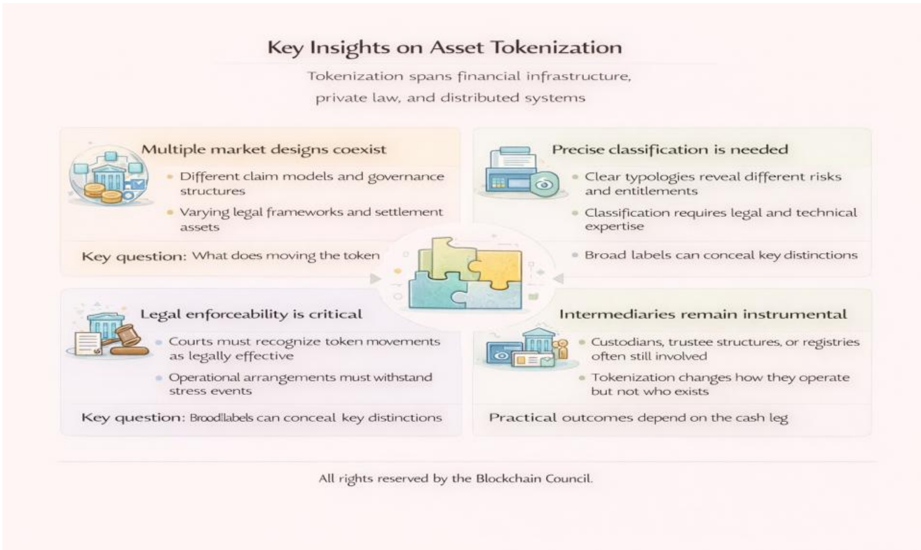
Report on Blockchain and Asset Tokenization

Introduction

Asset tokenization sits at an awkward intersection of financial market infrastructure, private law, and distributed systems engineering. It is discussed with equal confidence by central banks, securities regulators, technology vendors, crypto-native builders, and asset managers, yet there is little agreement on what the term actually denotes in legal or economic terms. In some contexts it refers to the use of blockchain systems to issue securities. In others it refers to digitally native cash equivalents used inside decentralized markets. Elsewhere it describes the digitization of real-economy claims such as invoices, warehouse receipts, or carbon credits. The same label is applied to products with radically different risk profiles, settlement mechanics, and enforceability properties.



This lack of shared meaning has practical consequences. Policy debates often talk past one another because participants are discussing different architectures under the same name. Market commentary alternates between sweeping claims of efficiency gains and warnings of systemic risk without specifying which designs produce which outcomes. Pilot projects are announced as proof of progress, but it is rarely clear whether they demonstrate a path to scale or merely the feasibility of moving data onto a new technical substrate. Even among sophisticated institutions, there is confusion about what a token holder legally owns, where ownership is recorded, and what happens when things go wrong.

This paper is written to address that gap. Its purpose is not to advocate for or against tokenization as a general concept, but to analyze it as a set of concrete market designs. The core claim of the study is simple: tokenization is not one market and not one technology. It is a family of arrangements that share the use of digital tokens but differ in legal structure, governance, settlement assets, and operational dependencies. Meaningful analysis requires disentangling those arrangements and examining them on their own terms.

The study takes a market-structure perspective. It asks how assets are issued, held, transferred, settled, serviced, and used as collateral when token-based systems are introduced, and how those functions interact with existing legal and institutional frameworks. It treats law, infrastructure, and operations as co-equal determinants of outcomes. Technical capability alone is not assumed to produce economic benefit. Likewise, legal permission alone is not assumed to produce adoption. The focus throughout is on where rights sit, how control is exercised, and where failure propagates.

Several observations motivate the approach.

First, most financial markets are already digital. Securities, fund interests, and bank balances have been recorded electronically for decades. The relevant question is therefore not whether information is electronic, but whether the introduction of tokens changes the authoritative record of ownership, the mechanics of settlement, or the allocation of operational responsibility. Without that distinction, tokenization is easily confused with earlier waves of digitization and dematerialization that solved different problems.

Second, many tokenized products rely on existing intermediaries and legal constructs even when they use new technical rails. Tokens are often layered on top of transfer agents, custodians, central securities depositories, trustees, or special purpose vehicles. In such cases, the token does not remove intermediaries; it changes how they interact. This can be valuable, but it also means that claims about disintermediation, instant settlement, or automated compliance need to be examined against the actual control points in the system.

Third, the cash leg matters as much as the asset leg. A tokenized bond that settles against off-chain bank money has a different risk profile from one that settles against a regulated stablecoin, a tokenized bank liability, or central bank money. Much of the recent policy attention to tokenization reflects concern about settlement finality, liquidity under stress, and dependencies on private payment rails. Any analysis that treats asset tokenization in isolation from settlement assets is incomplete.

Fourth, legal enforceability is the binding constraint on scale. A system can process transfers at high speed, but if courts, insolvency practitioners, and regulators do not recognize those transfers as legally effective, institutional adoption will remain limited. Questions of title, control, segregation, priority, and conflict of laws are not secondary details. They determine whether a tokenized position is treated as property or as a mere contractual claim, and whether it survives the failure of an intermediary.

Against that background, this paper has three objectives.

The first is conceptual clarity. The opening sections develop a precise vocabulary and classification schema that can be used across jurisdictions. Instead of relying on broad labels such as “real-world assets” or “digital securities,” the paper classifies tokenized products by the nature of the holder’s claim, the location of the authoritative record, and the legal and operational mechanisms that connect token movement to changes in entitlement. This allows products that look similar at the technical layer to be distinguished where it matters for risk and enforceability.

The second objective is comparative analysis. Tokenization is unfolding unevenly across jurisdictions, shaped by different regulatory choices and legal traditions. Some markets have introduced dedicated statutory forms for ledger-based securities. Others have created controlled sandboxes to test new infrastructure. Others have focused on modernizing private law concepts such as control and electronic transferable records. By using a consistent schema, the paper compares these approaches without forcing them into a single narrative of progress or delay.

The third objective is to ground discussion in observed market behavior. The study draws on public data, regulatory publications, and documented market initiatives to map where activity is actually occurring: which asset classes dominate, which use cases attract sustained volume, and where pilots remain isolated. It avoids projecting adoption curves based on technical possibility alone. Instead, it examines where incentives align for issuers, investors, intermediaries, and regulators.

The paper is written for a mixed audience. It assumes familiarity with financial markets and regulatory concepts, but not deep expertise in distributed systems. It also assumes some understanding of blockchain terminology, but it does not treat any specific platform as a reference point. Technical descriptions are kept at a level sufficient to explain legal and operational consequences. Where specialist terms are used, they are defined in context.

Several boundaries are explicit.

The study does not attempt to value the total addressable market for tokenization. Aggregate market size estimates vary widely and often depend more on assumptions than on data. Instead, the paper focuses on structure, adoption patterns, and constraints.

The study does not treat retail crypto markets as a proxy for institutional tokenization. While there are points of overlap, particularly in settlement assets and public-chain infrastructure, the drivers and risk tolerances differ. Retail market dynamics are referenced only where they affect institutional designs.

The study does not assume that tokenization is either inevitable or universally beneficial. In some contexts, existing infrastructure may already perform well relative to the costs of change. In others, tokenization may introduce new dependencies without offsetting gains. The analysis is intended to make those trade-offs visible.

Methodologically, the paper proceeds from definitions to structure to application.

It begins by fixing terminology and classification. This is not an abstract exercise. Without shared definitions, later discussion of regulation, market segmentation, or risk cannot be interpreted consistently. The taxonomy developed early in the paper is used throughout, so that when a case study refers to a tokenized bond, a tokenized fund, or a tokenized deposit, the reader can infer what that means in terms of legal rights and operational design.

It then maps the global market landscape. Tokenization activity is organized by region and jurisdiction, not by vendor or platform. The analysis highlights how regulatory archetypes shape what kinds of tokenized products can exist and who can participate in them. It also identifies cross-border seams where differences in investor eligibility, settlement assets, or recognition of on-ledger records create friction.

The paper next segments the market by asset class and use case. Instead of treating tokenization as a monolithic phenomenon, it distinguishes between issuance, trading, servicing, and collateral use. It examines why some segments, such as tokenized cash equivalents and collateral management, show faster adoption than others, such as secondary trading of tokenized corporate securities.

A dedicated section analyzes legal enforceability and regulatory comparatives. This section treats enforceability not as a compliance checklist but as a structural determinant of scale. It compares how different jurisdictions address questions of ownership, control, settlement finality, and insolvency in token-based systems, and it highlights areas where legal uncertainty remains a barrier even when technical pilots succeed.

The paper then turns to participants and dependencies. Tokenization changes which intermediaries are central, but it does not eliminate intermediation. Custodians, registries, settlement rail providers, data services, and network operators all become critical nodes. The analysis maps how concentration and dependency risks arise in tokenized markets and how they differ from those in traditional market infrastructure.

Finally, the paper assesses resilience and systemic considerations. It outlines plausible stress scenarios, such as settlement rail disruptions or data feed failures, and examines how different tokenization designs propagate or contain those shocks. The aim is not to predict crises, but to identify where design choices matter most for stability.

Throughout, the paper treats tokenization as a coordination problem. Technical capability, legal recognition, regulatory permission, and market incentive must align for a design to move from pilot to routine use. Many current initiatives demonstrate one or two of these elements, but not all. Understanding why requires looking beyond the token itself to the full claim stack and dependency graph.

The contribution of the study lies in making those layers explicit. By separating token format from legal right, and by mapping market activity onto a consistent schema, the paper provides a framework for comparing tokenization initiatives without relying on promotional language or assuming convergence. It allows policymakers to see where rule changes matter, market participants to see where risk sits, and researchers to ask more precise questions about adoption and impact.

In that sense, the paper is intentionally foundational. It does not close the debate on tokenization. It sets the terms on which that debate can be conducted with greater precision.

Keywords

Asset tokenization, digital tokens, distributed ledger technology (DLT), market infrastructure, securities law, private law, legal enforceability, settlement finality, custody and control, tokenized securities, tokenized funds, tokenized deposits, stablecoins, wholesale CBDC, delivery-versus-payment (DvP), authoritative record of ownership, electronic transferable records, insolvency and segregation, collateral and margining, cross-border regulation, regulatory sandboxes, central securities depositories (CSDs), intermediated holding models, financial market plumbing

Abstract

This paper examines asset tokenization as a set of market designs rather than a single technology or asset class. While tokens are often discussed as a way to modernize finance, products described as “tokenized” differ widely in legal structure, ownership records, settlement assets, governance, and operational dependence. Treating them as one category obscures where value is created, where risk shifts, and why adoption remains uneven across jurisdictions and use cases.

The study develops a precise vocabulary and classification schema based on claims and control. Instead of relying on branding or technical form, it asks what right a token holder has, against whom, and where that right is recorded as legally operative. Tokenized products are classified by instrument type, claim model, location of the authoritative record, and settlement design. This allows cross-border comparison between native and

non-native token structures, direct ownership and intermediated models, and contractual issuer claims, without assuming a single regulatory or technical path.

Using this schema, the paper maps the global market landscape by jurisdiction, asset class, and use case. It shows that current activity clusters around cash equivalents, government securities, fund interests, and collateral workflows, while secondary trading of tokenized securities remains limited. The analysis traces these patterns to legal enforceability, settlement design, and the role of existing market utilities rather than to technical constraints alone.

A central contribution of the paper is its treatment of legal enforceability as the main limiter on scale. Comparative analysis of securities law, crypto-asset regimes, and private law foundations shows how ownership, control, settlement finality, and insolvency treatment differ across markets and shape viable designs. The paper also maps participant roles, concentration, and dependency risks introduced by token-based systems.

By separating token format from legal right and market function, the paper provides a structured basis for evaluating tokenization initiatives without relying on promotional claims. It offers policymakers, market participants, and researchers a common lens for assessing where tokenization fits into financial market infrastructure and where its limits remain.

Definitions, Taxonomy, and Classification Schema

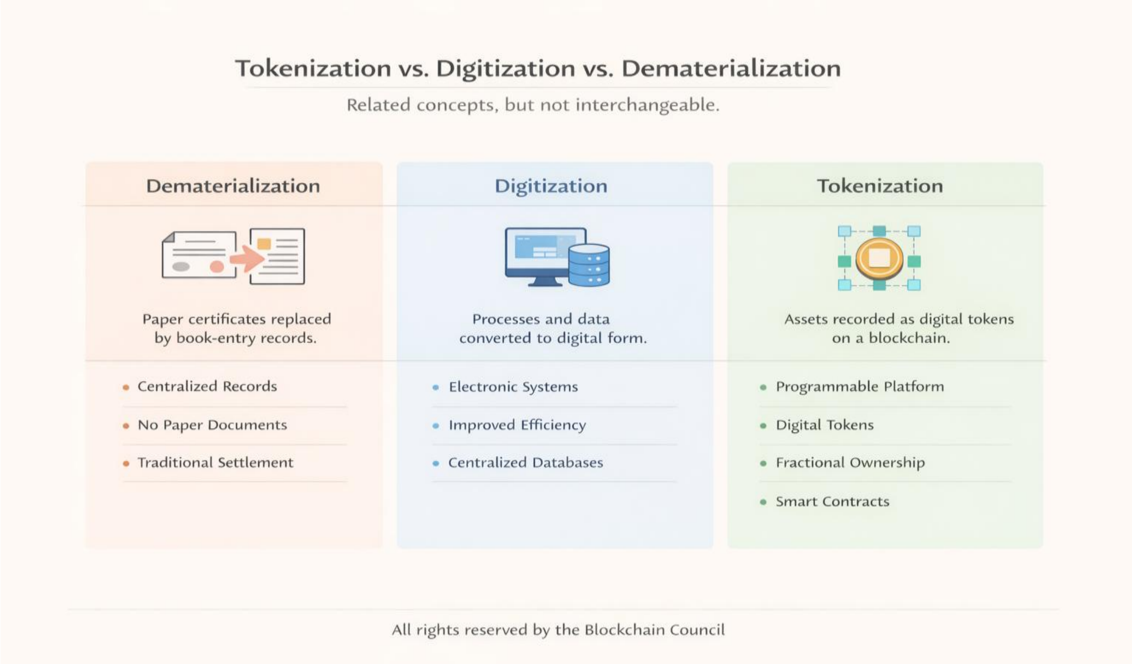
This section sets the shared vocabulary and classification structure used throughout the study. The term tokenization is used unevenly across markets, and sometimes as a marketing label rather than a technical or legal description. The aim here is to fix precise terms, state what a token represents in legal and economic terms, and define a consistent schema that makes cross-border case studies comparable.

Two design choices guide the approach.

First, definitions are written so they work across legal traditions. A term that only makes sense inside one country's securities law, payments law, or property law will not support a global comparison.

Second, classification follows claims and control rather than branding. Market participants often describe a product as "tokenized" even when the authoritative record of ownership is off-chain, settlement occurs in conventional money, or the token merely gates access to a contractual promise. The schema therefore asks: what right does a holder have, against whom, and where is that right recorded as legally operative?

Tokenization vs digitization vs dematerialization



The three terms are related but not interchangeable. Confusion between them is a common source of category errors in policy debate and market reporting.

Dematerialization

Dematerialization is the removal of paper-based certificates and physical documents as the authoritative record of ownership or entitlement. In dematerialized markets, legal ownership is represented through book-entry records maintained by intermediaries and infrastructure providers, commonly through central securities depositories (CSDs), custodians, and registrars.

Dematerialization can exist without any change in how transactions are processed beyond replacing paper with book entry. For public markets, dematerialization is often accompanied by standardized messaging formats, batch processing, and well-defined cutoffs for record dates and corporate actions. A dematerialized instrument can still settle slowly, rely on manual exception handling, and require reconciliation across many parties.

The practical research implication is that a dematerialized market is not automatically a “digital asset” market. Dematerialization mainly answers one question: is paper the controlling record? In many major markets the answer has been “no” for years.

Digitization

Digitization is broader and older. It refers to converting information and workflows into electronic form, generally in centralized databases or within closed networks. Most financial assets are already digitized in this sense. Securities positions, fund units, and bank balances are stored as electronic records in systems of record operated by transfer agents, registrars, CSDs, custodians, and banks.

Digitization improves speed and data handling, but it does not require a shared ledger, a token format, or programmable transfer rules. It also does not change the legal design by itself. A digitized asset can remain governed by the same intermediated holding model, the same settlement finality rules, and the same custody structure.

Digitization also spans different layers:

- **Data digitization**: converting documents, contracts, and records from paper to electronic files.
- **Workflow digitization**: moving processes such as onboarding, subscription, and reporting to electronic systems.
- **Market digitization**: enabling electronic trading, clearing, and settlement via networked infrastructure.

The point is not to subdivide digitization for its own sake. The point is to avoid treating "already electronic" as evidence of tokenization.

Tokenization

Tokenization adds a distinct element: assets (or representations of assets) are recorded and transferred using digital tokens on a programmable platform. A widely used central bank definition describes tokenization as "the process of generating and recording a digital representation of traditional assets on a programmable platform." The IMF similarly describes tokenization as recording and transferring assets on a widely shared and trusted digital ledger that can be programmed.

Under this framing, tokenization is not simply "assets in electronic form," because most assets have been electronic for decades. Tokenization is a specific arrangement in which:

- The asset is represented by a **digital token** that exists as an entry on a ledger.
- The ledger is part of a **programmable platform**, meaning software logic can update a common ledger based on defined rules.
- The token can carry **information and functionality**, not only static data. The BIS notes that digital tokens are entries in a database recorded digitally and may contain both information and functionality.

