-assets).

[96] The UK Law Commission concluded that crypto-assets constitute a "third category" of personal property, distinct from both things in possession and things in action. *See* Law Comm'n, *Digital Assets: Final Report*, Law Com. No. 412, ¶¶ 4.1–4.45 (2023).

framework: control-based assets require property concepts that transcend the traditional possession/chose-in-action dichotomy.

The New Zealand High Court reached similar conclusions in *Ruscoe v. Cryptopia*, the first appellate-level decision addressing crypto-asset property rights in the insolvency context. The court held that cryptocurrencies held by an exchange constituted property held on trust for customers—not assets of the exchange's estate. Critically, the court grounded its analysis in the functional characteristics of crypto-assets: they are identifiable (through blockchain records), capable of assumption by third parties (through key transfer), and have permanence (through the immutable ledger).[97]

Singapore's *Quoine v. B2C2* addresses a different dimension: the enforceability of smart contract execution. When algorithmic trading software executed trades at aberrant prices due to a system malfunction, the exchange sought to reverse them. The Court of Appeal held that trades executed by deterministic algorithms were binding contracts—rejecting unilateral mistake as a defense where the mistake resulted from the exchange's own systems.[98] This decision reinforces the constitutive dimension of synthetic jurisdiction: what the protocol executes is presumptively valid, and the burden falls on challengers to establish grounds for territorial-law intervention.

The English Court of Appeal's decision in *Tulip Trading v. Bitcoin Association* opens a new frontier: fiduciary duties of network developers.[99] The court held that Bitcoin developers may owe fiduciary duties to token holders, allowing the claim to proceed to

[97] *Ruscoe*, [2020] NZHC 728 at [120]–[128] (analyzing whether crypto-assets meet the definition of "property" under New Zealand law and concluding they do because they are identifiable, capable of assumption by third parties, have some degree of permanence, and are capable of being the subject of a claim).

[98] The Singapore Court of Appeal held that cryptocurrency trades executed by deterministic algorithms were binding contracts, rejecting the defense of unilateral mistake where the mistake resulted from the exchange's own systems. *Id.* at [101]–[109].

[99] Tulip Trading Ltd. v. Bitcoin Ass'n [2023] EWCA Civ 83, [2023] 4 W.L.R. 16 (Eng.) (holding that Bitcoin developers may owe fiduciary duties to token holders, allowing claim to proceed to trial).

trial.[100] If developers owe duties to holders, the network itself—synthetic jurisdiction—becomes subject to external accountability through territorial courts. The constitutive/regulative division holds: developers cannot be compelled to change the protocol through court order (that would require changing code that operates by consensus), but they can be held liable for failing to exercise reasonable care in protocol governance.

U.S. bankruptcy courts have provided the most extensive analysis of digital asset property rights. In *In re Celsius Network*, the court held that cryptocurrency deposited in "Earn" accounts became property of the debtor's estate, not customer property.[101] The critical factor was the terms of service: when customers deposited crypto into Earn accounts, title passed to Celsius.[102] By contrast, crypto in "Custody" accounts—where terms preserved customer title—remained customer property.

The *Celsius* analysis illuminates the relationship between control and ownership. Technical control (who holds the keys) did not determine property rights; legal control (who has title under the governing contract) did. Similar analyses in *Voyager* and *BlockFi* confirm that contractual arrangements—not mere key-holding—determine property rights in custodial contexts.[103] This jurisprudence supports the tokenized situs framework's emphasis on legal control as the connecting factor: the applicable law governs who has rights, and who has rights depends on the legal relationships established under that law.

These cases share a common methodology. Courts are not treating digital assets as sui generis phenomena requiring entirely new legal categories. Instead, they apply established

[100] *Id.* at [82]–[85] (Birss LJ) ("The developers of a given network are a sufficiently well-defined group to be capable of being subject to fiduciary duties... The case has a real prospect of success.").

[101] In re Celsius Network LLC, 647 B.R. 631 (Bankr. S.D.N.Y. 2023) (holding that cryptocurrency deposited in "Earn" accounts became property of debtor's estate, not customer property).

[102] *Id.* at 654–58 (analyzing terms of service to determine that title to deposited crypto passed to Celsius upon deposit, distinguishing custodial from non-custodial arrangements).

[103] Compare In re Voyager Digital Holdings, Inc., No. 22-10943 (Bankr. S.D.N.Y. 2022) (similar analysis under different terms of service) *with* In re BlockFi Inc., No. 22-19361 (Bankr. D.N.J. 2023) (reaching similar conclusions regarding commingled crypto holdings).

property principles—identification, permanence, third-party assumption, trust law, contractual interpretation—to new technological facts. The tokenized situs framework organizes this emerging jurisprudence by providing the conflicts infrastructure: courts applying these property principles need a way to determine which jurisdiction's principles apply. Control provides that connecting factor.

IV. TOKENIZED COLLATERAL IN PRACTICE

A. The BlackRock-Barclays-JPMorgan Transaction

On October 11, 2023, BlackRock, Barclays, and JPMorgan executed the transaction that demonstrates the tokenized situs in action. BlackRock tokenized shares in a money market fund on JPMorgan's Tokenized Collateral Network. These tokens were transferred to Barclays as collateral for an OTC derivatives trade. Settlement took one second.

Analyze this transaction through the tokenized situs framework. Where was the collateral located during the one-second transfer? The question is meaningless under traditional lex situs—the token had no location. But the question of which law governed is not meaningless; it was determined by the control structure. The parties had agreed to platform documentation specifying the applicable law. Control passed from BlackRock to Barclays through the blockchain transfer. The applicable law was determined by agreement, implemented through the control mechanism.

The transaction also illustrates synthetic jurisdiction. The TCN platform operates according to protocol rules that the parties accepted by joining the network. The transfer was valid because it complied with those rules—regardless of which territorial law might theoretically apply. The platform's rules, the smart contracts governing transfer, and the consensus mechanism that validated the transaction all form part of the synthetic legal order within which the parties operated.[104]

B. Institutional Expansion

The BlackRock transaction was not isolated. Fidelity International tokenized its Institutional Liquidity Fund on TCN in June 2024.[105] Siemens issued tokenized commercial

[104] J.P. Morgan, *Onyx Documentation* (2024).

[105] *Fidelity Tokenizes MMF on JPMorgan Blockchain*, CoinDesk (June 10, 2024).

paper on Onyx in September 2024.[106] The platform has processed over $300 billion in repo transactions.[107] Each transaction operates within the same framework: control-based property rights, party-selected choice of law, synthetic jurisdiction through platform rules.

Goldman Sachs, BNY Mellon, DTCC, and other major institutions are building competing platforms.[108] McKinsey projects $2 trillion in tokenized real-world assets by 2030.[109] Boston Consulting Group estimates the total tokenization opportunity at $16 trillion by the same date, including both securities and previously illiquid assets like real estate and private equity. The tokenized situs is not a theoretical speculation; it is operational infrastructure for an emerging market.

The competitive dynamics deserve attention. Different platforms implement different versions of synthetic jurisdiction. TCN operates as a permissioned network—only approved participants can join, and JPMorgan controls protocol upgrades. Public blockchains like Ethereum operate through decentralized governance—protocol changes require community consensus, and anyone can participate. Hybrid platforms attempt to combine permissioned security with public blockchain liquidity. Each architectural choice has legal implications: permissioned platforms may more easily satisfy regulatory requirements, but public platforms may offer greater composability with the broader DeFi ecosystem.

The geographic distribution of institutional adoption reinforces the framework's global scope. TCN's participants include institutions headquartered in the United States, United Kingdom, European Union, and Asia. When these institutions transact on a shared platform, they are simultaneously subject to their home jurisdiction's regulatory requirements and to the platform's synthetic jurisdiction. The tokenized situs framework operates at the

[106] *JP Morgan Onyx for Siemens Commercial Paper*, CoinDesk (Sept. 23, 2024).

[107] J.P. Morgan, *Kinexys Asset Tokenization* (2024).

[108] Goldman Sachs, *GS DAP: Digital Asset Platform* 5–12 (2024).

[109] McKinsey & Co., *Tokenization: A Digital-Asset Déjà Vu* (2024).

intersection: it determines which jurisdiction's property law governs while allowing each jurisdiction to impose its own regulatory requirements on participants subject to its authority.

C. Legal Architecture

The legal documentation for tokenized collateral transactions implements the tokenized situs framework through a multi-layered structure. Platform participation agreements establish the synthetic jurisdiction by binding participants to platform rules. Transaction-level agreements specify the applicable law. Smart contract specifications define the conditions under which control transfers.[110]

Consider the documentation hierarchy in a typical institutional transaction. At the platform level, TCN's participation agreement requires all participants to accept platform rules as the baseline governance framework—this creates the synthetic jurisdiction within which transactions occur. The participation agreement specifies that platform rules govern operational matters (what constitutes a valid transaction, how disputes over transaction validity are resolved), while allowing parties to choose applicable law for substantive property and contract questions.

At the transaction level, parties execute documentation that mirrors traditional collateral arrangements but incorporates control-based concepts. A tokenized securities lending agreement specifies: (1) the tokens to be lent, identified by blockchain address; (2) the collateral to be posted, also identified by blockchain address; (3) the smart contracts governing margin calls and liquidation; (4) the applicable law for property rights in the tokens and collateral; and (5) dispute resolution mechanisms. This documentation creates the bridge between synthetic and territorial jurisdiction—parties agree to platform rules while preserving access to territorial courts for disputes that protocol governance cannot resolve.

[110] ISDA, *Clause Library* § 5.2 (2024).

ISDA has developed clause libraries addressing digital assets, providing standardized language for the contractual component of control-based transactions.[111] The LMA has published guidance for DLT in loan trading.[112] These industry developments create the soft infrastructure that allows the tokenized situs framework to operate in practice. When disputes arise, courts can interpret standardized terms against the backdrop of market practice—the same methodology that has proven effective for traditional derivatives and lending documentation.

The integration of legal documentation with smart contract code presents particular challenges. Traditional contracts express obligations in natural language, interpreted by courts. Smart contracts express obligations in code, executed by protocol. When the natural language and the code diverge—as they inevitably sometimes will—which controls? Sophisticated documentation addresses this through hierarchy provisions ("in the event of conflict between the Master Agreement and the smart contract code, the Master Agreement controls for purposes of legal interpretation") and fallback mechanisms (specifying what happens when smart contract execution fails). But these solutions are imperfect; they rely on territorial courts to interpret and enforce agreements that purport to govern computational systems that courts cannot directly control.

[111] ISDA, *Clause Library for Digital Assets* § 3.2 (2024).
[112] LMA, *Guide to DLT Loan Trading* 12–20 (2024).

V. SMART CONTRACTS AND AUTOMATED ENFORCEMENT

Smart contracts—self-executing code on blockchain—create both the mechanism for the tokenized situs and challenges for its implementation. A smart contract can automatically transfer control of collateral when conditions are met: margin calls execute instantly, liquidations proceed without human intervention.[113]

This automation is a feature of synthetic jurisdiction. Within the network, the smart contract's execution is final. But synthetic jurisdiction intersects with territorial jurisdiction, and that intersection raises due process concerns. Traditional secured transaction law requires notice and opportunity to cure before enforcement.[114] Algorithmic liquidation can occur before the debtor knows a margin call has been triggered.