For research purposes, tokenization is treated as a spectrum rather than a single design. Two products can both be described as "tokenized" while differing on the authoritative record of ownership, the settlement asset used for delivery-versus-payment (DvP), the custody model, and how much logic is executed by code versus by operators.

To make comparisons defensible, this study distinguishes tokenization designs using four technical capabilities that frequently appear in policy and market analysis:

- **Fractionalization**: the ability to represent smaller economic units of an asset, potentially widening access and supporting finer-grained portfolio construction.
- **Programmability**: code-based instructions can execute when conditions are met.

- **Composability**: programmed instructions can be combined and reused to build more complex transactions and products.
- **Atomicity**: multiple steps can execute as one inseparable transaction.

These are capabilities, not automatic gains. Each capability only matters if it is enforceable in law, supported by governance, supported by custody and operational controls, and measured against observed outcomes.

Token types used in this study

The token universe is often described with retail crypto categories such as payment tokens, utility tokens, and NFTs. That taxonomy is too coarse for a study of market structure for tokenized financial and real-world assets. This research classifies tokens by the nature of the represented claim and the regulatory perimeter that commonly applies.

Native vs. non-native tokens (authoritative record)

A central distinction is whether the token ledger is intended to be the authoritative record of ownership or whether it is a representation layered on top of an existing system.

1 Native tokens

Native tokens are structures in which the token ledger is intended to serve as the official record of ownership or entitlement. In some implementations the on-chain record is the primary record and may be supported by off-chain backup records. IOSCO notes that tokenized products differ on whether off-chain or on-chain records are the official legal source of ownership, and that such differences can confuse investors if not properly disclosed.

In native designs, the token transfer is meant to be the legally operative act that updates ownership, subject to any transfer restrictions and eligibility rules. When native design works as intended, it reduces the gap between "technical settlement" and "legal settlement" because the ledger event and the legal state change are the same event.

Native design, however, raises demanding questions that must be answered explicitly in any case study:

- What legal rule makes the ledger authoritative?
- Who can amend the record if a transfer is impermissible, mistaken, or fraudulent?
- How are insolvency and segregation treated when the record of entitlement is on the platform?

2 Non-native tokens

Non-native tokens are structures in which the authoritative record remains off-chain in a traditional system, such as a transfer agent, registrar, or CSD. Tokens represent interests, access, or contractual claims linked to that off-chain record. IOSCO notes that investor rights to the underlying assets in non-native structures can vary widely depending on how the linkage is designed and disclosed.

Non-native structures can be easier to deploy because they may fit existing legal and operational frameworks. Yet they can also recreate the same reconciliation and dependency issues that tokenization is sometimes said to remove. If token transfers are not legally operative by themselves, then some off-chain process must mirror the transfer, confirm eligibility, and update the legal record.

For research measurement, the practical question is not whether a token exists. It is whether token movement is legally and operationally coupled to the off-chain record in a way that is consistent, auditable, and resilient to disputes.

Instrument-based token categories (what is being tokenized)

To support comparability, this paper uses five instrument categories based on what the token represents and what rules commonly apply.

Tokenized securities

Tokens representing equity, debt, or structured instruments that would generally be treated as securities (or similar regulated financial instruments) in most jurisdictions. This includes corporate bonds, asset-backed securities, and, in some regimes, tokenized shares or units of money market funds if treated as securities or fund interests.

This category is used when the token maps to an instrument that normally triggers prospectus or offering rules, market abuse rules, and custody and recordkeeping duties.

Tokenized fund interests

Tokens representing units or shares in collective investment schemes, including money market funds, private funds, or ETFs, depending on jurisdiction. The defining feature is that investors hold a fund interest rather than a direct pro rata interest in each underlying asset.

Fund interests bring specific operational requirements that often matter more than trading mechanics: subscription and redemption cycles, valuation points, fee calculations, transfer restrictions, and investor reporting.

Tokenized deposits and bank liabilities

Tokens representing claims on a regulated deposit-taking institution, commonly intended to serve as the cash leg for settlement or as a store of bank money on a token platform.

These are not "stablecoins" in the common retail sense if they remain a bank liability within a regulated perimeter.

This category matters because settlement in bank liabilities interacts with deposit protection, prudential rules, and the operational role of the issuing bank.

Tokenized real assets and title-linked instruments

Tokens linked to real estate interests, commodities, carbon credits, invoices, warehouse receipts, or other real-economy entitlements. In many cases, this category depends on legal recognition of electronic transferable records and on clear methods for proving and transferring control.

This category includes both tokenized claims on a pool of assets (for example, shares in a property SPV) and token structures intended to correspond to a transferable document (for example, a warehouse receipt).

Tokenized synthetic exposures

Tokens that provide price exposure via contractual promises, derivatives-like payoffs, or issuer guarantees without necessarily holding the underlying asset in a bankruptcy-remote structure. IOSCO notes that some non-native tokens can provide synthetic exposure rather than being backed by actual exposure, shifting counterparty risk to the token issuer.

This category is not a moral judgment; it is a risk and rights classification. Synthetic exposure can be legitimate and regulated when structured as a derivative or note. The research question is whether the token's marketing and disclosures match the legal reality of the holder's claim.

Cash-leg tokens (settlement assets)

Although this study focuses on asset tokenization, the cash leg often determines whether a tokenized market can grow beyond pilots. Settlement design affects credit risk, finality, liquidity management, and regulatory requirements.

This paper uses the following labels for settlement assets:

- **Tokenized deposits**: bank money represented on a token platform.
- **Stablecoins**: typically issued by non-bank entities, with regulatory treatment varying by jurisdiction and structure.
- **Wholesale CBDC**: central bank liabilities designed for wholesale settlement.
- **RTGS-linked settlement**: off-chain central bank money settlement in an RTGS system linked to token movement.

These labels are analyzed separately from the tokenized asset because two cases that tokenize the same instrument can have very different risk profiles if they settle in different cash legs.

Asset classes covered and how they are mapped

For a global study, asset coverage must be broad enough to capture major market trajectories but structured enough to support consistent comparisons. This research groups assets into three top-level buckets. Each tokenized product is mapped to one bucket and one subcategory.

Public market instruments

Public market instruments tend to have clearer legal frameworks, established custody norms, and standardized disclosures.

1 Sovereign and quasi-sovereign debt

- Sovereign debt: treasury bills, notes, and bonds.
- Agency and supranational debt.

These instruments often test whether tokenization changes issuance cycles, allocation mechanics, secondary trading access, and settlement timelines, while preserving established investor protections.

2 Corporate and listed instruments

- Investment grade and high yield corporate debt.
- Listed equities.
- Exchange-traded products (ETFs and ETNs, where relevant).

In these subcategories, measurement focuses on whether tokenization changes post-trade processing, corporate actions handling, and liquidity formation, and whether any benefits survive the reality of compliance gating and existing market infrastructure.

Private market instruments

Private markets are often cited as a natural fit because settlement timelines are longer, intermediaries are numerous, and processes remain manual or fragmented in many segments. They also feature heterogeneous legal structures and bespoke transfer restrictions.

1 Fund interests and ownership interests

- Private equity fund interests.

- Infrastructure and project finance interests.
- Structured private products (SPVs, feeder funds).

For these instruments, the research focus is often on transfer restrictions, cap table management, investor eligibility, and servicing.

2 Credit and receivable instruments

- Private credit and loan participations.
- Trade finance receivables and invoice financing.

Here the research focus is whether tokenization reduces onboarding friction, improves transferability within constraints, supports better servicing and reporting, and reduces dispute rates.

Real assets and commerce-linked instruments

This bucket includes assets where "ownership" is tied to title, possession, or control of a document or record.

Real estate and property-linked structures

- Real estate interests via SPV shares.
- Fractional interests where legally permitted.

- Title-linked instruments where a token is meant to correspond to a title record or transferable document.

Commodities, environmental attributes, and logistics documents

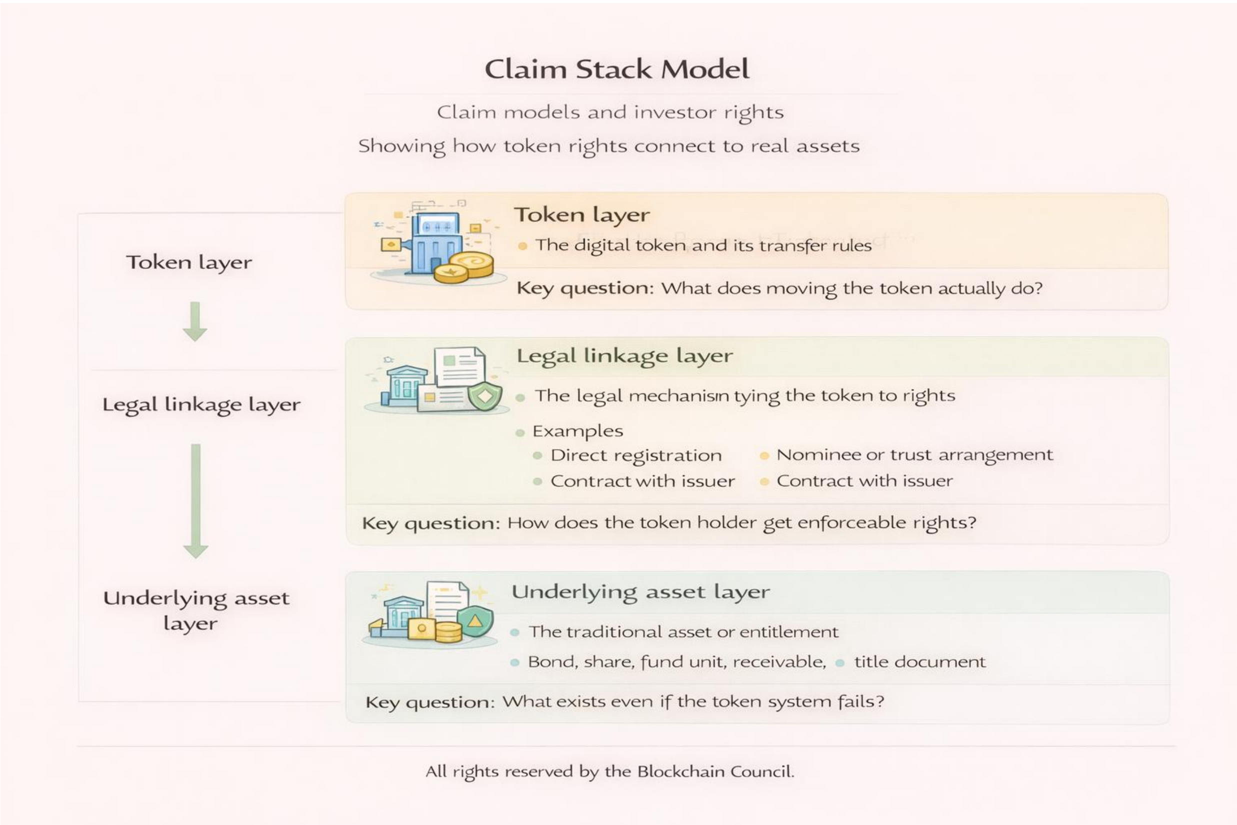
- Commodities, such as tokenized warehouse receipts or allocated metals claims.
- Carbon credits and environmental attributes.
- Logistics documents (bills of lading, warehouse receipts).
- Agricultural finance instruments (warehouse receipt financing).

For these instruments, the central research focus is the linkage between the token and the enforceable right, and how "control" is established and proven across borders.

Claim models and investor rights

Tokenization systems can look similar at the technical layer while creating very different legal and economic rights. A research-grade comparison therefore models every tokenized asset as a claim stack with three layers.

Claim stack (three-layer model)



1 Underlying asset layer

The underlying asset is the traditional instrument or entitlement: a bond, share, fund unit, receivable, title document, or commodity claim. This layer defines the baseline legal rights that exist outside the token system.

2 Legal linkage layer

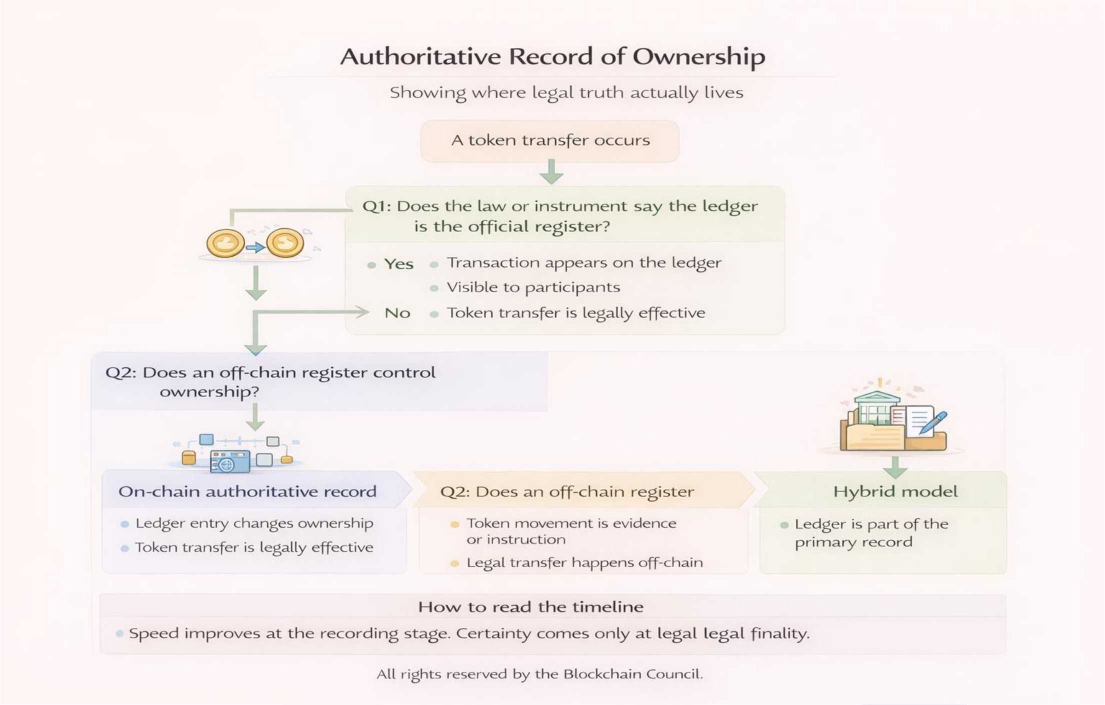
The legal linkage is the mechanism connecting token holders to the underlying asset. Examples include direct registration rules, nominee or trustee arrangements, contractual terms against an issuer, or statutory recognition of an electronic transferable record.

3 Token layer

The token layer is the digital representation and its transfer rules: how tokens are minted, transferred, restricted, redeemed, burned, and corrected. This layer is where platform logic and governance show up directly.

Across case studies, the central question is: what does the token holder legally own or control, and what is treated as the authoritative record?

Three core claim models



This study uses three claim models to classify tokenized products in a way that remains comparable across jurisdictions.

Model A: Direct title or direct registered ownership via the token ledger (native model)

- The token ledger is intended to be the authoritative record of ownership.
- Transfers on the ledger are intended to change ownership directly, subject to applicable rules.

Model A provides the clearest conceptual mapping between token transfer and ownership transfer. It also places heavy demands on legal recognition of ledger records, settlement finality rules, governance procedures, and dispute resolution.

In case studies classified as Model A, special attention is paid to the source of legal authority for ledger updates, the scope of operator powers, and what happens if ledger state conflicts with external records.

Model B: Beneficial ownership via an intermediary (intermediated model)

- The underlying asset remains in an off-chain system.
- Tokens represent beneficial interests recorded by a transfer agent, custodian, trustee, or nominee.
- Token transfers may be mirrored by off-chain updates.

Model B can be easier to deploy because it can sit inside established rules for custody, recordkeeping, and client asset protections. Yet it can also reintroduce reconciliation steps, operational dependencies, and disputes about which record controls in edge cases.

In case studies classified as Model B, the research focuses on how mirroring is performed, what happens during exceptions (fails, reversals, freezes), and whether the platform adds meaningful process change or mainly a new interface.

Model C: Contractual claim on a token issuer or SPV (issuer claim model)

- The token holder has a contractual right against the issuer.
- The issuer may or may not hold the underlying asset on a segregated basis.

IOSCO notes that some structures represent synthetic exposure, while others are backed by actual exposure, and that protections may be weaker than conventional securitizations if bankruptcy-remote structures are not used.

Model C concentrates counterparty risk in the issuer and puts a premium on plain disclosure. A holder may believe they "own the asset," while legally they own a claim against a company or SPV that references the asset.

Authoritative record of ownership

A recurring cross-jurisdiction issue is the identity of the authoritative record.

- Some implementations treat off-chain book-entry records as the official legal source of ownership and use on-chain records as a convenience layer.
- Others treat on-chain records as the official legal source of ownership, with off-chain records as backups.

- Hybrid approaches also exist, where the blockchain is part of the primary recordkeeping system, but an operator retains unilateral powers to correct impermissible transactions.

This distinction matters for investor protection and for research measurement because "on-chain settlement" does not necessarily mean "legally final settlement." A ledger update can be reversed at the legal layer if finality has not been reached or if governing rules allow correction.