The constitutional dimension cannot be ignored. *Fuentes v. Shevin* established that significant property interests require pre-deprivation notice and hearing.[115] Does smart contract liquidation satisfy this standard? The answer depends on characterization. If the smart contract is viewed as self-help repossession—analogous to a secured creditor's right under UCC § 9-609 to repossess collateral "without breach of the peace"—then procedural protections may not apply.[116] But if the smart contract is viewed as quasi-judicial adjudication of the debtor's default, procedural due process attaches.[117]

The state action doctrine provides the analytical framework. Under *Lugar v. Edmondson Oil Co.*, private conduct becomes state action when two conditions are met: the deprivation results from the exercise of a right or privilege created by state rule, and the

[113] Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996).

[114] U.C.C. § 9-610(B).

[115] *See* Fuentes v. Shevin, 407 U.S. 67, 80–82 (1972) (requiring notice and hearing before deprivation of property); Sniadach v. Family Fin. Corp., 395 U.S. 337 (1969) (extending due process to wage garnishment).

[116] UCC § 9-609 permits self-help repossession "without breach of the peace." Smart contract liquidation arguably satisfies this standard, as no physical confrontation occurs. But the analogy may not hold for consumer transactions. *See* James J. White & Robert S. Summers, *Uniform Commercial Code* § 25-5 (6th ed. 2010).

[117] Matheny v. Parry, 467 F.3d 1290, 1295 (10th Cir. 2006) (discussing procedural due process requirements for property deprivation).

private actor can be characterized as a state actor.[118] Smart contract liquidation presents an interesting case under this framework. The "right" to liquidate arises from the smart contract code and platform terms, not from state-created rules. The protocol developers and validators are not state actors in any traditional sense. On this analysis, smart contract enforcement is purely private ordering—consensual arrangements executed through code.

But a different analysis is possible. *Skinner v. Railway Labor Executives' Association* held that private action becomes state action when the government "compels" or "significantly encourages" it. As regulators increasingly mandate blockchain-based systems—the EU's DLT Pilot Regime, for example, or potential future requirements for tokenized securities—the state action calculus may shift. A smart contract executing on a government-sanctioned platform, enforcing rights recognized by government-enacted statutes, begins to look more like delegated state power than pure private ordering.

The Article 9 self-help analogy deserves closer scrutiny. Courts have consistently held that repossession without breach of the peace does not constitute state action.[119] The secured creditor acts on contractual rights, not state-delegated authority. Smart contract liquidation operates similarly: the creditor's right arises from the lending agreement, and the smart contract merely automates enforcement. But two distinctions matter. First, self-help repossession involves physical action that the debtor can resist—triggering the "breach of the peace" limitation that protects debtor interests. Smart contract execution is instantaneous and irresistible; there is no moment for the debtor to invoke judicial protection. Second, self-help repossession is an exceptional remedy in traditional secured transactions; judicial foreclosure

[118] *See* Lugar v. Edmondson Oil Co., 457 U.S. 922, 937 (1982) (establishing two-part test for state action); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) (private action becomes state action when government compels or significantly encourages it).

[119] On the limits of self-help under Article 9, *see* Williams v. Ford Motor Credit Co., 674 F.2d 717, 719–20 (8th Cir. 1982) (self-help repossession without breach of peace does not constitute state action triggering due process).

remains the norm. In DeFi lending, automated liquidation is the standard—indeed the only—enforcement mechanism.

The tokenized situs framework does not resolve this tension; it clarifies its stakes. The applicable law—determined by the control-based choice-of-law rules—will specify what procedural protections apply. Parties choosing a law that permits algorithmic liquidation accept those terms. But regulators may impose mandatory rules that override party choice, just as they do for consumer protection in other contexts.[120]

The Oracle Problem as Jurisdictional Interface

Oracle systems present the most significant challenge to the tokenized situs framework—and the clearest illustration of its limits. Smart contracts are deterministic: given the same inputs, they produce the same outputs. But smart contracts require external data—prices, events, conditions—that must be fed onto the blockchain through "oracles."[121] This is the "oracle problem": how to import real-world information into a trustless system without reintroducing the trust dependencies that blockchain was designed to eliminate.

The oracle problem is not merely technical; it is the *primary jurisdictional interface risk* in the tokenized situs framework. Recall the constitutive/regulative distinction: synthetic jurisdiction is constitutive (it determines what the ledger says), while territorial jurisdiction is regulative (it determines what consequences follow). The oracle is the point where external information becomes constitutive—where real-world data is inscribed into the authoritative record.[122]

[120] Regulation (EU) 2023/1114, art. 66 (requiring crypto-asset service providers to "act honestly, fairly and professionally in the best interests of clients").

[121] *See* Chainlink, *What Is the Blockchain Oracle Problem?* (2023), https://chain.link/education-hub/oracle-problem.

[122] The constitutive/regulative distinction maps onto this problem. The oracle provides data that the smart contract treats as constitutive—it determines what the ledger will record. But territorial law may treat the oracle's accuracy as a regulative matter—subject to liability if incorrect.

When an oracle reports incorrect data, the constitutive layer is poisoned. Consider a collateralized loan governed by a smart contract that liquidates collateral if the collateral's value falls below a specified threshold. If the price oracle reports an incorrect price—whether through manipulation, error, or latency—the smart contract may execute a liquidation that is "valid" from the perspective of synthetic jurisdiction but "wrong" from the perspective of territorial law.[123]

The Mango Markets exploit of October 2022 illustrates the risk. An attacker manipulated the price oracle to inflate collateral values artificially, then borrowed against the inflated collateral and withdrew the funds before the manipulation was detected. From the protocol's perspective, every transaction was valid—the smart contracts executed exactly as programmed. From territorial law's perspective, this was fraud. The attacker was subsequently charged with commodities fraud and manipulation.