Control, possession, and transferable records in commerce

For tokenized instruments linked to trade and title documents, the legal concept of control is central. The UNCITRAL Model Law on Electronic Transferable Records (MLETR) treats an electronic transferable record as functionally equivalent to a paper transferable document if a sound method is used to identify the record, maintain its integrity, and establish exclusive control by a person. Control is treated as the functional equivalent of possession.

For the purposes of this study, control is treated as a measurable attribute rather than a slogan. In case studies involving warehouse receipts, bills of lading, or similar instruments, the paper records:

- How exclusive control is established.

- How control transfers from one party to another.
- How integrity is protected.
- Whether local law recognizes that control as equivalent to possession.

Where legal recognition is incomplete, the case study documents the workaround used (for example, contractual commitments, operator undertakings, or reliance on existing registries) and the residual risk that follows.

Minimum disclosure fields for investor rights

Investor confusion often stems from unclear rights and unclear records. For a tokenized asset to be treated as suitable for institutional analysis in this study, the following disclosure fields are treated as minimum required:

- The authoritative record of ownership (on-chain, off-chain, or hybrid).
- The legal nature of the token (security, fund interest, deposit claim, or contractual claim).
- Whether underlying assets are held in a segregated, bankruptcy-remote structure.
- Roles and responsibilities of the issuer, custodian, transfer agent, and platform operator.
- The circumstances under which transactions can be corrected, reversed, or frozen.
- Redemption terms and liquidity constraints.

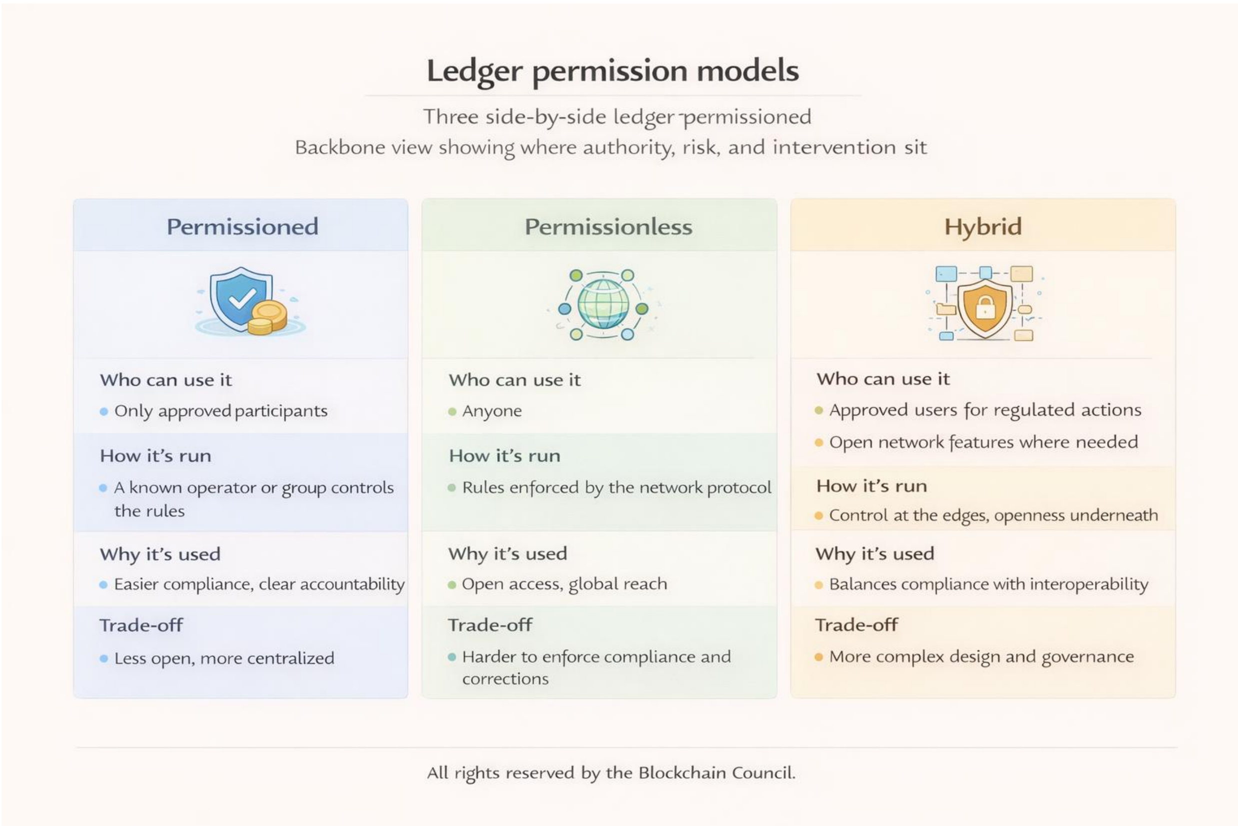
These disclosures are later used as scored indicators in the readiness index.

Ledger models and platform governance

Tokenized markets vary not only by asset type and legal structure, but also by ledger design and platform governance. The BIS describes programmable platforms as technologies that allow eligible participants to develop and execute applications that update a common ledger, and it describes a “token arrangement” as the set of platforms and participating entities that enable financial market functions using digital tokens.

This study classifies ledger models along five dimensions. The goal is not to select a single “best” architecture, but to make architectural differences visible in a way that supports risk and outcome comparisons.

Permission model



1 Permissioned networks

Participants are approved, identity is known, and governance is typically managed by an operator or consortium. Deterministic transaction processing is more common, and compliance controls can be enforced at the node or account layer.

2 Permissionless networks

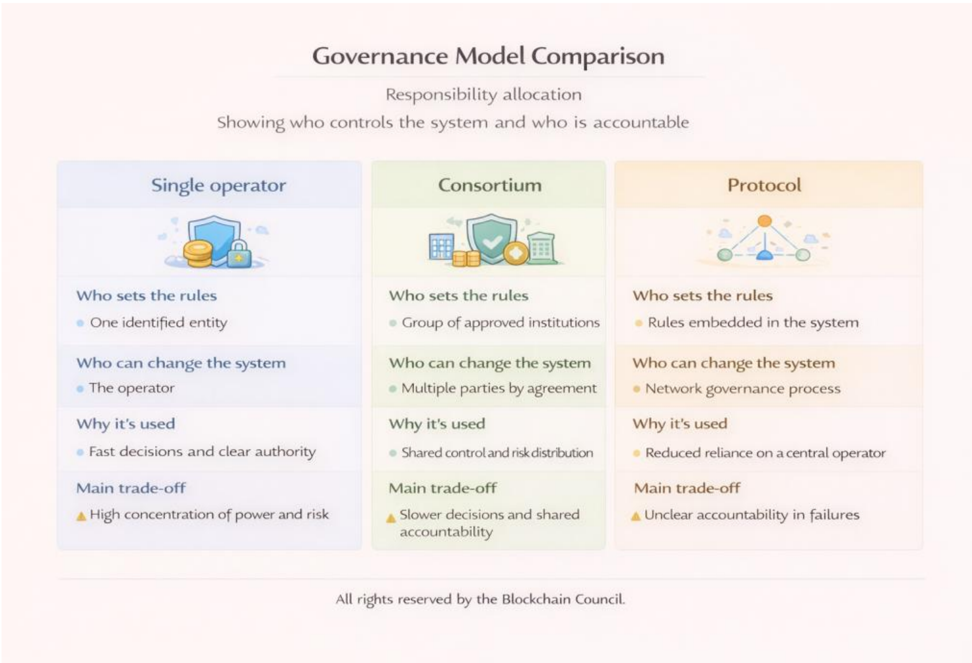
Participation is open, consensus is decentralized, and settlement can be probabilistic depending on protocol design. Compliance controls, where present, often sit at the application layer rather than the base ledger.

3 Hybrid models

Hybrid models combine controlled access for regulated functions with limited use of public networks, such as anchoring, timestamping, or posting settlement proofs. Another hybrid form issues tokens on a public network but uses transfer restrictions and identity controls to limit who can hold or move the token.

The permission model matters because it shapes identity assurance, governance procedures, compliance enforcement, and the handling of technical or legal exceptions.

Governance model



Governance Model Comparison

Responsibility allocation

Showing who controls the system and who is accountable

	Single operator	Consortium	Protocol
Who sets the rules	One identified entity	Group of approved institutions	Rules embedded in the system
Who can change the system	The operator	Multiple parties by agreement	Network governance process
Why it's used	Fast decisions and clear authority	Shared control and risk distribution	Reduced reliance on a central operator
Main trade-off	▲ High concentration of power and risk	▲ Slower decisions and shared accountability	▲ Unclear accountability in failures

Single-operator governance

One entity controls upgrades, node admission, rule changes, and corrective actions. This can simplify decision-making, but it concentrates power and can create single-point operational and legal risk.

Consortium governance

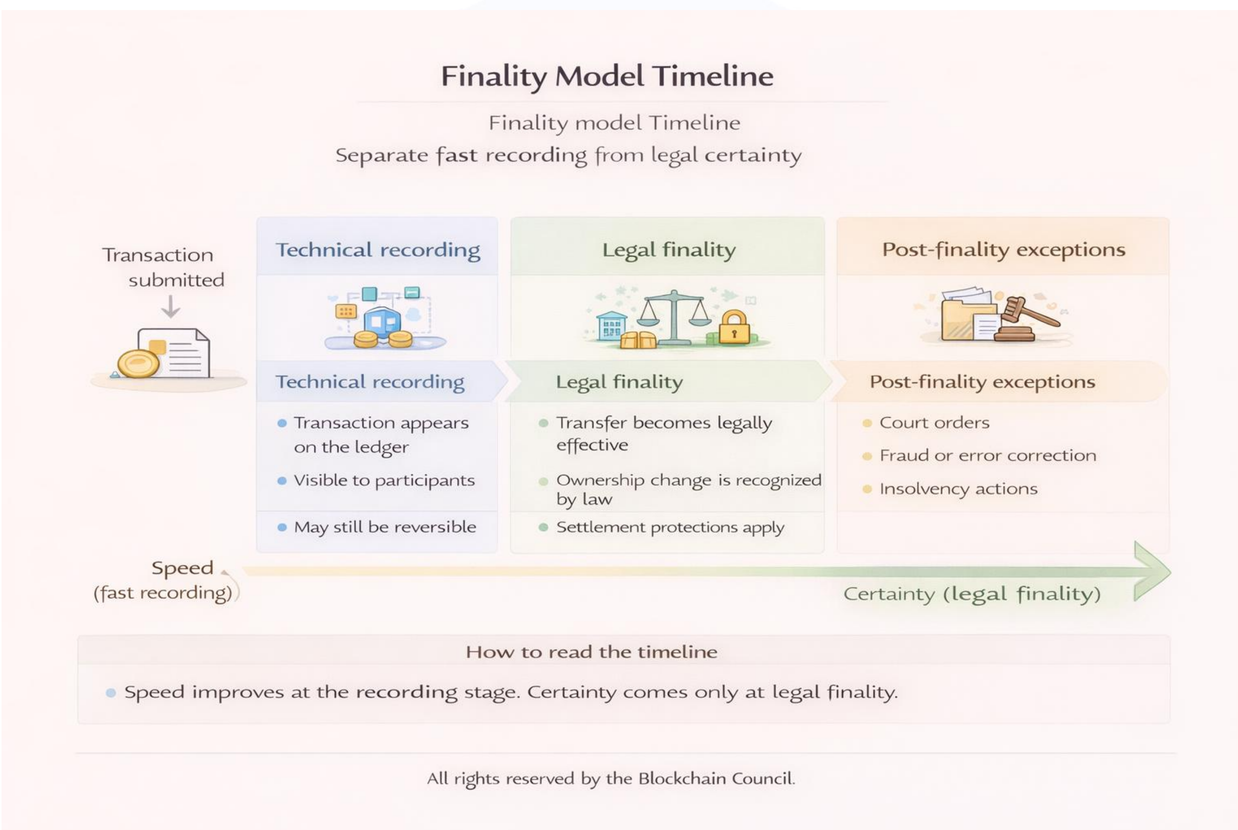
Rule changes and upgrades require multi-party agreement. Consortium governance can distribute risk and reduce unilateral control, but it can also slow change and complicate accountability when faults occur.

Protocol governance

Governance is embedded in protocol rules, sometimes involving token-based voting or community processes. Protocol governance raises questions about who bears fiduciary or regulatory duties, how disputes are resolved, and how emergency actions occur.

Governance affects legal finality, operational resilience, the practical ability to implement compliance requirements, and the allocation of responsibility when code and law diverge.

Finality model



Legal finality is a legally defined moment after which a transfer cannot be revoked or unwound. IOSCO notes that the point at which operational token transfers coincide with legal final settlement can be unclear depending on technology features and design choices, and it notes additional uncertainty in multi-layer network designs.

For each case study, the paper records:

- Whether finality is deterministic or probabilistic.
- The contractual definition of finality used by the operator.
- How finality is mapped to applicable settlement finality laws, where relevant.
- How errors and disputes are handled after "finality" at the technical layer.

A case can have fast technical recording but delayed legal finality. The study treats those as different outcomes.

Single-ledger vs. multi-ledger arrangements

Single-ledger arrangements

Issuance, transfer, and settlement all occur on one platform. This can reduce interfaces and timing gaps, but it concentrates operational dependency in one system.

Multi-ledger arrangements

The asset exists on one ledger while the cash leg or compliance registry exists on another. This design requires interoperability mechanisms such as messaging, bridging, or coordinated settlement procedures.

Layered networks

Assets may exist on a layer that depends on another layer for security or settlement assurance. IOSCO notes that layered designs can complicate finality analysis.

Multi-ledger and layered arrangements are treated as first-class design choices in this study because they affect settlement risk, operational risk, and where points of failure live.

Data availability and confidentiality model

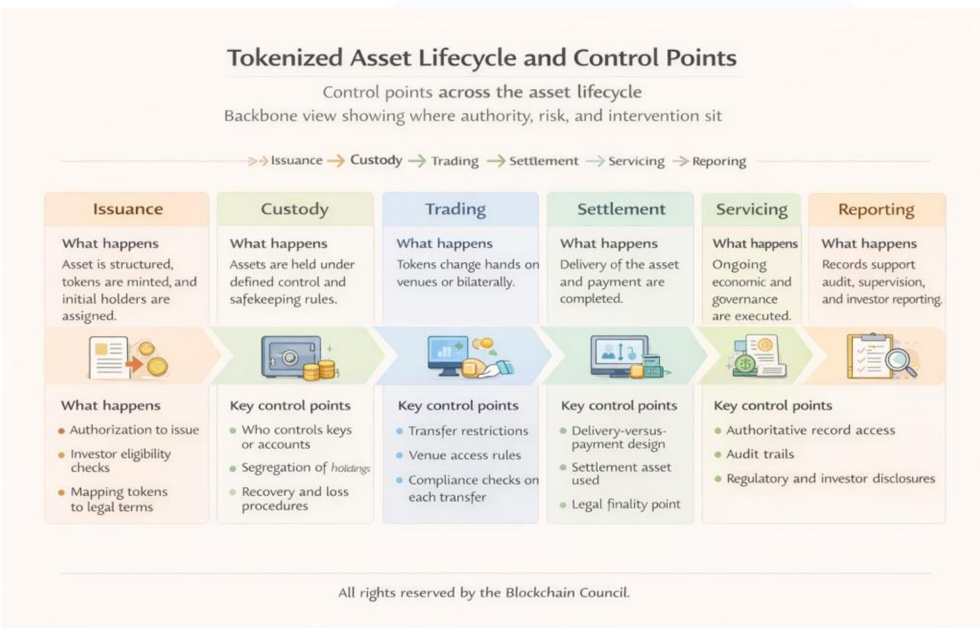
Institutional adoption often requires selective disclosure, privacy, and compliance logging. This study classifies confidentiality approaches as:

- **Open readability**: ledger data can be read broadly, sometimes publicly.
- **Restricted readability**: a permissioned ledger where only approved parties can read full data.

- **Privacy-enhanced designs**: selective disclosure and other confidentiality methods that limit what counterparties and observers can see while still supporting audit and compliance.

Each approach carries trade-offs for auditability, market surveillance, interoperability, and user privacy.

Control points across the asset lifecycle



Tokenization can change the asset lifecycle by moving multiple functions into a shared ledger environment with programmable logic. To compare projects consistently, the study breaks the lifecycle into six stages and defines “control points” at each stage. A control point is a moment or mechanism where a party can approve, block, reverse, or otherwise determine the state of ownership, transfer, or settlement.

The purpose of this mapping is practical: it makes accountability visible. It also reduces the risk that a case study overstates "on-chain" activity when the real decision points remain off-chain.

Issuance

Control points during issuance include:

- Asset creation and legal documentation.
- Minting of tokens and mapping to issuance terms.
- Investor onboarding and eligibility checks.
- Primary allocation and subscription flows.
- Delivery of disclosures and capture of consents.

Research focus: does tokenization reduce issuance cycle time, reduce manual checks, or lower operational error rates? Where cycle time falls, the case study records whether the change comes from shared data, from code execution, from simpler governance, or from a narrower investor set.

Custody and safekeeping

In tokenized markets, "custody" can mean private key management, control of a wallet, or control of an account on a permissioned network. The study records:

- Who controls private keys or signing authority.
- Whether custody is direct (investor-controlled) or intermediated (custodian-controlled).
- Segregation model (omnibus vs segregated addresses).
- Recovery procedures, incident response, and loss allocation.

For commerce-linked instruments, custody also intersects with legal control concepts under frameworks like MLETR.

Custody analysis is not limited to technology. It also includes legal duties, operational arrangements (such as multi-signature policies), and the practical ability to recover from compromised keys or operator failure.

Transfer and trading

Control points in transfer and trading include:

- Transfer restrictions such as allowlists, jurisdiction gating, holding periods, and investor caps.

- Venue rules: bilateral transfer, request-for-quote (RFQ), order book, or automated market maker (AMM) designs.
- Compliance controls embedded in transfer logic.
- Corporate actions eligibility cutoffs and record dates.

Research focus: do restrictions reduce secondary liquidity, or do they allow compliant liquidity that could not otherwise exist? The study treats this as an empirical question and records what evidence is available on turnover, depth, or other liquidity proxies.

Settlement

Control points in settlement include:

- Whether DvP is achieved and how it is implemented.
- Settlement asset type (tokenized deposits, stablecoins, CBDC, or RTGS linkage).
- Netting and finality rules.
- Fail management and dispute handling.

Because legal finality may not match technical recording, settlement design is documented with both technical and legal lenses. Where a platform offers “instant settlement,” the case study separates (i) recording time, (ii) availability of the settlement asset, and (iii) the legal point of no return.

Servicing and corporate actions

Many expected gains are in servicing rather than in trading. Servicing includes interest payments, dividend distribution, fees, redemptions, and voting. Control points include:

- Interest, dividend, and fee calculations.
- Tax withholding logic and reporting.
- Voting rights and proxy mechanisms.
- Redemptions and burn mechanisms.
- Lifecycle events such as calls, maturities, and conversions.

Research focus: can servicing be executed by code without unacceptable model risk, oracle risk, or governance risk? The case study documents where external data enters the system, who is responsible for that data, and what happens when data is wrong or late.

Reporting, audit, and supervision interfaces

Control points for oversight include:

- Audit trails and immutable logs.
- Data access for regulators and auditors.
- Market surveillance hooks for integrity monitoring.
- Incident reporting and logging of corrective actions.

The study evaluates whether tokenization reduces reconciliation needs while preserving strong oversight and auditability. Where a platform claims that audit becomes "built in," the case study asks what auditors and supervisors can actually see, under what permissions, and in what timeframes.

Standardized case study template

To enable consistent comparison across jurisdictions and asset classes, every case study in this paper follows the same template. The template forces clarity on investor rights, authoritative records, settlement design, and measurable outcomes. It also reduces the risk that narratives focus on technology while skipping legal and operational design.

Case identification

- Case name and short description.
- Jurisdiction(s) and applicable legal regime.
- Asset class and instrument category (from Sections and).
- Maturity stage (pilot, limited production, scaled production).
- Target investor segment (retail, accredited, institutional).

Economic terms and lifecycle

- Instrument terms (coupon or dividend, maturity, fees, redemption rules).
- Corporate actions and servicing requirements.
- Transferability constraints and eligibility rules.

Rights and authoritative record

- Claim model (direct title, beneficial ownership, issuer contractual claim).
- Authoritative record of ownership (on-chain, off-chain, hybrid).
- Evidence of ownership and dispute resolution process.

- Segregation and insolvency treatment (including bankruptcy-remote structures if used).

Token and platform design

- Token standard or specification used (if disclosed).
- Permission model (permissioned, permissionless, hybrid).
- Governance model (operator, consortium, protocol).
- Finality model and legal mapping approach.
- Interoperability dependencies (bridges, messaging layers, settlement links).

Custody and control

- Custody model (self-custody, regulated custodian, nominee).
- Key management and recovery procedures.
- Controls for freezes, reversals, and corrective transactions.

Compliance and supervision

- KYC/AML approach and eligibility enforcement.
- Transfer restriction logic and monitoring.
- Regulator access model (reporting feeds, node access, audit access).

Measured outcomes and evidence grading

- KPIs tracked (issuance time, settlement time, fail rates, servicing execution rates, cost metrics).
- Data sources and whether metrics are audited, independently verified, or self-reported.
- Secondary market metrics (if applicable): turnover, depth, spread proxies, redemption behavior.
- Incidents: operational failures, governance events, smart contract issues, dispute cases.

Risk analysis

- Main risks by category: legal, operational, technology, liquidity, counterparty, governance.
- Risk mitigations in place and their tested effectiveness.
- Residual risk assessment.

Replicability assessment

- Preconditions for replication in another jurisdiction.

- Dependencies that limit portability (legal recognition, settlement asset availability, custody infrastructure).
- Implementation complexity rating.

Tokenized Asset Lifecycle and Infrastructure Patterns

A tokenization project usually fails (or pays off) at the handoffs.

The market overview can tell you *where* tokenization is showing up. That does not tell you *how* the work runs end to end. In live systems, the stress points are predictable: issuance to distribution, trading to settlement, custody to servicing, servicing to collateral reuse, and finally unwind. These are also the points where teams discover mismatched records, unclear responsibility, and weak assumptions about finality.

Regulators often evaluate tokenization by taking the familiar functions of capital markets and mapping them onto a new technical stack. They then ask what changes when parts of the workflow become programmable: who can change a record, who is accountable when code misbehaves, what "final" means when there are multiple ledgers, and what happens during outages or chain governance events. IOSCO uses an explicit lifecycle lens—issuance and distribution, trading and post-trade, and asset servicing such as custody and collateral management—and notes that risks can appear in different ways depending on architecture and token structure.

This section uses that lifecycle lens to do two things:

1. Give a practical blueprint for the tokenized asset lifecycle, from claim design to unwind.
2. Introduce a small set of infrastructure patterns you can reuse across instruments and jurisdictions.

The goal is not to promote any one network or product. The goal is to make the moving parts legible.

A lifecycle blueprint you can reuse

You can treat the phases below as the backbone of the section. Each phase includes the design choices that tend to drive later constraints.

Phase 0: Asset and claim design

Before any code, decide what is being tokenized and what the token *means*.

Claim type and legal form

Define the legal claim the holder receives. Examples include:

- A direct security
- A beneficial interest
- A deposit-like claim
- A fund unit
- A contractual right

Write down whether the token is intended to be the definitive ownership record or a parallel record used for convenience.

Ownership record model

Tokenization is partly a record-keeping question. Some implementations place the definitive record on a regulated venue ledger. IOSCO describes an example under Swiss law in which SDX's distributed ledger is the main register and definitive record of ownership, with the SDX CSD supporting issuance, settlement, custody, and ownership recording into that register.

Other implementations keep the authoritative register off-chain and treat the blockchain record as a mirror or evidence layer.

Tokenization structure

Distinguish common structures early, because they change everything downstream:

- **Token as record of title** vs **token as representation** with an off-chain register taking priority
- **Native on-chain instrument** vs a **digital twin** representation

IOSCO notes that in some tokenized money market fund structures, the blockchain record may act as proof of ownership or as a backup record. Depending on setup, issuers or transfer agents may have the ability to correct records.

These choices are not just technical. They determine who can reverse errors, how disputes are resolved, and what "possession" means.

Phase 1: Pre-issuance architecture choices

This is where "infrastructure patterns" start to matter. Use ICMA's lifecycle framing for DLT-based debt securities as a scaffold: pre-issuance considerations, issuance, registration and safekeeping, trading and settlement, investor considerations, servicing and lifecycle events, and third-party engagement.

Network and governance choice

Start with the network model and governance. The question is not simply "public vs private." It is what permissions exist at each layer and who controls them.

- **Validator layer**: who can run nodes and participate in consensus
- **Access layer**: who can read, write, or submit transactions
- **Application layer**: who can deploy and invoke contracts, and under what policies

IOSCO distinguishes public permissionless and permissioned arrangements and uses layered terminology to frame risks.

Where the "golden record" lives

Pick the placement of the authoritative record.

- **On-chain as single source of truth** (possible for certain instruments and jurisdictions)
- **Off-chain authoritative register** with an on-chain mirror

This decision drives reconciliation work, audit approaches, and the role of transfer agents and CSDs.

Smart contract control and change management

Decide how code changes and emergency actions work.

- Upgradeability model (fixed contracts vs upgrade paths)
- Emergency controls and pause mechanisms

- Bug response and rectification procedures nIOSCO points to smart contract bugs and the difficulty of rectification, especially on public permissionless chains.

Treat these controls as part of governance, not as a developer preference. They are core to operational risk.

Phase 2: Issuance and primary distribution

Write this phase as a sequence with explicit gates. A simple, repeatable sequence is:

1. Issuance authorization
2. Minting
3. Allocation
4. Investor eligibility checks
5. Delivery into custody or to investor wallets under custody controls

Identity and eligibility enforcement

Regulated distribution depends on identity, eligibility, and transfer restrictions.

Permissioned token standards can embed identity checks and restrictions in token logic. ERC-3643 is often presented as an identity- and compliance-forward standard for regulated assets.

Transfer restrictions as code

Spell out how restrictions are enforced:

- Who can hold the asset
- Which transfers are permitted
- What happens on forced transfer or legal action
- How rule updates are approved

The key point is architectural: controls can move "left" into the asset itself when transfer rules sit in contract logic.

Disclosure and investor communications

Tie disclosure artifacts—terms, risk factors, offering documents—to token metadata and to lifecycle events. If documents can change, record who can change them and how notice is delivered.

Primary issuance delivery

Describe the delivery model:

- Delivered into a custodian account
- Delivered into an investor wallet with custodian policy controls
- Delivered into an on-venue custody arrangement

Make the custody boundary explicit because it defines who is responsible for keys, sanctions screening, and loss recovery.

Phase 3: Secondary trading and market structure

Split the question into (1) where trading happens and (2) how it connects to post-trade.

Venue models

Common models include:

- Traditional exchanges extending to tokenized instruments
- Permissioned DLT venues
- Bilateral OTC workflows (common in private credit, repo, and structured products)

Different venues imply different rules for membership, surveillance, transparency, and settlement timing.

Fragmentation and interoperability

As tokenization spreads, fragmentation becomes a practical constraint. IOSCO flags interoperability and fragmentation as material issues.

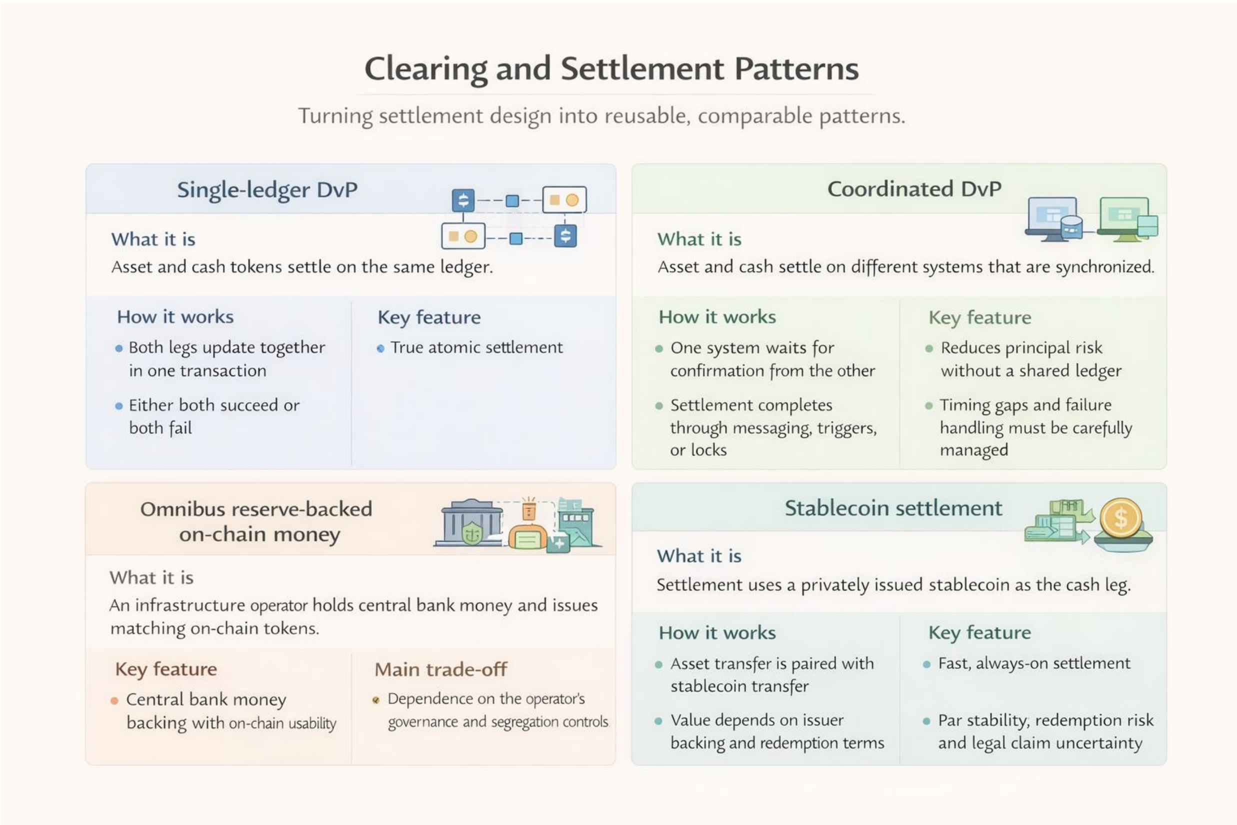
In design terms, fragmentation shows up as:

- Multiple token standards and identity schemes
- Incompatible settlement assets
- Bridging or messaging layers that add new risk
- Parallel liquidity pools with thin depth

Operational differences

Proponents argue tokenized fixed income can reduce siloed data, fragmented workflows, and manual processes that lengthen settlement periods. When the workflow is truly end-to-end, shorter cycles can follow. When it is not, teams often add new steps to reconcile on-chain state with off-chain books.

Phase 4: Clearing and settlement patterns



This is the core infrastructure section. Settlement is where legal finality, credit exposure, and liquidity meet.

DvP and atomic settlement as the organizing concept

CPMI describes tokenization work that targets atomic settlement of multi-leg transactions such as delivery versus payment (DvP) and payment versus payment (PvP). The idea is simple: all legs execute or none execute. This reduces principal risk by conditioning the final settlement of one obligation on the other.

Use DvP as the organizing frame:

- What DvP means in a token context
- How conditional execution works on programmable platforms
- How multi-leg synchronization is achieved (single ledger vs coordinated ledgers)
- Where automation is safe and where manual intervention still exists

Atomicity is not a marketing term. It is an architectural property. You can only claim it if you can show how both legs reach finality under the same set of failure modes.

Settlement asset choices and the money leg

Many institutional pilots stall here because the “money leg” carries the hardest constraints: central bank money access, credit risk, operating hours, liquidity, and regulatory perimeter.

CPMI describes options central banks consider for providing central bank money as a settlement asset in token arrangements, including:

- Linking existing central bank payment systems to token platforms
- Issuing tokenized central bank money
- Making tokenized central bank money available on multi-asset platforms alongside tokenized deposits, with DvP across updates and interbank settlement

The IMF's Fintech Note on tokenized reserves adds a structured typology and compares tokenized asset settlement solutions, including:

- **RTGS link approaches** (trigger or synchronization) that coordinate delivery of a tokenized asset on a DLT platform with payment in traditional reserves
- **Omnibus account models** where a financial market infrastructure (FMI) holds funds at the central bank and issues on-chain money tokens fully backed by reserves

Write this subsection as a comparison with stable criteria. The goal is to make trade-offs visible.

Comparison criteria

- **Finality and atomicity**: can the design produce true all-or-nothing settlement, or only coordinated completion with residual timing gaps?
- **Use of central bank money vs private credit risk**: is the money leg a claim on the central bank, a bank deposit, an e-money claim, or a stablecoin?
- **Hours of operation and liquidity**: does the system run continuously, and if so, how is liquidity managed outside RTGS hours?
- **Governance and accountability**: who runs the rails, who can intervene, and under what rules?

- **Integration burden**: what needs to change in existing FMI processes and legal documentation?

The IMF notes that all six solution types it compares support DvP, but that atomic settlement depends on architecture, and that single-ledger coexistence of money and assets can enable atomic settlement.

A catalog of settlement patterns

Define a short pattern catalog you can refer to throughout the paper.

Pattern 1: Single-ledger DvP

Money tokens and asset tokens live on the same platform. DvP can be atomic because the platform can commit both legs together.

Key questions:

- What is the settlement asset (tokenized central bank money, tokenized deposits, another form)?
- Who controls issuance and redemption of the money token?
- What is the finality model and what law governs it?

Pattern 2: Compatible-ledger DvP (coordinated settlement)

Money and asset legs sit on different systems. A synchronization mechanism coordinates completion (for example, an RTGS link style design).

Key questions:

- How is synchronization implemented (messaging, triggers, locking, conditional release)?
- What happens if one system completes and the other fails?
- Who is responsible for dispute handling and unwind?

Pattern 3: Reserve-backed on-chain money via an omnibus structure

An FMI holds funds at the central bank and issues on-chain money tokens backed 1:1 by reserves.

Key questions:

- How are backing and segregation proven and audited?
- What redemption rights exist and when?
- What happens during insolvency or operational outage?

Pattern 4: Stablecoin settlement

Settlement uses a stablecoin as the payment leg.

CPMI contrasts stablecoin settlement with deposit-based settlement and notes issues such as deviations from par and the lack of settlement in central bank money.

Key questions:

- What supports the stablecoin's value, and what are redemption terms?
- What is the legal claim of the holder?
- How does the design manage par drift and run risk?

Phase 5: Custody, safekeeping, and key management

Custody is both a legal control function and a technical security function.