The tokenized situs framework clarifies the legal consequences of oracle failure without resolving the underlying risk. The applicable law—determined by control and party choice—will specify whether oracle providers owe duties to affected parties, what standard of care applies, and what remedies are available.[124] A negligent oracle might face liability under the Restatement's framework for negligent misrepresentation causing economic harm. A manipulated oracle might trigger securities fraud claims. But these are regulative consequences—they operate on persons after the fact. They do not undo the constitutive record on the blockchain.[125]

[123] The Mango Markets exploit of October 2022 demonstrates oracle manipulation risk. An attacker manipulated the price oracle to inflate collateral values, then borrowed against the inflated collateral and withdrew the funds. *See* Indictment at 4, United States v. Eisenberg, No. 1:23-cr-00010 (S.D.N.Y. Jan. 9, 2023).

[124] *See* Restatement (Third) of Torts: Liab. for Econ. Harm § 5 (Am. L. Inst. 2020) (discussing liability for negligent misrepresentation causing economic harm).

[125] On the choice-of-law implications of oracle disputes, *see* Carla L. Reyes, *If Rockefeller Were a Coder*, 87 GEO. WASH. L. REV. 373, 410–18 (2019).

Technological responses to the oracle problem include decentralized oracle networks, which aggregate data from multiple sources to reduce manipulation risk, and economic mechanisms like staking, which create financial penalties for oracle misbehavior.[126] These mechanisms reduce risk but cannot eliminate it. The fundamental insight of the tokenized situs framework is that the oracle represents the boundary between constitutive and regulative jurisdiction—the point where synthetic jurisdiction depends on external data and is therefore vulnerable to external corruption. Risk mitigation at this interface is essential for any collateral structure relying on automated enforcement.[127]

[126] For analysis of decentralized oracle networks as risk mitigation, *see* Steve Ellis, Ari Juels & Sergey Nazarov, *Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks* 12–24 (Chainlink Labs White Paper, 2021).

[127] On the distinction between endogenous risk (within the protocol) and exogenous risk (from oracle data), *see* Nic Carter & Linda Jeng, *DeFi Protocol Risks: The Paradox of DeFi*, in *Regulating Blockchain: Techno-Social and Legal Challenges* 215, 228–32 (Philipp Hacker et al. eds., 2019).

VI. RISK TAXONOMY

The tokenized situs framework provides clarity about which law applies; it does not eliminate the risks inherent in tokenized collateral. A comprehensive risk taxonomy is essential for practitioners structuring transactions and policymakers designing regulatory frameworks. These risks can be organized into four categories: market risks, technological risks, legal risks, and operational risks.

A. Market Risks

Volatility and valuation risk arise because tokens can diverge from underlying asset values. A token representing real estate interests may trade at discounts or premiums unrelated to property fundamentals.[128] Cryptocurrency volatility amplifies this risk—Bitcoin's value has fluctuated by more than 50% within single calendar years. Control-based collateral structures must incorporate appropriate overcollateralization ratios.[129]

The Luna/TerraUSD collapse of May 2022 illustrates algorithmic stablecoin risk. Approximately $40 billion in value was destroyed within days when the algorithmic peg mechanism failed.[130] Collateral structures relying on stablecoins must assess the stability mechanism—whether algorithmic, fiat-backed, or crypto-collateralized—and adjust overcollateralization accordingly.

Liquidity risk is particularly acute for tokenized real-world assets. While the token may be technically transferable on blockchain, finding buyers for fractional interests in illiquid underlying assets may prove difficult.[131] The twenty-four-hour global nature of

[128] Maker Protocol, *Collateralization Ratios* (2024).

[129] *See generally* Christoph Brunnermeier et al., *The Digitalization of Money* (BIS Working Paper No. 941, 2021) (analyzing volatility in digital asset markets).

[130] The Luna/TerraUSD collapse of May 2022 illustrates algorithmic stablecoin risk. Approximately $40 billion in value was destroyed within days. *See* In re Terraform Labs PTE Ltd., No. 24-10070 (Bankr. D. Del. filed Jan. 21, 2024).

[131] On liquidity risk in tokenized markets, *see* Dirk A. Zetzsche, Douglas W. Arner & Ross P. Buckley, *Decentralized Finance*, 6 J. FIN. REG. 172, 195–98 (2020).

crypto markets compounds this risk: margin calls can occur when traditional markets are closed and liquidity is minimal.[132]

B. Technological Risks

Smart contract vulnerabilities present the most prominent technological risk. Code has bugs; bugs can be exploited. The 2016 DAO hack extracted $60 million through a reentrancy vulnerability—a flaw in the code's logic that allowed repeated withdrawals before balance updates.[133] Professional audits, formal verification, and conservative code practices mitigate but cannot eliminate this risk.[134]

Custodial and key management risks exist even when smart contracts function correctly. Private keys can be lost, stolen, or compromised. The FTX collapse revealed that even regulated custodians may commingle customer assets.[135] Multi-signature arrangements reduce single points of failure but introduce coordination complexity.[136]

Quantum computing presents a longer-term threat. Current cryptographic standards—particularly elliptic curve cryptography used in Bitcoin and Ethereum—may become vulnerable to quantum attacks within decades.[137] NIST has begun standardizing post-quantum cryptographic algorithms, but blockchain networks will require coordinated upgrades to implement them.