Custody models

Describe custody as a spectrum:

- Full custody
- Shared custody
- Hosted custody
- Self-custody

IOSCO treats custody as part of asset servicing and focuses analysis on custody and collateral management.

The custody model answers practical questions:

- Who can move the asset?
- Who bears loss if keys are compromised?
- How are sanctions and transfer restrictions enforced?
- What does recovery look like if keys are lost?

Key management patterns

Explain key security in concrete terms.

- Hardware security modules (HSMs)
- Multi-party computation (MPC)
- Policy controls (limits, whitelists, time locks)
- Approval workflows (dual control, segregation of duties)
- Recovery and re-key procedures

Reconciliation and exception handling

Even when the token ledger is authoritative, firms keep internal books.

Cover:

- How on-chain balances are reconciled to internal records
- What triggers exceptions

- Who can correct a record and how the correction is logged

This is where "token as title" versus "token as mirror" becomes operationally visible.

Phase 6: Asset servicing and lifecycle events

Servicing is where tokenization's promise is loudest and where scaled operations are hardest.

IOSCO defines asset servicing as operational support across lifecycle activities, including custody, valuations, accounting, compliance reporting, and transaction processing such as dividend or income distribution. Its discussion focuses mainly on custody and collateral management, but the broader servicing perimeter still matters for a lifecycle view.

Coupon, dividend, and income distribution

Write the distribution workflow as a set of steps:

- Event declaration and parameters
- Record date logic and entitlement snapshot
- Entitlement calculation
- Distribution execution
- Tax withholding or reporting hooks where applicable

Clarify which parts can be encoded and which parts still depend on off-chain inputs (rates, tax forms, or corporate resolutions).

Corporate actions

Corporate actions are rarely "one click," even on chain.

Cover major categories:

- Splits and consolidations
- Calls and redemptions
- Conversions and exchanges
- Consent solicitations
- Elections and optional events

Explain what can be enforced by token logic and what requires agent discretion and legal steps. Corporate actions are also where forced transfer features and legal intervention clauses in security token standards become relevant.

Tokenized fund servicing

For tokenized funds, include:

- NAV publication and price feeds
- Subscriptions and redemptions

- AML review flows
- Transfer agent responsibilities and correction rights

Reporting and audit trails

Chain state can prove some things well—timestamped transfers and current balances, for example. Other facts still require external attestation, including identity checks, valuation sources, and cash backing in some money token designs.

Make the boundary explicit: what is proven by ledger state and what relies on off-chain evidence.

Phase 7: Collateral, repo, securities lending, and asset mobility

Collateral is a high-impact area because small time savings can translate into real liquidity value.

IOSCO notes observed implementation of digital custody and improved collateral mobility, including examples such as intraday repo transactions.

Industry signal: DTCC real-time collateral tokenization

DTCC has announced a platform for tokenized, real-time collateral management using its AppChain framework, aimed at institutional collateral workflows. DTCC describes its

Collateral AppChain as network-agnostic, supporting assets issued on various networks while connecting with existing market infrastructure.

Use this example to show how many early deployments focus on back-office mobility and risk controls, not retail trading.

Collateral workflow patterns

Structure the subsection around concrete patterns.

Eligibility and valuation rules

- Eligibility schedules and asset filters
- Haircuts and margin rules
- Concentration limits
- Rule enforcement and exceptions

Substitution and intraday mobility

- Substitution rights and timing windows
- Intraday movements and cut-off logic
- Event hooks that update eligibility after price moves or corporate actions

Reuse and rehypothecation controls

- Permission rules for reuse
- Traceability of reuse chains where possible
- Limits on re-pledge depth

Default management and liquidation

- Default triggers and notice steps
- Freeze and transfer controls
- Liquidation workflows and sale procedures n Keep the focus on control points: who can trigger actions, what evidence is needed, and what happens during disputes.

Phase 8: Redemption, buybacks, default events, and unwind

A lifecycle section is not complete without the end of the lifecycle.

Redemption and buyback flow

Describe the mechanics:

- Burn vs lock mechanisms
- Cash leg design and settlement choice
- Timing: when redemption is final and when it can be reversed

Defaults, payment failures, and dispute handling

Cover failure modes that matter in practice:

- Missed payments and cure periods
- Disputes over ownership or eligibility
- Smart contract faults and emergency controls

Forks, outages, and chain governance events

Discuss operational continuity:

- Outage playbooks
- Reconciliation after halted blocks or congestion
- Governance decisions that affect transaction validity

Tie this back to legal finality. A system needs a credible path to preserve the legal record even when the technical system is stressed.

Phase 9: Cross-cutting risk, controls, and accountability

IOSCO's framing is useful here: many risks map to existing categories, but can be amplified or show up in new ways depending on the DLT architecture and tokenization structure.

IOSCO points to operational vulnerabilities such as cyber-attacks on nodes, congestion, data leakage, smart contract bugs, and key loss.

A practical way to write this part is to map controls to stages.

Controls by lifecycle stage

Pre-issuance

- Threat modeling and security reviews
- Contract testing and third-party audits
- Governance, change control, and emergency procedures

Issuance and distribution

- Eligibility enforcement and transfer restrictions
- Allocation controls and investor communications
- Document control and notice rules

Trading

- Venue surveillance and access controls
- Membership rules and permissions
- Interoperability constraints and bridge risk controls

Settlement

- Finality model and legal basis
- DvP assurance and failure handling
- Liquidity arrangements and operating hours

Custody

- Key security, approvals, and recovery
- Segregation of duties and policy enforcement
- Incident response and loss allocation

Servicing

- Event governance and authorization
- Data integrity and oracle controls
- Auditable record of off-chain inputs

Collateral

- Valuation sources and margin rules
- Concentration limits and liquidation safeguards
- Default triggers and dispute handling

Controls are only meaningful when ownership of each control is clear.

A reusable pattern language for tokenization infrastructure

Many papers describe tokenization as a single idea. Production systems look more like a set of repeatable patterns combined in different ways.

A layer model you can apply consistently

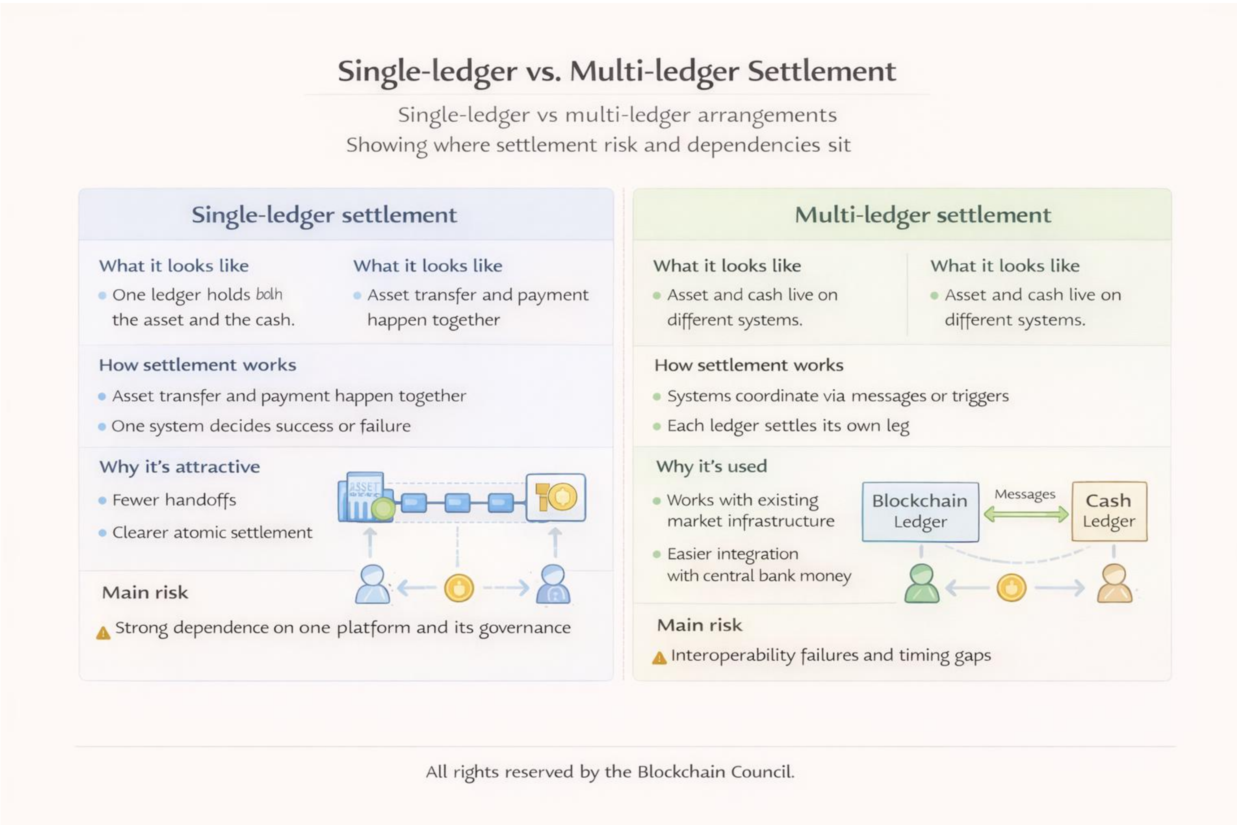
IOSCO's layered model helps describe architectures without getting trapped in product names.

Use these layers as a standard template:

- **Access / application layer**: wallets, user interfaces, APIs
- **Service / contract layer**: on-chain logic, identity checks, transfer rules
- **Asset / token layer**: token creation, mint/burn, permissions, metadata
- **Platform / settlement layer**: ledger state, consensus, finality, cross-ledger interaction

If you describe each system you cite using these layers, the paper stays coherent across networks and jurisdictions.

Unified ledger and multi-ledger approaches



The BIS describes a unified ledger concept as a common venue where central bank digital currencies, private tokenized monies, and tokenized assets can coexist on one programmable platform. It also stresses that this does not require one global ledger; APIs can connect multiple ledgers.

Pair that concept with "network of networks" approaches seen in market pilots.

IOSCO includes an example describing the Canton network as a network of applications where ledger replication is not publicly available in the same way as fully replicated public chains, framing it as an interoperability approach. Canton has also described pilots that span tokenization, fund registry, digital cash, repo, securities lending, and margin management, with interoperability across applications.

In practice, the choice is often not “single ledger or not.” It is:

- Which assets and money legs must share a ledger to meet settlement goals
- Where it is acceptable to use coordinated completion across ledgers
- How governance and accountability work across applications

Compliance-forward token standards

Treat token standards as programmable interfaces for eligibility and legal controls.

- **ERC-3643** is commonly presented as a permissioned token standard that embeds identity checks and transfer restrictions at the token layer.
- **ERC-1400 and related security token standards** include interfaces and events for issuance and redemption, and may include forced transfer capabilities for legal action contexts.

The paper does not need developer detail. What matters is what these standards enable:

- Eligibility checks baked into transfer rules
- Transfer restriction updates under defined governance
- Forced actions under a legal process

- Better audit trails for who initiated changes

Institutional signals that show how adoption may unfold

DTCC tokenization services and time-bounded regulatory posture

The SEC's no-action letter for DTC's DTCC Tokenization Services is a useful marker for how regulators may permit time-bounded pilots with defined constraints.

The letter describes withdrawal without further action three years after launch and references anticipated launch timing for the preliminary base version, with later expansion envisioned subject to additional parameters.

Use this to discuss:

- How systemically important FMIs may test tokenization in staged steps
- Likely guardrails around scope, participants, and risk controls
- A plausible path from pilot features to broader clearing agency compliance

Collateral modernization as a near-term wedge

DTCC's tokenized collateral work, including its Collateral AppChain descriptions, shows a path that prioritizes mobility and control in collateral operations rather than retail-facing tokenized equities.

This matters because collateral workflows have clear pain points, clear participants, and clear measures of value (time, funding use, and operational error rates).

Practical indicators for market maturity

A jurisdiction can publish a tokenization policy lane and still have little real activity. For research mapping, it helps to separate **permission to operate** from **evidence of operation**.

A practical maturity scan can use five observable indicators.

1) Repeated issuance, not one-off pilots

A single issuance can prove that documentation, onboarding, and settlement can be made to work once. Repeated issuance is more meaningful because it tests staffing, controls, and exception handling over time. Hong Kong's repeated tokenized green bond issuance pattern illustrates the difference between a demonstration and a program (HKMA [16]; Treasury Bureau [17]).

2) Who holds the asset, and how they hold it

Markets with only bilateral transfers among a small group of institutions behave differently from markets that can support broader institutional distribution or limited retail access. A research map should note whether holdings are constrained to:\n

- a closed institutional group,\n
- professional investors under a licensed venue perimeter,\n
- a hybrid where traditional custody remains available,\n
- or direct on-chain holding where allowed.

3) Evidence that the cash leg works in routine operations

Many tokenized instruments can be issued with off-chain cash, but broader activity requires predictable cash movement and settlement finality. Indicators include whether the jurisdiction is testing:\n

- regulated stablecoin rails (under local rules),\n
- tokenized bank liabilities,\n
- wholesale CBDC settlement or interfaces,\n
- or other central bank money solutions (ECB [6]; BIS [31]).

4) Post-trade and servicing reality

Issuance numbers alone can mislead. Servicing is where real work concentrates: register updates, corporate actions, NAV calculations, reporting, and handling exceptions. A market that can run those steps under audit and supervision is more mature than a market that can mint tokens but still relies on manual servicing and reconciliation.

5) Pathways for institutional risk controls

Institutions adopt new infrastructure when they can apply familiar control patterns: segregation of duties, approval chains, and documented incident processes. In practice, this shows up in custody policy design (multi-party approvals, role separation), change control for smart contracts, audit and assurance coverage for underlying holdings, and documented procedures for freezes and court-ordered transfers.

Taken together, these indicators turn a "policy map" into a market map. They also support segmentation by showing where tokenization is functioning as a full lifecycle process versus where it is still functioning as a front-end format layered onto traditional servicing and settlement.

Regulatory design trade-offs that shape tokenization outcomes

Jurisdictions often face the same design trade-offs and resolve them in different ways. Those choices explain why tokenization outcomes vary.

Trade-off 1: Legal certainty vs controlled experimentation

Some jurisdictions aim to create a clear legal category for ledger-based instruments and license venues and intermediaries accordingly (Switzerland is often discussed in this light via the DLT Act and FINMA licensing activity (FINMA [9], [10])). Others create controlled lanes to test infrastructure functions and gather evidence for future rule changes (EU DLT Pilot Regime and UK DSS (EUR-Lex [1]; Bank of England [2]; FCA [7])).

For segmentation, the difference matters because controlled lanes often come with scope limits that constrain asset choice and investor reach. A jurisdiction can be "ahead" in infrastructure experimentation while still having low issuance volumes because the lane is intentionally narrow.

Trade-off 2: Where the authoritative record sits

Markets that keep the authoritative record in a CSD or transfer agent and use tokens as synchronized representations can preserve familiar investor protections, but they may carry ongoing reconciliation work between systems. Markets that place the authoritative record on a ledger can reduce some duplication, but they must specify how corrections, reversals, and court orders work in ledger operations.

This trade-off is not only technical. It determines what investors truly hold and what they must rely on if something goes wrong.

Trade-off 3: Open networks vs controlled participation

Public chain formats can support broad accessibility for permitted products, but they raise questions about transfer enforcement, custody risk, and dependence on public network governance. Permissioned networks can support controlled participation and may fit institutional expectations more easily, but they concentrate governance and operational dependence in fewer hands.

A research map should treat this as a choice about control and dependence, not as a debate about ideology.

Trade-off 4: Tokenized instrument first vs tokenized cash first

Tokenizing instruments without addressing the cash leg often produces “paper benefits”: faster issuance steps paired with slow settlement and manual reconciliation. Approaches that address the cash leg early—regulated stablecoins, tokenized deposits, wholesale CBDC interfaces—aim to remove that ceiling (MAS posture and the ECB’s settlement experimentation are examples of this policy direction (Reuters [15]; ECB [6])).

Trade-off 5: Market structure continuity vs new venues

Some approaches emphasize continuity: instruments remain tied to existing venues and post-trade utilities while tokenization becomes an additional format. The US post-trade utility signals around DTC tokenization services point toward this approach (SEC [4];

DTCC [12]). Other approaches create dedicated venues or infrastructure lanes that test new combinations of trading and settlement functions.

Continuity can speed adoption because it uses existing distribution, custody, and compliance paths. It can also create a different concentration risk: tokenization becomes dependent on the choices of a few utilities and their approved networks.

Cross-asset structural patterns that matter more than the "asset type" label

Asset class labels are useful for organizing the map, but the operational and legal structure often matters more than whether the underlying is a bond, a fund unit, or a credit exposure. Three structural questions show up across asset classes.

1) Direct vs vehicle-based claims

Many tokenized products are claims on a vehicle (fund, SPV, note issuer) that holds the underlying asset. That can be appropriate, but it shifts the investor's primary risk relationship:\n

- The investor relies on the vehicle's governance and insolvency treatment.\n
- Proof of holdings, administration, and servicing become central.\n

- Secondary transfers may require additional checks to ensure eligibility and disclosure duties remain satisfied.

This structure is common in public-chain cash equivalent products and in many private market tokenization attempts.