Network governance risks emerge from the decentralized nature of blockchain consensus. The Ethereum hard fork following the DAO hack demonstrated that communities

[132] Gorton & Zhang document the instability of private money systems without regulatory backing. Gary B. Gorton & Jeffery Y. Zhang, *Taming Wildcat Stablecoins*, 90 U. CHI. L. REV. 101 (2023).
[133] Nathaniel Popper, *A Hacking of More Than $50 Million*, N.Y. Times (June 17, 2016).
[134] Trail of Bits, *Smart Contract Security Best Practices* (2024).
[135] The FTX collapse revealed custodial risk even with regulated entities. Customers' assets were commingled with proprietary trading. *See* In re FTX Trading Ltd., No. 22-11068 (Bankr. D. Del. filed Nov. 11, 2022).
[136] For analysis of private key management risk, *see* Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 870–85 (2015).
[137] On quantum computing threats to current cryptographic standards, *see* NIST, *Post-Quantum Cryptography Standardization* (2024), https://csrc.nist.gov/projects/post-quantum-cryptography.

can split over fundamental decisions, resulting in competing chains.[138] 51% attacks—where a single entity gains majority control of network consensus—present existential risk to smaller blockchains.[139]

The governance problem is not merely technical; it is constitutional in the classical sense. Who has authority to change protocol rules? What happens when the community disagrees? The Ethereum/Ethereum Classic split after the DAO hack illustrates the stakes: one chain reversed the fraudulent transactions (restoring $60 million to the victims), while the other maintained immutability (preserving the attacker's gains). Both chains continue to operate, with different communities and different values. For property law, this creates a novel question: which chain's record is authoritative? The tokenized situs framework cannot answer this question directly—it determines which law applies, not which blockchain fork represents the "real" ledger—but it provides the infrastructure for courts to address the question under applicable law.

Cross-chain interoperability adds further layers of complexity. As assets move across bridges between blockchains—Bitcoin locked on one chain while synthetic Bitcoin circulates on another—the property questions multiply. Which blockchain's record is authoritative for the synthetic asset? What happens when bridge contracts fail, as they have repeatedly (the Ronin bridge hack extracted $625 million, the Wormhole hack $326 million)? The tokenized situs framework applies at each layer: the original asset on its native chain, the locked asset in the bridge contract, and the synthetic asset on the destination chain each present property questions that control-based analysis can address—but each also presents risks that parties must understand and manage.

[138] The Ethereum hard fork following the DAO hack illustrates governance risk. The community split over whether to reverse the theft, resulting in two chains (Ethereum and Ethereum Classic). *See* Vitalik Buterin, *Hard Fork Completed* (Ethereum Foundation Blog, July 20, 2016).

[139] 51% attacks—where a single entity gains majority control of network consensus—present existential risk to smaller blockchains. *See* Joseph Bonneau, *Why Buy When You Can Rent? Bribery Attacks on Bitcoin-Style Consensus*, in *Financial Cryptography and Data Security* 19 (2016).

C. Legal Risks

Regulatory fragmentation creates classification uncertainty. The same token may be classified differently across jurisdictions—security, commodity, payment instrument, or something else entirely.[140] The tokenized situs framework addresses choice of law for property rights, but regulatory classification remains a distinct question that varies by jurisdiction.[141]

The classification divergence is not merely theoretical. A token that is a "security" under U.S. law may be a "crypto-asset" under MiCA, a "virtual asset" under Korean law, and a "cryptographic asset" under Japanese law. Each classification carries different disclosure requirements, licensing obligations, and custody rules. An issuer structuring a cross-border token offering must navigate this matrix—and the choice of law for property rights (which the tokenized situs framework addresses) does not determine regulatory classification (which remains governed by each jurisdiction's regulatory law).

The enforcement landscape compounds complexity. The SEC has pursued enforcement actions against token issuers under U.S. securities law, even when issuers are located abroad and tokens are sold primarily to non-U.S. persons. The CFTC has asserted jurisdiction over crypto-assets as commodities. State attorneys general pursue actions under consumer protection law. Each regulator applies its own classification framework, its own jurisdictional analysis, and its own remedial approach. A tokenized asset perfectly compliant under the property law of one jurisdiction may violate regulatory law in a dozen others.

Cross-border insolvency treatment of crypto-assets remains deeply unsettled. When a crypto custodian becomes insolvent, which jurisdiction's insolvency law applies? Are

[140] SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946).
[141] SEC v. Ripple Labs, Inc., 2023 WL 4507900 (S.D.N.Y. July 13, 2023).

customer assets property of the estate or held in trust?[142] The tokenized situs framework provides the choice-of-law analysis, but substantive insolvency rules differ dramatically across jurisdictions.

AML/CFT compliance obligations create friction for privacy-preserving blockchain architectures. FATF guidance requires virtual asset service providers to collect and transmit originator and beneficiary information—difficult to reconcile with pseudonymous blockchain transactions.[143] Privacy-preserving compliance mechanisms such as zero-knowledge proofs may bridge this gap, but regulatory acceptance remains uncertain.[144]

Sanctions compliance presents particular challenges. When an address is designated by OFAC, transactions with that address become prohibited—but the blockchain continues to accept those transactions regardless.[145] The constitutive/regulative distinction applies: the blockchain records the transaction (constitutive), but territorial law imposes penalties on the persons involved (regulative).

D. Operational Risks

Cross-chain and bridge risks emerge when tokens move between blockchains. Bridge protocols have proven extraordinarily vulnerable—the Ronin Network lost $625 million, Wormhole $320 million.[146] The tokenized situs framework applies within each blockchain;

[142] Cross-border insolvency treatment of crypto-assets remains unsettled. *See* UNCITRAL, *Model Law on Cross-Border Insolvency* (1997); *cf.* In re Celsius Network LLC, No. 22-10964 (Bankr. S.D.N.Y. filed July 13, 2022).

[143] Financial Action Task Force [FATF], *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* 25–40 (2021) (addressing AML/CFT compliance).

[144] Privacy-preserving compliance mechanisms such as zero-knowledge proofs may bridge the gap between regulatory requirements and blockchain privacy. *See* Shafi Goldwasser, Silvio Micali & Charles Rackoff, *The Knowledge Complexity of Interactive Proof Systems*, 18 SIAM J. COMPUT. 186 (1989).