2) Servicing intensity as a hidden segmentation axis

Two products can be the same size and still require very different servicing work. A short-duration cash equivalent with predictable redemptions has a different servicing burden than a fund unit with frequent subscriptions and redemptions, or a private credit exposure with covenant monitoring and collections. Servicing intensity influences:\n

- how much can be made automatic,\n
- what data must be kept accurate,\n
- what exception handling is needed,\n
- and whether a market can support many small holders without overwhelming operations.

For research segmentation, servicing intensity often predicts where tokenization will move from pilots to production earlier.

3) Data dependence and verification scope

Tokenized instruments often rely on off-chain facts: NAV values, portfolio composition, reserve attestations, corporate actions, eligibility status, and regulatory restrictions. The wider the gap between "what the token shows" and "what must be true off-chain," the more the market depends on data providers, verification processes, and controls.

That is one reason why cash equivalents and government security exposures dominate public-chain RWAs (RWA.xyz [30], [32]). Their off-chain fact set is narrower and more standard than many private market assets.

Workflow walk-through: tokenized bond issuance in a regulated setting

A research chapter benefits from at least one concrete workflow description. The goal is not to claim that any jurisdiction uses the same steps, but to show where work concentrates and where risks enter.

A tokenized bond issuance, using the structures described in this chapter (digitally native, hybrid, or representation models), typically involves these phases.

Phase 1: Structuring and legal terms

The issuer and counsel specify the instrument's terms and, critically, how token state maps to legal rights:\n

- what ownership means,\n
- where the authoritative record sits,\n
- how transfers are restricted,\n
- and how court orders and corrections are handled.

If the token is a representation rather than the legal instrument itself, the terms must also define who is responsible for maintaining the link between token and underlying instrument and what happens if that link fails.

Phase 2: Compliance design and onboarding rules

Eligibility rules are translated into operational steps. In practice this often includes:\n

- identity checks and investor classification,\n
- onboarding and approval workflows,\n
- and transfer restriction mechanisms (whether enforced by intermediaries, on-chain logic, or both).

The operational test is whether eligibility rules remain enforceable across secondary transfers, not only at initial purchase.

Phase 3: Issuance and primary allocation

Token creation and allocation must match the authorized issuance amount and the allocations agreed during placement. This phase produces immediate operational questions:\n

- how allocations are confirmed,\n
- how errors are corrected,\n
- and what audit evidence exists for the allocation process.

Phase 4: Primary settlement and DvP mechanics

Settlement can be:\n

- tokenized cash settlement (stablecoins, tokenized deposits, or wholesale CBDC interfaces),\n
- or off-chain cash with on-chain transfer steps coordinated through contractual processes.

The more off-chain the cash leg is, the more "atomic settlement" becomes an operational aspiration rather than an achieved property.

Phase 5: Servicing and lifecycle events

After issuance, the bond requires coupon payments, possible calls, redemptions, and reporting. The practical test is whether lifecycle steps can be executed on schedule and corrected when exceptions occur (late data, failed transfers, custody outages). This is where confidence in tokenized markets is built or lost.

Hong Kong's repeated tokenized green bond issuance pattern is useful because it demonstrates not only initial issuance mechanics but repeated lifecycle execution over multiple batches (Treasury Bureau [17]; HKMA [16]).

Workflow walk-through: tokenized fund units and the servicing burden

Funds are a key segmentation category because their value proposition often sits in servicing rather than trading. A tokenized fund unit still has to support a full lifecycle.

A tokenized fund workflow commonly includes:

1) Subscription intake and cutoff management

Investors submit subscription requests. The system must enforce dealing cutoffs, investor eligibility, and any jurisdiction-specific constraints. Even if token transfers are used, subscription eligibility remains a controlled process in regulated settings.

2) NAV calculation and publication

NAV remains a critical data input. Tokenization can change how NAV is shared and used in servicing, but it does not remove the need for accurate valuation and controlled publication.

3) Register updates and entitlement tracking

Whether the authoritative record sits in a transfer agent system or on a ledger, the fund must maintain a correct investor register. If tokens mirror entitlements held elsewhere, reconciliation and exception management remain central.

4) Transfers and secondary movement

Transfers must respect eligibility rules. In practice, many tokenized fund designs keep transfers within a controlled perimeter, at least initially, because eligibility enforcement and reporting duties can be hard to maintain in open transfer settings.

5) Redemptions and cash delivery

Redemptions require dependable cash movement and correct accounting. The cash leg again becomes decisive: tokenized cash rails can reduce timing risk; off-chain cash can keep the process closer to existing operational patterns but may limit speed and automation.

6) Reporting, tax, and withholding

Reporting duties often determine whether the product can be distributed cross-border. Tokenization can change data flow, but it does not remove jurisdiction-specific reporting and withholding duties. That is one reason regulated intermediaries remain central in fund tokenization discussions.

MAS's Guardian Funds Framework is directly relevant because it targets the tokenized fund lifecycle and servicing functions rather than treating tokenization as a one-step issuance exercise (MAS [14]).

Incentives and business models across participants

Tokenization adoption is shaped by incentives. A participant map that ignores incentives risks treating the market as a technical system rather than a commercial and regulated system.

Issuers and asset owners adopt tokenization when it reduces operational burden, widens distribution within permitted investor categories, or improves control over servicing. They face added obligations in structure clarity, disclosure, and ongoing servicing controls.

Banks and broker-dealers adopt tokenization when it improves collateral mobility, reduces settlement delays, or improves client servicing. They are cautious when custody policies, cash rails, or data dependencies create new operational risk.

Asset managers adopt tokenization when it reduces register and servicing work and connects to distribution. They are sensitive to servicing readiness because funds live or die on correct NAV, reporting, and redemption processing.

Custodians can become gatekeepers because custody policy is often the true control layer: who can transfer, under what approvals, and under what recovery procedures. Custodians also bear reputational and operational risk if key management fails.

CSDs and post-trade utilities have strong incentives to explore tokenization when it can be offered as a service that keeps existing entitlements and investor protections consistent while adding a new operating format. The US no-action context around DTC tokenization services is best read through this lens (SEC [4]; DTCC [12]).

Venues and network operators seek order flow and usage. Their challenge is that many tokenized instruments transfer and redeem but do not generate steady exchange-style trading volume. That shifts commercial focus toward workflow transfers, collateral use, and servicing connectivity.

Data, assurance, and oracle providers gain importance as tokenized products rely on verified off-chain facts. Their incentives can create concentration risk if a small number of providers become default sources for NAV, reserve attestations, or corporate action triggers.

Measuring concentration and dependence in tokenized markets

This chapter lists concentration dimensions. For research use, it also helps to state how concentration can be measured, even when full data is not available.

Asset concentration measurement can use market value shares by product type and by issuer. Public-chain dashboards such as RWA.xyz provide one view for on-chain products (RWA.xyz [30], [32]), though broader represented value measures require careful interpretation.

Network concentration measurement can track which base layers carry the majority of tokenized value and transaction activity and whether activity depends on a small set of node operators or client software stacks.

Settlement rail concentration measurement can track which settlement assets are actually used for DvP and collateral movement and how often operations fall back to off-chain cash and reconciliation.

Service provider concentration measurement can track custody stack usage (dominant custody technology and providers), dominant identity and permissioning tooling, dominant audit and assurance providers, and dominant data feed sources for NAV and pricing.

Market infrastructure concentration measurement can track whether tokenization routes are consolidating around a few utilities and their approved networks (a central question raised by US post-trade utility signals (SEC [4]; DTCC [12], [13])).

Even where numeric concentration indices are not available, dependency mapping remains useful. A dependency map that identifies single points of failure (cash rails, custody policy engines, data feeds, upgrade governance) can be more informative than an asset issuance league table.

Change control and operational continuity as first-order risk factors

Tokenization shifts some risk from human process to system change control. In conventional market infrastructure, change is governed by defined release cycles, approval structures, and incident playbooks. Tokenized systems must provide an equivalent discipline.

Research mapping should therefore note, for each operating model:\n

- who can change code or policy rules,\n
- how changes are tested and approved,\n
- what rollback or correction processes exist,\n

- how outages are handled,\n
- and what evidence is kept for supervisors and auditors.

This is not a technical footnote. Many tokenized market failures, if they occur, are likely to be operational: poor change control, unclear recovery steps, weak exception handling, or unclear legal authority to correct a broken state.

Legal Enforceability and Regulatory Comparatives

Why legal enforceability limits scale in tokenization

Tokenization reaches institutional scale only when market participants can answer, with confidence, a small set of legal questions across the whole lifecycle: what right the token represents, who holds that right, how it moves from one party to another, what counts as final settlement, what happens if an intermediary fails, and what rules apply when parties sit in different jurisdictions.

These questions sound basic because they are. They are also where many tokenization programs slow down. The technical ability to issue and move tokens is not the hard part.

The hard part is making sure that the token movement has the legal effect market participants assume it has.

Regulators have mostly converged on a practical framing: tokenization can resemble familiar capital markets activity, but legal uncertainty, operational weaknesses, and fragmented infrastructure can change how familiar risks appear. IOSCO's 2025 work is explicit that legal uncertainty can be a material constraint and that outcomes depend on domestic legal frameworks and context (see Reuters coverage of IOSCO's risk analysis: https://www.reuters.com/sustainability/boards-policy-regulation/global-securities-watchdog-says-tokenization-creates-new-risks-2025-11-11/?utm_source=chatgpt.com).

This section is written as a research backbone. In a full chapter, you would expand each subsection with jurisdiction-specific case studies, instrument-level drafting examples, and the regulator notices and statutory provisions that drive the conclusions.

The enforceability problem set

A tokenized instrument is rarely "just a token." It is usually a stack of relationships: issuer and holder, holder and custodian, venue and participant, participant and settlement agent, and often a separate administrator that maintains the link between token state and off-ledger records. Enforceability hinges on how that stack is drafted and which law the stack sits under.

A disciplined way to write enforceability analysis is to separate three things that often get blurred:

- The technical fact of a ledger state change.
- The contractual meaning the parties assign to that state change.
- The legal meaning a court or regulator will assign to it under the relevant statute and private law rules.

Tokenization can reduce some operational steps, but it can also add new dependency points: custody policy engines, admin keys, data feeds, and platform operators whose failure can stop transfers or trigger wrong lifecycle events. A market can tolerate those dependencies only if rights and remedies are clear.

What follows is a set of core questions. A tokenization program that cannot answer them cannot grow beyond small, relationship-based pilots.

What the token is, as a matter of law

The first enforceability question is blunt: what is the token in legal terms?

A token can be several different things. The enforceability analysis changes depending on which one you are using.

A security in a token wrapper

In many jurisdictions, a tokenized security is treated as a security. The legal perimeter and conduct rules follow the familiar regime. The token is a format, not a new category of asset.

This approach is visible in Hong Kong's posture, where tokenization is treated as an added layer on top of traditional securities regulation, paired with extra safeguards and operational expectations for intermediaries. It is also visible in US commentary that the security status of an instrument does not change because a token is used in issuance, transfer, or recordkeeping.

For enforceability, the main question in a "security in a wrapper" model is whether the wrapper changes the investor's actual right. If the investor's enforceable right still depends on an off-ledger register and an intermediary's performance, then a token movement is not, by itself, a legal transfer. It may be evidence of a transfer request, or it may be part of the settlement process, but the legally effective step remains elsewhere.

A paper that treats "tokenized securities" as a single category will miss these distinctions. Two products can both be "tokenized securities" while having very different title mechanics and insolvency outcomes.

A crypto-asset outside the financial instrument perimeter

In the EU, MiCA targets crypto-assets that are not already covered by existing financial services law, with specific treatment of asset-referenced tokens and e-money tokens. MiCA applies from 30 December 2024, with stablecoin-related titles applying earlier from 30 June 2024 (EUR-Lex: https://eur-lex.europa.eu/EN/legal-content/summary/european-crypto-assets-regulation-mica.html?utm_source=chatgpt.com).

This perimeter matters to tokenization even when the end goal is tokenized securities. Settlement rails, custody providers, exchanges, and wallet services that touch tokenized workflows may sit partly inside MiCA depending on what instruments are used for payment and what services are offered.

From an enforceability view, a MiCA-perimeter crypto-asset is not automatically a financial instrument. That affects disclosure, custody expectations, and what legal remedies look like when things go wrong. It also shapes how courts and regulators think about investor understanding: whether a buyer is expected to know they are holding an on-ledger object with its own risk profile, not a dematerialized security governed by classic market infrastructure rules.

A ledger-native security created by statute

Some jurisdictions have moved toward explicit statutory recognition of ledger-based securities. Switzerland's DLT reforms are often cited here. The point is not that a token is used; the point is that the law creates a recognized way to issue rights that are constituted by ledger entry, and then licenses venues tailored to those rights.

In this model, the ledger entry can be title, not merely evidence. That shifts many enforceability questions from "does this representation track the off-ledger truth?" to "how does the law govern ledger truth, and how are exceptions handled?"

The design choice is demanding. If the ledger is title, the market must specify processes for court orders, sanctions actions, error correction, and system outages. In practice, that pushes toward regulated market infrastructure and defined operator responsibilities.

A trade or payment instrument expressed as an electronic transferable record

Tokenization is often discussed as a capital markets topic, but enforceability questions overlap with trade and payments law. Under UNCITRAL's Model Law on Electronic Transferable Records (MLETR), the goal is functional equivalence: electronic records should be capable of doing what paper negotiable instruments do, including enabling possession-like control, transfer, and, where adopted, cross-border recognition.

MLETR is technology-neutral. It can be implemented using registries, token systems, or distributed ledgers. The enforceability shift is that the law focuses on whether the system supports exclusive control and prevents duplicate transfer, rather than whether it is "blockchain."

This matters because some tokenization projects—especially those tied to trade finance, bills of lading, warehouse receipts, or negotiable notes—depend on possession-like logic more than on securities law. A research chapter should treat these as a distinct category with its own legal tests.

A property object under private law, even when it is not a security

Some legal systems have moved toward clearer recognition that certain digital assets can be treated as property under private law. England and Wales, for example, moved toward statutory clarity by confirming a third category of personal property capable of accommodating certain digital assets.

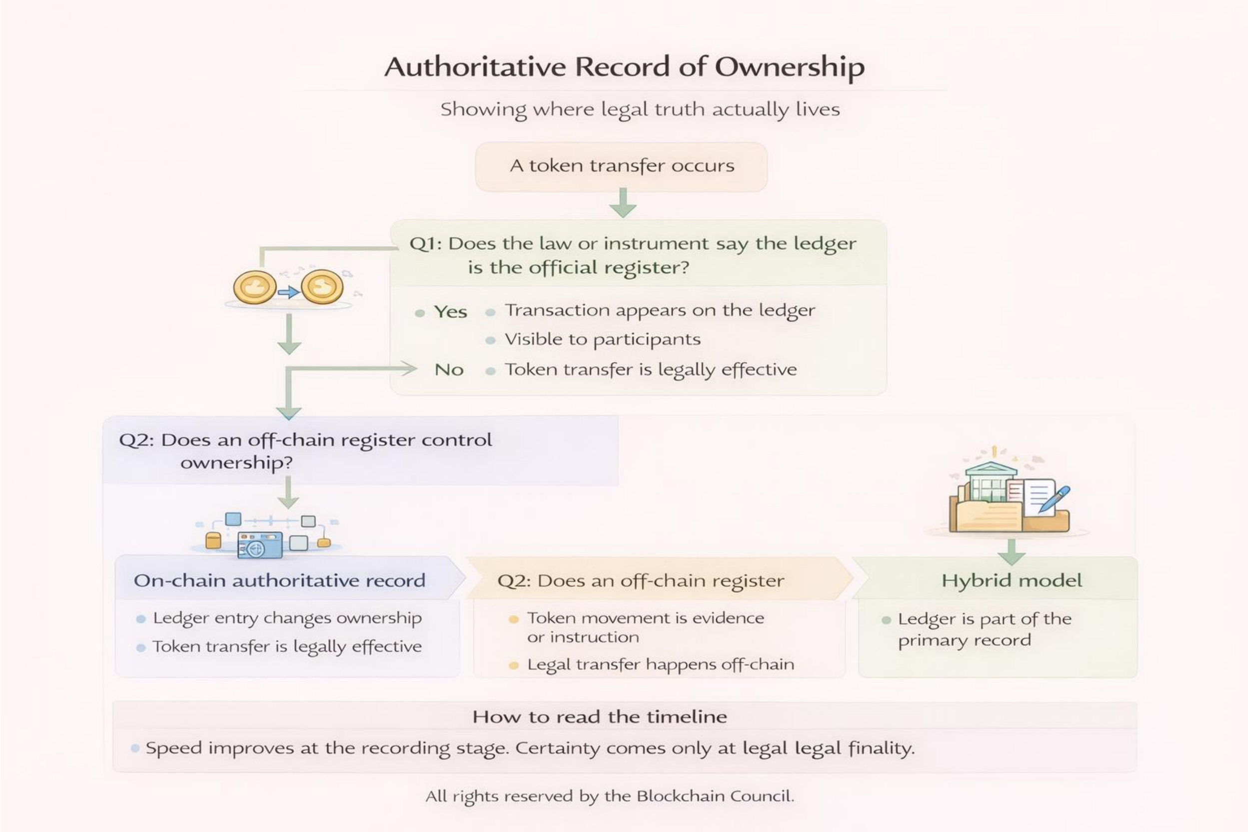
This matters because a market does not only need securities law to function. It needs property and private law rules that answer: can the asset be owned, can it be traced, can it be recovered, can a security right attach, and can a buyer take free of earlier claims under certain conditions?