[145] On the interaction between tokenized situs and sanctions compliance, *see* Office of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 2021).

[146] Bridge protocols connecting different blockchains have been frequent attack targets. The Ronin bridge hack of March 2022 resulted in $625 million in losses. *See* Chainalysis, *Cross-Chain Bridge Hacks Emerge as Top Security Risk* (2022).

cross-chain movements create additional complexity as control passes through intermediate protocols.[147]

Oracle risks, discussed extensively in Part V, are operational in nature. The reliability of external data sources determines whether automated enforcement mechanisms function correctly. Decentralized oracle networks reduce single points of failure but do not eliminate manipulation risk.

Environmental risks have become salient for institutional adoption. Proof-of-work consensus mechanisms consume substantial energy, creating both direct costs and reputational concerns.[148] Ethereum's transition to proof-of-stake reduced energy consumption by approximately 99.95%, but Bitcoin and other proof-of-work networks remain energy-intensive.

Interoperability standards remain immature. Different blockchain networks use different protocols, making cross-chain transactions complex and error-prone. Industry efforts to develop common standards are ongoing but incomplete. The tokenized situs framework assumes a functioning blockchain infrastructure; operational failures in that infrastructure create risks that conflicts doctrine cannot address.

Human error remains a persistent operational risk. Private key loss is irreversible—unlike a lost password, a lost private key cannot be reset by any authority. Estimates suggest that 20% of all Bitcoin ever mined is permanently inaccessible due to lost keys. For institutional adoption, this means robust key management infrastructure: hardware security modules, multi-party computation, and recovery mechanisms that balance security against the

[147] On interoperability standards, *see* World Economic Forum, *Digital Asset Interoperability: Principles for Blockchain Network Design* 8–15 (2023).

[148] Environmental concerns focus primarily on proof-of-work consensus mechanisms. Ethereum's transition to proof-of-stake reduced energy consumption by approximately 99.95%. *See* Ethereum Foundation, *Ethereum's Energy Consumption* (2022).

risk of permanent loss. The tokenized situs framework provides the legal infrastructure; operational infrastructure must develop in parallel.

Finally, concentration risk deserves attention. Although blockchain networks are notionally decentralized, practical concentration exists at multiple levels: a small number of mining pools control majority hash power on proof-of-work networks; a small number of validator nodes secure proof-of-stake networks; a small number of infrastructure providers (Infura, Alchemy) route most blockchain traffic. These concentration points create systemic risk—and potential regulatory chokepoints. If a regulator wished to intervene in blockchain transactions, targeting concentrated infrastructure might prove more effective than targeting the nominally decentralized network. The tokenized situs framework's constitutive/regulative distinction anticipates this: territorial regulators act on persons, not protocols, and concentrated infrastructure providers are persons within regulatory reach.

VII. IMPLICATIONS AND RECOMMENDATIONS

The tokenized situs framework has implications for lawmakers, courts, practitioners, and scholars. This Part translates the theoretical framework into concrete guidance for each audience.

A. For Lawmakers: Adopting Control-Based Frameworks

The framework counsels adoption of control-based property concepts. UCC Article 12 provides a model. Jurisdictions that adopt control-based perfection and choice-of-law rules will attract digital asset business; those that cling to location-based concepts will find their property law increasingly irrelevant to the most dynamic asset class in global finance.

Three legislative priorities emerge. First, jurisdictions should enact statutory recognition of digital assets as property—either within existing categories (as England has done through common law development) or as a sui generis category (as the UK Law Commission recommends). Second, secured transactions law should recognize control as a perfection method with super-priority over filing. Third, choice-of-law rules should explicitly adopt party autonomy as the primary connecting factor, with control-based rules as the fallback.

Civil law jurisdictions face particular challenges. The *numerus clausus* principle may require legislative action to create new property categories; judicial development alone may be insufficient. Korea's regulatory approach—protecting customers through trust structures rather than property recognition—provides one model. Germany's ongoing law reform efforts may produce another. The tokenized situs framework is agnostic on the substantive solution; it requires only that some jurisdiction's law applies and that control determines which one.

B. For Courts: Applying the Three-Factor Test

Courts confronting digital asset disputes should apply the three-factor control test developed above. When asked which law governs property rights in a blockchain token, courts should proceed through three inquiries.

First, determine technical control: who holds the private keys? This is typically verifiable through blockchain forensics, expert testimony on transaction histories, or stipulation by the parties. For non-custodial holdings, technical control usually determines the outcome. For custodial arrangements, proceed to the second inquiry.

Second, determine legal control: do contractual arrangements, trusts, or fiduciary relationships allocate control differently from key-holding? The *Celsius* bankruptcy provides the template: examine the terms of service, account agreements, and course of dealing to determine whether the key-holder has title or merely custody. Where legal control diverges from technical control, legal control should generally prevail for choice-of-law purposes—the thief who steals keys does not thereby obtain the right to choose applicable law.

Third, verify effective control: can the legal controller actually exercise control? This serves as a reality check. A beneficiary with legal rights but no practical ability to exercise them—because a custodian is uncooperative, keys are lost, or multi-signature requirements cannot be satisfied—may lack the connection to any jurisdiction that conflicts doctrine requires.

Once control is established, the choice-of-law analysis follows. If the parties have chosen applicable law (through platform terms, transaction documentation, or general agreements), that choice governs—subject to public policy limitations that any choice-of-law regime recognizes. Absent party choice, the law of the controller's habitual residence or principal place of business provides the closest connection.

Courts should resist two temptations. First, the temptation to treat digital assets as sui generis phenomena requiring entirely new legal categories. The emerging jurisprudence demonstrates that existing property concepts—identification, permanence, exclusion, trust, contract—apply to new technological facts.[149] Second, the temptation to defer to protocol outcomes as legally determinative. Smart contract execution establishes what happened on the blockchain; it does not establish what should happen under applicable law. The *Quoine* decision's treatment of algorithmic trades as binding contracts does not mean courts must accept every protocol outcome—it means courts apply contract law (including defenses like fraud, duress, and illegality) to protocol-executed transactions.

C. For Practitioners: Structuring for Certainty

For practitioners, the framework emphasizes the importance of contractual choice of law in digital asset transactions. Party autonomy is the primary connecting factor; parties who fail to specify applicable law leave the question to default rules that may not serve their interests.

Transaction documentation should address five elements. First, explicit choice of governing law—not merely for the contract but specifically for property rights in the digital assets. Second, specification of the control mechanism: which keys, which addresses, which smart contracts govern transfer and enforcement. Third, clear allocation of control between the parties: who holds keys, who can authorize transactions, who bears loss if keys are compromised. Fourth, integration with the platform's terms: major platforms like TCN have their own documentation that may create conflicts with transaction-level agreements. Fifth, dispute resolution mechanisms: which courts or arbitral bodies will resolve disputes, and how will they obtain the technical evidence necessary to apply the three-factor test.

[149] *See generally* Kelvin F.K. Low & Eliza Mik, *Pause the Blockchain Legal Revolution*, 69 INT'L & COMP. L.Q. 135 (2020) (cautioning against treating code-based solutions as legally determinative).

Sophisticated practitioners will also consider insolvency implications. The choice of governing law affects whether customers receive proprietary protection or unsecured claims in the event of custodian insolvency. English and New Zealand law, following *Ruscoe*, may provide stronger customer protection than German law, where *Aussonderung* rights depend on property classification that remains uncertain for crypto-assets. Choice of law is not merely a technical exercise; it is a strategic decision with real consequences for creditor priority.

D. Policy Tradeoffs and Limitations

The tokenized situs framework involves genuine policy tradeoffs that lawmakers and courts should recognize.

First, party autonomy versus regulatory oversight. Control-based choice of law enables parties to select favorable legal regimes—including regimes with minimal investor protection, weak enforcement, or permissive treatment of conflicts of interest. This is regulatory arbitrage by design. The framework trusts parties to select regimes appropriate to their sophistication and risk tolerance. For retail participants, this trust may be misplaced. Mandatory rules—minimum disclosures, segregation requirements, capitalization standards—may be necessary to protect unsophisticated participants regardless of party choice.[150]

Second, efficiency versus accountability. The tokenized situs framework prioritizes transaction efficiency—instant settlement, reduced counterparty risk, lower friction. But efficiency has costs. When smart contracts execute automatically, there is no opportunity for human review of potentially erroneous or fraudulent transactions. When synthetic jurisdiction

[150] The proportionality inquiry reflects the general principle that property rights are not absolute but subject to regulatory limitation. *See* Joseph William Singer, *Property as the Law of Democracy*, 63 DUKE L.J. 1287 (2014).

operates through code, there may be no meaningful appeal from protocol decisions. The *Tulip Trading* litigation—seeking to impose fiduciary duties on developers—represents one attempt to create accountability within decentralized systems. Whether such duties are desirable, and how they can be enforced, remains contested.

Third, innovation versus stability. Blockchain technology continues to evolve rapidly. The tokenized situs framework is designed for current technological reality—cryptographic key pairs controlling assets on distributed ledgers. Quantum computing may break current cryptographic assumptions. Multi-party computation may blur the concept of "control." Artificial intelligence may increasingly make decisions that currently require human authorization. A framework built on control must adapt as the technological meaning of control changes.

E. For Scholars: Research Agendas

For scholars, the tokenized situs framework opens research agendas in conflicts theory, property theory, and the law of technology. How should synthetic jurisdiction interact with territorial jurisdiction when they conflict? What procedural protections should be mandatory regardless of party choice? How should conflicts doctrine adapt as artificial intelligence increasingly determines control?

Three questions deserve particular attention. First, the due process implications of automated enforcement. When smart contracts execute without judicial process, do they implicate state action doctrine? The Article 9 self-help repossession analogy provides a starting point, but the scale and speed of smart contract execution may require different analysis. Second, the relationship between protocol governance and territorial law. When hard forks split networks, which chain inherits the legal obligations of the original? When protocol upgrades change the rules, are participants bound by changes they opposed? Third, the implications of control-based property for traditional property theory. If control is the new possession, what happens to the rich theoretical literature on possession's role in property formation, transfer, and extinguishment?

Emerging technologies will challenge the framework's foundations. Multi-party computation (MPC) enables cryptographic operations to be performed jointly without any single party possessing the complete key material. When control is distributed across multiple parties in this way, who "controls" for conflicts purposes? The three-factor test provides a starting point—technical control is distributed, legal control depends on the arrangements among the parties, effective control asks who can actually authorize transactions—but the details require working out.

Artificial intelligence presents emerging challenges. As AI systems increasingly manage digital assets, the question arises whether AI "controls" assets it manages. Under current doctrine, no: AI systems are tools, and control rests with the humans or entities that deploy them. This answer may become strained as AI systems become more autonomous, but the tokenized situs framework assumes control is attributable to legal persons—a question for future development as the technology evolves.

Finally, the relationship between tokenized situs and public law deserves sustained attention. This Article has focused on private law—property rights, secured transactions, conflicts of law. But digital assets intersect with public law at every turn: securities regulation, tax law, sanctions, anti-money laundering. The tokenized situs framework provides the conflicts infrastructure for private law questions; it does not address how public law jurisdictional claims should be resolved. Whether a token is a "security" under SEC jurisdiction, whether a transaction triggers tax liability, whether dealing with a counterparty violates sanctions—these questions have their own jurisdictional frameworks that interact with, but are not determined by, the tokenized situs.