Research implication

A research paper should avoid treating “tokenized assets” as one category. Every enforceability statement depends on which legal perimeter applies. Transfer rules, custody obligations, collateral treatment, and insolvency outcomes can differ sharply even when the ledger mechanics look the same.

Where the authoritative record sits, and what makes a transfer legally effective

After classification, the next question is where the authoritative record of ownership and entitlements lives, and what event counts as title transfer.



Two broad models appear across markets.

On-ledger authoritative record

In an on-ledger authoritative model, the ledger entry is the definitive record of ownership. Title transfer is tied to ledger state change, under a statute or regulated regime that recognizes that ledger state change as legally effective.

This model tends to require one of the following:

- A statutory form of ledger-based security or property right.

- A regulated market infrastructure framework that treats a DLT record as the official record for the instrument.

The advantage is conceptual clarity: the transfer that the market sees is the transfer the law recognizes. The trade-off is governance load. If the ledger is the book of record, then legal systems must answer how reversals work, what happens when keys are lost, and how public policy actions (sanctions, court orders) are carried out.

Off-ledger authoritative record with on-ledger representation

In an off-ledger authoritative model, the token is evidence or a synchronized representation, but the definitive register remains with a transfer agent, CSD, issuer register, or similar arrangement.

This model is common in markets that want to keep existing investor protection and settlement finality structures intact. It can also be a bridge when private law does not yet treat a ledger entry as title.

The enforceability risk is that market participants can confuse operational visibility with legal effect. A token movement that looks final on a ledger may still be conditional under the legal register rules. In disputes, the off-ledger record often wins.

IOSCO has noted that tokenization structures vary, including whether blockchain records are definitive or serve as proof or backup, and whether intermediaries can correct records depending on design (see Reuters coverage of IOSCO: https://www.reuters.com/sustainability/boards-policy-regulation/global-securities-watchdog-says-tokenization-creates-new-risks-2025-11-11/?utm_source=chatgpt.com).

Research implication

Enforceability analysis must document where the "truth" lives and what legal mechanism makes a transfer effective, not just what is operationally visible. A reader should be able to answer, for a given instrument:

- What system a court will treat as the book of record.
- What step creates legal transfer.
- Whether the on-ledger state is title, evidence of title, or a transfer instruction.

Possession, control, and how ownership is demonstrated

The next question is the legal analogue to possession. This is the pivot point for both ownership and secured transactions.

Markets have converged on control-based legal tests in several contexts, but the tests are not identical across jurisdictions.

Exclusive control and singularity in electronic transferable records

Electronic transferable record regimes aim to reproduce the role that possession plays for paper negotiable instruments. The law is not impressed by the fact that a file exists. It is impressed by whether the system makes it possible to identify a single authoritative record and to show that one party has exclusive control.

The UK's Electronic Trade Documents Act explains that an electronic trade document must be capable of being transferred and possessed in a way that prevents duplicate transfer. The Act's logic is divestibility and exclusive control: a transfer must divest the transferor of control so the same record cannot be "spent" twice.

Singapore's Electronic Transactions (Amendment) Act 2021 adopts electronic transferable records and includes cross-border validity concepts, supporting enforceability where the record is issued or used outside Singapore. UNCITRAL's MLETR has the same aim: enable legal use of electronic transferable records domestically and across borders.

In tokenization research, these regimes are useful because they show a legal approach to the double-spend problem that does not depend on any single technology. A system can satisfy the legal test using a registry, a permissioned ledger, or another design, so long as the legal requirements are met.

Control of a controllable electronic record under updated commercial law

In the US, the 2022 UCC amendments introduce a new Article 12 framework for controllable electronic records, and related changes to Article 9 for secured transactions. The direction is to tie priority and perfection concepts to "control" rather than to possession of a physical object.

New York's enactment with an effective date in 2026 is notable because New York law often governs major capital markets documentation. For market practice, that means the control concept is likely to show up in drafting and enforcement logic for secured financing over tokenized assets.

Control is not the same as holding a private key

A practical research warning belongs here: legal control does not always map one-to-one with private key possession.

Institutional custody often splits control across:

- a custodian's key management system,
- a policy engine that enforces approvals,
- multi-party authorization (for example, multiple signers), and

- operational and compliance gates.

A party can have legal control without ever touching a private key if the legal and contractual structure makes the custodian an agent holding the asset on the party's behalf and limits the custodian's ability to move it without authorization.

Conversely, a party can hold a private key but lack legal control if the key is held in breach of a custody agreement or if the asset is subject to a legal restraint.

This is why research writing should treat "control" as a legal and institutional standard, not as a technical shorthand.

Research implication

When writing enforceability, define control precisely:

- What statute or private law rule defines control for the asset type.
- What evidence proves control (ledger state, custody attestation, control agreement).
- How control is lost or transferred.
- How control is shared or split across parties.

Without this, secured lending, collateral reuse, and bankruptcy analysis cannot be done with discipline.

Settlement finality and legal recognition of irrevocability

Tokenization discussions often focus on atomic settlement. Enforceability requires clarity on a different point: when does a transfer become irrevocable as a matter of law, and what protects that finality.

Finality is both legal and operational. The same ledger event can be technically final under network rules and still be reversible in law, depending on the framework.

A careful analysis should address:

- When a transfer becomes irrevocable as a matter of law.
- Whether settlement finality protections attach to the DLT system and its participants.
- How errors, forks, reversals, and outages are handled.

Regulated market infrastructure regimes

In the EU, the DLT Pilot Regime is designed to allow testing of DLT market infrastructures while preserving investor protection and market integrity (EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022R0858&utm_source=chatgpt.com). The regime is not only about letting tokens move. It is about testing trading and settlement in a setting where liability chains and operational standards are set in advance.

A research chapter should pay attention to liability allocation. If losses arise from operational failure, who bears them? How does a participant seek remedy? These are the practical questions that determine whether institutions treat the settlement system as safe enough for meaningful volume.

In the UK, the Digital Securities Sandbox is a live financial market infrastructure sandbox with temporarily modified legal and regulatory requirements to test issuance, trading, and settlement under supervision (Bank of England: https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox?utm_source=chatgpt.com; FCA: https://www.fca.org.uk/firms/innovation/digital-securities-sandbox?utm_source=chatgpt.com).

Network events are not legal events

In public networks, a transaction may be "final" in a practical sense after enough confirmations. But legal finality is a separate question. If a court orders a reversal, or if fraud is proven, or if an intermediary was not authorized to transfer, the law may treat the transfer as voidable or void even if the ledger will not roll back.

That tension is not a flaw of tokenization; it is a mismatch between technical irreversibility and legal remedies. Institutions will not accept technical irreversibility as a substitute for legal finality protections unless the system rules and the legal regime make outcomes predictable.

Research implication

Finality analysis should always be tied to the legal framework under which the venue or settlement system operates, not to the consensus method of a network. A reader should be able to tell:

- what rule makes settlement final,
- what exceptions exist,
- what remedies apply when something goes wrong,
- and who bears losses when failures are operational rather than market-driven.

Insolvency, client assets, and the difference between property claims and contract claims

Insolvency is where tokenization wrapper designs often fail. Many tokenization products work during normal operations because nobody tests the hard edge cases. Insolvency forces the question: whose asset is it, and what happens when an intermediary collapses.

A research analysis should cover at least:

- Whether client assets are segregated and bankruptcy-remote.
- Whether the customer's claim is a property-based claim (stronger) or merely contractual (weaker).
- What rights a custodian has to lend, pledge, or otherwise use assets.
- Whether a secured creditor's interest can be created, perfected, and enforced quickly.

Custody structures and client asset segregation

Custody in tokenized markets can be arranged as:

- direct holding by the investor (self-custody),
- holding through a custodian as agent or trustee,
- holding through an omnibus structure where assets are pooled,
- holding through layered custodians and sub-custodians.

Each structure implies different outcomes in insolvency. A client that has a clear property right held on trust or in a segregated account has stronger prospects than a client whose position is only a claim against an intermediary.

Tokenization can obscure these differences because the ledger may show a token balance without telling the reader whether that balance is held on trust, held in an omnibus arrangement, or represents only a contractual IOU.

Security interests and collateral enforceability

Collateral use cases are a driver of tokenization programs. Collateral only works if a security right can attach, be perfected, and be enforced without delay. For this, markets need a legal rule that maps to the way the asset is controlled.

UNIDROIT's Principles on Digital Assets and Private Law provide a comparative template here. They organize the problem set around transfers, custody relationships, security rights, priority rules, and insolvency, and they discuss concepts such as an innocent acquirer taking free of prior claims and control as a basis for effectiveness and priority.

Even where the Principles are not adopted as domestic law, they are useful as a benchmark. They force the researcher to specify:

- when a buyer takes free of earlier claims,
- when and how a security right becomes effective against third parties,
- how priority disputes are resolved,
- and what happens on insolvency of an intermediary.

Research implication

When you write about client protection in tokenized markets, avoid vague assurances. Tie the analysis to:

- the custody contract,
- the segregation method,
- the legal mechanism that makes the client's right a property-based right rather than merely a debt,
- and the secured transactions rules that govern perfection and priority.

If the token is only a representation of an off-ledger entitlement, your analysis must also cover the off-ledger custodian and administrator arrangements, because that is where the client's enforceable right will live.

The code layer, contract law, and what happens when software misbehaves

A tokenized instrument usually has at least two layers:

- the legal terms (offering document, instrument terms, subscription agreement, custody agreement, venue rulebook), and
- the on-ledger logic that moves tokens and carries out lifecycle events.

The second layer does not replace the first. It is a performance mechanism. Enforceability depends on how the two layers fit.

Governing law, forum, and distributed participation

Tokenized systems often have participants in multiple countries, even when the issuer is local. That creates friction in choosing governing law and forum.

A researcher should ask:

- Which law governs the instrument terms.
- Which law governs ownership claims in the token or underlying right.
- Which law governs the custody relationship.
- Which law governs the venue rules and dispute resolution.

These can be different. A bond can be governed by one law, the custody agreement by another, and the venue rulebook by a third. Tokenization makes this more visible because transfers can happen at any time and across borders.

What the code is, legally

A second question is how the system treats smart contract code:

- Is the code an operative performance tool that executes the legal terms?
- Is it merely an evidentiary record of what happened?
- Is it part of the contract itself?

Markets vary. Some systems treat code as a tool under an agreement that still governs. Others try to make code the definitive statement of the parties' rights.

IOSCO has flagged that software bugs and operational weaknesses can be hard to rectify and that risks can show up differently depending on architecture (see Reuters coverage of IOSCO: https://www.reuters.com/sustainability/boards-policy-regulation/global-securities-watchdog-says-tokenization-creates-new-risks-2025-11-11/?utm_source=chatgpt.com).

When code behaves unexpectedly

Enforceability writing should cover the hard cases:

- The code executes a transfer that was not intended.
- The code fails to execute a coupon or redemption.
- The code enforces a restriction incorrectly.

- A data feed gives wrong input and triggers actions.

The legal questions are practical:

- Can the action be reversed?
- Who has the authority to pause or patch?
- What liability applies?
- What remedies does the harmed party have?

A tokenization design that cannot answer these questions in advance will struggle to win institutional participation.

Upgradeability, admin keys, and accountability

Many tokenization systems rely on some form of upgrade or administrative control. This is often necessary for fixes and compliance actions. It also creates a governance problem: who can change the rules of the system.

A useful way to write this part is as a governance triad:

- Who can change the code.
- Under what conditions.
- With what liability if something goes wrong.

Then compare two common operating styles.

Permissioned venues and controlled upgrades

In permissioned systems and regulated venues, the operator is known, participation is controlled, and upgrades can be subject to a formal change process. That supports accountability: the operator can be supervised and can be held responsible for failures.

The trade-off is concentration. Participants must accept that a small number of operators and service providers have power over the system. The governance process must therefore be well specified and auditable.

Public networks and off-ledger enforcement

In public networks, upgrade and control can exist at several layers:

- the base protocol,
- the smart contract,
- the administrator controls embedded in the contract,
- and the practical influence of large service providers.

Even if the code has no admin keys, participants can still face protocol upgrades they did not choose.

Enforcement of accountability often sits off-ledger. A harmed party will usually rely on contract terms, claims against identifiable service providers, or regulatory action against intermediaries.

Research implication

Do not treat admin control as a purely technical topic. It is a legal accountability topic. A good research subsection links governance rights, duty and liability, audit and disclosure, and the way the system handles emergency actions.

Mapping the regulatory perimeter

A research chapter should separate three regulatory planes. Mixing them produces confusion.

Financial instrument regulation

This plane covers securities, funds, derivatives, and market infrastructure rules.

Hong Kong's posture is a clear example: tokenized securities are treated as traditional securities with an added token layer, and existing regimes apply, paired with extra safeguards and operational expectations around recordkeeping, market readiness, and intermediary conduct.

In the EU, the DLT Pilot Regime covers issuance, recording, transfer, and storage of tokenized financial instruments within a pilot framework (EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022R0858&utm_source=chatgpt.com).

Crypto-asset-specific regulation

This plane targets crypto-assets that sit outside classic financial instrument regimes.

MiCA applies from 30 December 2024, with stablecoin-related titles applying since 30 June 2024, setting a harmonized EU framework for issuance and services for in-scope crypto-assets (EUR-Lex: https://eur-lex.europa.eu/EN/legal-content/summary/european-crypto-assets-regulation-mica.html?utm_source=chatgpt.com).

This plane matters to tokenization because settlement tokens, custody and exchange services, and some token representations may sit here even when the economic exposure is tied to a traditional asset.

Private law foundations

This plane makes ownership, custody, and collateral enforceable. It includes property law, commercial law concepts for control, secured transactions rules, and insolvency.

England and Wales' property law modernization is relevant here: recognition of a third category of personal property aims to provide a clearer base for certain digital assets.

UNIDROIT Principles provide a harmonized private law template for custody, transfers, security rights, priority, and conflict-of-laws logic structured around control.

UNCITRAL's MLETR provides a technology-neutral framework supporting cross-border use of electronic transferable records.

Research implication

Tokenization succeeds when all three planes fit together. Many pilots work technically but stall because private law is unclear or because financial instrument rules do not yet allow an end-to-end market infrastructure to operate on a DLT stack.

Comparative jurisdiction profiles

The subsections below are written to be expanded. Each can become 10–20 pages in a full paper by adding statutory text, regulator notices, and instrument examples.

European Union

The EU design splits between tokenized financial instruments and crypto-assets.

DLT Pilot Regime (Regulation (EU) 2022/858) creates a controlled pathway for DLT market infrastructures to test trading and settlement of DLT financial instruments while maintaining investor protection and market integrity (EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022R0858&utm_source=chatgpt.com).

MiCA (Regulation (EU) 2023/1114) harmonizes rules for crypto-assets not already regulated under existing financial services law, with stablecoin-related titles applying from 30 June 2024 and the wider regime from 30 December 2024 (EUR-Lex: https://eur-lex.europa.eu/EN/legal-content/summary/european-crypto-assets-regulation-mica.html?utm_source=chatgpt.com).

Enforceability themes to cover include the relationship between DLT financial instruments under the Pilot and traditional dematerialized securities concepts, liability allocation between operators and intermediaries, and treatment of settlement assets in pilot contexts.

United Kingdom

The UK combines an infrastructure sandbox with private law modernization.

The Digital Securities Sandbox is set out by the Bank of England and FCA as an FMI sandbox to test issuance, trading, and settlement with temporary modifications to requirements (Bank of England: https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox?utm_source=chatgpt.com; FCA: https://www.fca.org.uk/firms/innovation/digital-securities-sandbox?utm_source=chatgpt.com).

The Property (Digital Assets etc) Act 2025 establishes a third category of personal property aimed at clarifying the legal basis for certain digital assets. The Electronic Trade Documents Act 2023 enables electronic trade documents to have equivalent legal effect to paper, relying on exclusive control and divestibility logic.

Enforceability themes to cover include how DSS interacts with settlement finality protections, how the new property category affects custody disputes and remedies, and how ETDA control logic can inform tokenized instrument design beyond trade.

Switzerland

Switzerland's DLT reforms are often framed as a legal certainty approach: create a statutory form for ledger-based securities and license venues tailored to those instruments.

Enforceability themes include how registration agreements create a constitutive link between the right and ledger entry, and how insolvency and private international law adaptations affect cross-border participants.

United States

The US combines a securities law perimeter with modernized commercial law.

Regulatory statements and guidance focus on custody and risk controls for crypto-asset securities held by intermediaries. The 2022 UCC amendments introduce Article 12 on controllable electronic records and related Article 9 changes for secured transactions. New York's enactment effective June 3, 2026 is notable given market practice.

Enforceability themes include how legal control interacts with institutional custody, how security rights are perfected and prioritized under updated UCC rules, and how third-party wrapper tokenization efforts raise questions about rights mapping.

Singapore

Singapore's Electronic Transactions Act amendments in 2021 adopt MLETR-aligned concepts for electronic transferable records, including cross-border validity ideas.

MAS Project Guardian and published frameworks provide policy and market design context for tokenized finance, even where enforceability remains instrument-specific.

Enforceability themes include how electronic transferable record logic can underpin possession-like claims, how fund tokenization interacts with transfer restrictions and record integrity, and how settlement asset design choices affect finality and risk.

Hong Kong

Hong Kong treats tokenization as a wrapper on top of existing securities rules, with added safeguards and operational expectations for intermediaries.