CONCLUSION

Where is a bitcoin? The question that opened this Article now has an answer: the question is malformed. Bitcoins are not located anywhere. They are computational states distributed across a global network. Traditional conflicts doctrine, built on the premise that property has location, cannot answer questions about property that lacks location.

The tokenized situs provides the replacement framework. Control becomes the new connecting factor. The applicable law is the law chosen by the parties or, in the absence of choice, the law with which the controller has the closest connection. Blockchain networks create synthetic jurisdiction—a layer of computational rules that operates alongside territorial law. The tokenized situs framework connects these layers, providing the conflicts infrastructure for property in computational space.

The framework's key contributions can be stated precisely. First, it explains why traditional conflicts doctrine fails for digital assets: the lex situs rule depends on property having location, and digital assets lack location in the relevant sense. Second, it identifies control as the functional replacement: control is verifiable, tracks the functional reality of property rights, and provides the connecting factor that location cannot. Third, it articulates the constitutive/regulative distinction that explains how synthetic and territorial jurisdiction interact: blockchain networks constitute property rights by determining what the ledger says, while territorial courts regulate those rights by determining their legal consequences.

A crucial clarification on this third point: constitutive jurisdiction—the blockchain's determination of what the ledger records—does not erase voidability under territorial law. A transaction that is valid on the blockchain may still be voidable for fraud, mistake, duress, or illegality under applicable territorial law. But the remedy is in personam, not in rem. The court cannot rewrite the blockchain; it can only act against the persons who control the relevant assets. This means damages, contempt, or orders compelling transfer—not ledger reversal. The constitutive layer remains intact; the regulative layer provides accountability. This division of labor is not a bug but a feature: it preserves the integrity of the blockchain record while subjecting persons who interact with it to legal consequences for their conduct.

The normative case for control rests on its functional superiority to alternatives. Control is epistemically accessible—verifiable by examining publicly available blockchain data. It aligns with the functional reality of digital asset property—who can transfer, exclude, and enjoy benefits. It promotes commercial efficiency—enabling party autonomy and predictable default rules. And it coheres with established property theory—extending traditional concepts of possession and exclusion to computational contexts.

The emerging jurisprudence confirms the framework's practical relevance. English courts in *AA v. Persons Unknown* and New Zealand courts in *Ruscoe v. Cryptopia* have recognized crypto-assets as property. Singapore courts in *Quoine v. B2C2* have enforced smart contract execution. U.S. bankruptcy courts in *Celsius* and *Voyager* have analyzed the property consequences of custodial arrangements. These decisions share a common methodology: applying established property concepts to new technological facts. The tokenized situs framework organizes this jurisprudence by providing the conflicts infrastructure courts need.

The framework's limitations should be stated with equal clarity. It operates at the conflicts level; it does not harmonize the substantive property law that different jurisdictions apply. Civil law systems may classify digital assets differently than common law systems—and those classifications have real consequences, particularly in insolvency. The framework enables regulatory arbitrage; parties can select favorable legal regimes. Whether such arbitrage is desirable depends on one's priors about party autonomy, investor protection, and the proper scope of regulatory authority. These are policy questions that the framework clarifies but does not resolve.

The insolvency consequences deserve particular emphasis. As demonstrated by the contrast between *Ruscoe* (New Zealand trust protection) and *Mt. Gox* (Japanese unsecured creditor treatment), the difference between proprietary protection and relegation to unsecured claims can be trillion-dollar in magnitude across global markets. Rational lenders will deliberately avoid custody arrangements in *numerus clausus* jurisdictions that have not legislatively resolved the property classification question, preferring either common law jurisdictions (where flexible property categories enable trust-based protection) or *sui generis* civil law jurisdictions (such as France) that have created specific legislative mechanisms recognizing blockchain-based property rights. This is not merely theoretical—it is a risk management imperative that will shape capital flows in digital asset markets. The control-based choice-of-law framework enables this sorting function: by permitting parties to select the applicable law, it creates the mechanism through which capital migrates toward protective legal regimes and away from jurisdictions where insolvency means subordination to general creditors.

This is not merely doctrinal refinement. It is paradigm shift. The €25 trillion collateral market is migrating to blockchain infrastructure. Cross-border transactions that once required days now settle in seconds. Institutions that master the tokenized situs framework will be best positioned to navigate the structural realities of digital finance. Those that insist on asking where digital assets are located will find themselves unable to answer the questions that matter.

The tokenized situs is coming whether doctrine accommodates it or not. Commercial practice has already moved. Financial institutions are building the infrastructure. Markets are forming. The question for lawmakers, courts, and scholars is whether to lead the transition or be rendered irrelevant by it. This Article has provided the theoretical framework for that leadership—a framework grounded in functional analysis, supported by emerging jurisprudence, and designed for the property questions that the twenty-first century will increasingly demand we answer.

A final observation on method. This Article has proceeded from commercial reality to legal doctrine—from the BlackRock-Barclays transaction to the constitutive/regulative distinction. This is deliberate. Property law exists to serve commerce, not the reverse. When commercial practice develops new forms of property, doctrine must adapt or become irrelevant. The tokenized situs framework is adaptation: a reconception of conflicts principles that takes seriously the technological reality of blockchain-based property. Future developments—quantum computing, artificial intelligence, new consensus mechanisms—will require further adaptation. The framework's value lies not in providing final answers but in providing a method: functional analysis of property concepts, attention to commercial reality, and willingness to revise foundational premises when those premises no longer apply.

Beale's categorical claim—that property can have no legal situs other than the state where it is—remains true for property that has location. But it was always an empirical claim about the nature of property, not a logical necessity. Digital assets demonstrate the contingency: property can exist without location, and when it does, property law must find new connecting factors. Control is that factor. The tokenized situs is the framework. The paradigm shift is underway.