Themes include always-available token records versus market readiness for pricing and liquidity, enforcement of transfer restrictions, and cross-border participation effects.

Abu Dhabi Global Market and other MLETR adopters

Treating MLETR adoption as a legal readiness indicator can help segment cross-border enforceability for tokenized trade finance and negotiable instrument workflows.

Themes include how electronic transferable record rules support tokenized trade flows and how conflict-of-laws rules support cross-border recognition.

Conflict of laws and cross-border recognition

Even when all participants are institutions, tokenization can involve an issuer in one country, governing law in another, a venue or operator in a third, and investors and custodians across many legal systems.

Classic connecting factors—asset location, debtor location, intermediary location, place of register—are hard to apply to digital assets. Control-based connecting factors offer an alternative benchmark, consistent with UNIDROIT and the US UCC direction.

A practical research structure is to explain why classic connecting factors struggle, then show how control-based ideas can narrow uncertainty, then link that back to custody arrangements that split control across firms.

An enforceability checklist for tokenized instruments

Instrument and register documentation should identify classification and applicable regime, specify where the authoritative record is kept, define the event that creates legal transfer, and set out correction and dispute handling.

Custody and control documentation should define who can initiate transfers, how approvals work, what counts as control under the relevant law, how liability is allocated for key compromise and operational error, and how segregation and asset-use rights are handled.

Venue and settlement documentation should define finality rules, outage fallback processes, and accountability and reporting expectations.

Cross-border documentation should set governing law and forum, state choice-of-law logic for ownership and security rights, and set out recognition approaches where electronic transferable record regimes apply.

How this chapter ties back to a broader tokenization paper

Tokenization scale is not only a technology problem. It is a coordination problem across securities law, crypto-asset regimes, and private law foundations.

Jurisdictions are taking different routes: statutory forms for ledger-based securities (Switzerland), FMI sandboxes (UK and EU Pilot pathways), crypto-asset perimeter rules that shape settlement tokens and provider licensing (EU MiCA), commercial law modernization (US UCC updates), and electronic transferable record modernization that supports cross-border recognition (MLETR adopters).

Harmonization tools such as the UNIDROIT Principles provide a common vocabulary even where local law differs. That vocabulary—control, transfer, custody relationship, security right, priority, and insolvency—helps convert tokenization from a set of experiments into a market that institutions can assess and price.

Conclusion

Asset tokenization is often sold as a single idea: put assets "on-chain," and markets become faster, cheaper, and more open. This paper reaches a different conclusion. Tokenization is not one thing. It is a bundle of design choices that can produce very different legal rights, operational pathways, and failure modes. The same token format can represent direct ownership, beneficial ownership through an intermediary, or a simple contract claim against an issuer. The same "tokenized bond" can settle against off-chain bank money, a regulated stablecoin, a tokenized bank liability, or central bank money. The same ledger can be treated as the book of record in one jurisdiction and as a mirror record in another. Without naming those choices, most debates about tokenization collapse into slogans.

The first contribution of the study is to separate token format from legal right. A token is a record on a platform. A tokenized product is the full arrangement that gives that record meaning: the instrument terms, the register, the custody relationship, the settlement process, the servicing stack, the rules for exceptions, and the set of parties who can intervene. Institutional markets do not scale on technical capability alone. They scale when rights are plain, evidence is clear, settlement is recognized as final, and remedies are predictable under stress. Tokenization changes how those conditions can be met, but it does not remove the need for them.

The second contribution is a classification structure built around claims and control. Many products described as "tokenized" are not built on the idea that a ledger transfer is a legal transfer. They are built on the idea that a ledger transfer is a convenient representation of a legal transfer that happens elsewhere. Some designs are native, where the ledger is intended to be the controlling record; others are non-native, where the controlling record remains with a registrar, transfer agent, or depository, and the token is a synchronized representation or access gate. Neither posture is inherently superior. Each shifts risk, cost, and governance requirements. But the distinction is decisive for interpretation. A paper that treats both as the same thing will either overstate what tokenization changes or miss what it leaves untouched.

When tokenized markets are viewed through this lens, the emerging global landscape becomes easier to explain. Activity is not spread evenly across asset classes or use cases. It clusters where the product structure is simple, the cash leg is workable, and the operational payoff is immediate. Tokenized cash equivalents and government securities-style exposures have grown in public-chain settings because they meet clear demand: yield, predictable redemption, and collateral utility inside always-available markets. Tokenized fund interests attract attention because funds are operationally heavy:

subscriptions, redemptions, valuation points, reporting, and transfer restrictions create recurring work that lends itself to better tooling and tighter reconciliation. Collateral workflows show traction because they target a narrow but costly set of pain points: margin calls, collateral substitution, settlement fails, and audit trails. By contrast, broad secondary trading of tokenized corporate securities remains limited because the barriers are not mainly technical. They are structural: fragmented venues, restricted transfer rules, custody readiness gaps, and the simple fact that liquidity forms where market makers can hedge and settle with confidence.

This pattern supports a broader point. Tokenization is most credible when it is treated as market plumbing work rather than as product novelty. The early value is rarely "new assets." It is cleaner processes around familiar assets: how entitlements are recorded, how corporate actions are handled, how collateral moves, how settlement instructions are matched, and how exceptions are resolved. Where tokenization is framed as a replacement of existing systems in one leap, it tends to stall. Where it is framed as a controlled redesign of narrow functions, it tends to advance.

The paper also shows why the cash leg sets the ceiling. Tokenization of the asset leg without a workable settlement asset often leaves the system stuck in a hybrid that looks modern but still depends on conventional money movement and manual reconciliation. That hybrid can still be useful—especially in issuance and servicing—but it will not deliver the strongest claims made for token-based settlement, such as delivery-versus-payment in one step or intraday collateral motion with fewer failure points. This is why many jurisdictions and industry groups have spent as much time on tokenized money, stablecoin regimes, tokenized bank liabilities, and wholesale central bank settlement experiments as they have on tokenized securities themselves. Settlement is where credit risk, liquidity risk, and legal finality meet. If settlement cannot be made predictable under stress, tokenization remains bounded to small volumes and narrow participant sets.

At the same time, settlement design introduces its own dependencies. Stablecoin rails can become single points of failure if market liquidity relies on one or two issuers, or if redemption becomes contested during market stress, or if regulatory action freezes flows at the worst moment. Tokenized bank liabilities can reduce some of those risks by keeping settlement inside supervised banking perimeters, but they introduce bank balance sheet and operational concentration issues. Wholesale central bank settlement can offer strong finality, but it requires careful integration with market infrastructure and clear rules on access. The conclusion is not that one settlement form is the answer. The conclusion is that settlement design is not a side topic. It is a core determinant of whether tokenization becomes routine or remains episodic.

The strongest limiting factor identified in the study is legal enforceability. Institutions need to know what a token holder owns, how that ownership is proven, and what happens in insolvency. These questions are not academic. They decide whether a tokenized position is treated as a property right or as a contract claim, whether it can be used as collateral with clear priority, and whether it survives the failure of an intermediary. This is why private law foundations—control, possession analogues, electronic transferable records, priority rules, and conflict-of-laws logic—matter as much as securities regulation. A jurisdiction can permit tokenized issuance in principle and still block scale in practice if courts and insolvency rules do not treat ledger records as meaningful, or if custody and segregation rules do not map cleanly onto token-based control arrangements.

The enforceability lens also clarifies why sandboxes and pilot regimes matter. They are not simply "innovation programs." They are evidence-generation tools designed to test how rights, records, and settlement behave in live conditions. They force participants to specify who is responsible for errors, how reversals occur, what happens when keys are lost, and how court orders are carried out. Those are the points that determine whether tokenization can move beyond controlled demos. If a sandbox does not demand clarity on those issues, it becomes a marketing stage. If it does, it becomes a bridge between technical feasibility and legal certainty.

A second structural finding is that tokenization changes intermediation rather than removing it. The core intermediaries—custodians, registries, depositories, transfer agents, settlement services, and venues—remain central, even when tokens are used. What changes is where trust concentrates. Tokenization can reduce some reconciliation work, but it adds new service dependencies: key management systems, policy engines, data feeds that trigger lifecycle events, platform operators with upgrade powers, and network operators who govern the runtime environment. These are not peripheral vendors. In practice they become part of the market's core infrastructure. That shifts operational risk and concentration risk into places that may sit outside traditional oversight frameworks unless regulation and supervision adapt.

This shift is visible in how markets are forming around infrastructure hubs. Where central market utilities extend tokenization into existing custody and post-trade rails, adoption can be easier because the distribution network already exists. Participants can interact with tokenized representations without rewriting their entire operating model. But this also increases dependency on a small set of approved networks and operators. In the long run, tokenization may not create a flat market of interchangeable platforms. It may create a layered market where a few utilities and a few settlement rails become gatekeepers. That structure can bring stability, but it must be understood as a trade: easier adoption in exchange for tighter concentration.

Cross-border friction remains a defining constraint. Tokenized instruments do not stay inside borders just because securities law is domestic. Participants, custodians, and service providers often span jurisdictions, even when issuance is local. The seams that matter most are not national borders on a map; they are differences in investor eligibility rules, transfer restriction enforcement, recognition of ledger records as ownership records, treatment of settlement assets, and tax characterization of token transfers and fractional interests. A token transfer that is recognized as effective in one jurisdiction may be treated as only evidence in another. A security interest perfected through control in one legal system may not map cleanly onto another system's priority rules. A tokenized trade document recognized under an electronic transferable record regime in one jurisdiction may face uncertainty when presented elsewhere. These seams do not make tokenization impossible, but they shape where scale appears first: in controlled participant networks, in professional investor channels, and in structures that rely on well-understood governing law choices.

A key practical implication of this research is that tokenization outcomes must be measured, not assumed. The paper proposes measurable indicators for each segment—issuance, trading, servicing, and collateral—because claims of speed and cost reduction mean nothing without a baseline and a method. In issuance, the relevant measures include time from term finalization to issuance, completion time for primary settlement, exception rates, and cost per onboarded investor. In trading, the measures include spreads and depth relative to comparable instruments, settlement failure rates, availability of market maker liquidity under compliance gating, and fragmentation across venues. In servicing, the measures include processing time for corporate actions, workload reduction in reconciliation, audit trail completeness, and incident resolution time. In collateral, the measures include time to meet margin calls, collateral velocity within permitted bounds, dispute reduction, and performance under stress. These measures can be collected without requiring perfect transparency into every system. What is required is that tokenization initiatives define the metrics in advance and report them in a comparable way.

The importance of measurement is not merely academic. Tokenization is often justified as a modernization investment. Modernization projects fail when they do not define success criteria. They also fail when they measure only what is easy—transaction speed on a platform—rather than what matters—legal finality, exception handling, and cost of operations across the full lifecycle. If tokenization does not reduce exception handling costs, shorten dispute resolution, or reduce settlement fails in real conditions, then the benefit case weakens, regardless of how elegant the platform appears.

A second implication is that tokenization design must start from the claim model. Whether a product is Model A (direct ownership tied to the token ledger), Model B (beneficial ownership through an intermediary), or Model C (contract claim against an issuer or SPV) determines almost every downstream question. It determines what must be disclosed, what must be supervised, what evidence proves ownership, what happens in insolvency, and whether collateral rights can be made clean. Many market problems arise when a product is marketed as Model A while operating as Model B or C. That mismatch is not a technical issue; it is a disclosure and investor protection issue. It also explains why some regulators stress clarity about whether a token holder holds the underlying asset or a representation. Without that clarity, trading liquidity stays thin because counterparties do not know what they are buying.

The conclusion from this is straightforward: tokenization work should be written as rights mapping work. Every tokenized product should state, in plain terms:

- what the holder owns or is owed,
- who owes it,
- what record controls in a dispute,
- what event makes transfer legally effective,
- what happens when a transfer is impermissible or mistaken,
- how settlement becomes final,
- how client assets are segregated,
- and what happens in insolvency.

If those statements cannot be made plainly, the product is not ready for scale.

For policymakers and supervisors, the paper's findings point to a set of priorities that are more concrete than "support tokenization." One priority is to clarify the status of ledger records and the conditions under which they can serve as ownership records. Another is to clarify custody and control standards that fit institutional practice, where control is often split across roles and approval systems. A third is to set clear expectations for exception handling: freezes, reversals, court orders, sanctions actions, and recovery after outages. A fourth is to address settlement assets and access rules, because tokenized markets cannot mature on an uncertain cash leg. A fifth is to address cross-border recognition and conflict-of-laws issues for tokenized claims, especially where electronic transferable records or control-based security rights are involved. None of these require regulators to pick a specific technology. They require regulators to define the legal and operational outcomes the market must be able to show.

For market participants—issuers, investors, custodians, venues, and service providers—the practical takeaway is that tokenization is a systems project, not a platform purchase. Issuers must decide whether they are offering direct ownership, beneficial ownership, or a contract claim, and then draft and operate accordingly. Investors must demand clarity on rights mapping, insolvency posture, and settlement finality, rather than accepting "on-chain" as a substitute for diligence. Custodians must treat key management and policy enforcement as core risk work, because custody failures in token systems can propagate quickly and be hard to unwind. Venues must confront liquidity formation realities: fragmented markets do not build deep liquidity simply by being open all the time. Service providers must accept that they are becoming part of market infrastructure and will be held to higher standards over time, including audit, continuity, and clear liability terms.

The study also suggests a likely direction of market evolution. Tokenization is moving toward hybrid models that preserve familiar protections while introducing token-based workflows in targeted ways. This is visible in government bond programs that combine digitally native issuance with optional access through conventional rails, and in market utility initiatives that tokenize representations while keeping entitlements intact. These approaches lower the adoption barrier for institutions because they do not demand that every participant rebuild custody and settlement from scratch. At the same time, they create a path where tokenization becomes embedded inside existing market infrastructure rather than replacing it. Over time, this could yield a system where tokenized representations are common in post-trade processes, collateral management, and servicing, while open secondary markets remain concentrated in a small set of assets that suit always-available trading and simple redemption.

The paper does not claim that this path is inevitable. It is a consequence of incentives and constraints. Institutions are willing to adopt new rails when they can preserve enforceability and supervision. They are less willing to adopt structures that require new legal assumptions about ownership and finality without clear remedies. Hybrid paths fit that risk posture. Whether they lead to deeper structural change depends on whether legal frameworks evolve to support more native ownership records, and whether settlement assets evolve to support finality and liquidity under stress without concentrating risk in one rail.

Several research gaps remain, and they matter for both policy and market design.

One gap is empirical reporting on real operating outcomes. Many tokenization announcements report issuance size or the fact of a pilot. Few report how many exceptions occurred, how many transfers required manual intervention, how long dispute resolution took, or how much servicing workload changed. Without this, it is hard to compare designs or to know where benefit claims hold.

A second gap is the treatment of tax and withholding in tokenized systems. Tax is often treated as an afterthought in tokenization narratives. In practice it shapes investor participation, transfer friction, and servicing cost. Tokenized systems that cannot handle withholding, reporting, and investor classification cleanly will remain constrained to narrow channels.

A third gap is the treatment of data integrity as market infrastructure risk. Tokenized markets rely on data feeds for valuation, corporate actions, proofs of holdings, and lifecycle triggers. Failures here can cause mispricing and forced transfers even when the underlying asset is stable. Research and supervision should treat key data services as critical nodes, with clear standards for assurance and continuity.

A fourth gap is conflict-of-laws design for tokenized collateral and electronic transferable records. Control-based approaches can narrow uncertainty, but they also interact with custody arrangements that split control among parties. More work is needed to map how control evidence is recognized across borders and how priority disputes are resolved when the parties and systems span jurisdictions.

A fifth gap is how market integrity rules adapt to always-available trading and transfer. Market abuse rules, best execution norms, surveillance expectations, and fair pricing assumptions were shaped in markets with defined trading hours and centralized venues. Tokenized markets can run continuously and across fragmented venues, which raises new practical questions about surveillance, data consolidation, and fair access. Research and regulation will need to address these mechanics rather than relying on general statements about technology.

Finally, the study returns to a framing that runs through every chapter: tokenization is a coordination problem. It requires technical capability, legal recognition, regulatory permission, and market incentive to line up. Many current initiatives demonstrate one or two of these elements. Few demonstrate all. This is not a failure. It is the normal pattern of market infrastructure change. Settlement and custody systems do not change quickly because they are built to survive stress, not to ship features.

The value of a rights-and-control schema is that it turns that coordination problem into something the market can reason about. It allows policymakers to see which legal clarifications would unlock specific designs. It allows market participants to see where dependencies and liabilities sit. It allows researchers to compare case studies without assuming that all “tokenization” is the same thing.

If tokenization becomes routine in parts of capital markets, it will not be because tokens exist. It will be because market participants can point to clear answers on ownership, control, finality, and insolvency, and because settlement assets support those answers under stress. If tokenization remains bounded, it will not be because ledgers were too slow. It will be because enforceability and settlement design did not keep pace with technical possibility, or because the cost of new dependencies outweighed the gains.

The practical message to end on is therefore plain. Tokenization should be evaluated as a market structure redesign, case by case, with claims and control as the starting point. The question is not whether an asset can be represented as a token. Almost any asset can be represented as a token. The question is whether the tokenized product creates clear rights that survive disputes and failures, whether settlement is final in a way that courts and regulators recognize, and whether the operational system can handle exceptions without breaking trust. Where the answer is yes, tokenization can become a useful part of financial market plumbing. Where the answer is no, tokenization remains a demo, even if it looks impressive on a screen.