Tokenised Private Shares: What Changes and What Remains Legally Off-Chain

A Global Ownership, Transfer and Settlement Control Framework for Digital Private Securities

Authored by Chennakeshav Adya
Independent Researcher
August 2026

Abstract

Tokenising a private share can change how an interest is represented, distributed, instructed, transferred and serviced. It does not by itself decide what the holder legally owns, which record prevails, whether the issuer recognises the transfer, who may participate, when settlement becomes final, how restrictions apply or which remedy survives a technology failure. Those outcomes depend on the instrument, corporate law, securities law, governing documents, regulated activities, books and records, custody structure, transfer mechanics, payment asset, platform rules and jurisdictions involved.

This paper develops a global ownership, transfer and settlement control framework for tokenised private shares. It distinguishes issuer-native securities, issuer-linked notification tokens, custodial tokenised entitlements and synthetic tokenised exposures. For each model, it identifies the legally authoritative record, holder claim, transfer event, identity layer, restrictions, cash leg, corporate actions, reconciliation duties and failure remedies. The framework includes an on-chain and off-chain control matrix, model-classification tree, transfer state machine, delivery-versus-payment architecture, corporate-action workflow, exception dashboard, ten-day readiness diagnostic and thirty-day implementation office.

The analysis draws on current official materials from the US Securities and Exchange Commission, the Financial Conduct Authority, the Bank of England, the European Securities and Markets Authority, the Dubai Financial Services Authority, the Abu Dhabi Global Market Financial Services Regulatory Authority and the Bank for International Settlements. Applicable requirements depend on the issuer, instrument, holder, activity, venue, operator, custody model, communication, settlement asset and jurisdiction. Current legal, regulatory, compliance, financial-crime, sanctions, data-protection, tax and accounting advice is required. Worked values, thresholds, timelines and scenarios are management assumptions used solely to demonstrate the framework.

JEL Classification: G15, G18, G23, G24, G32, G38

Keywords: tokenised private shares, digital securities, distributed ledger technology, private markets, transfer restrictions, settlement finality, corporate actions, ownership records

1. Begin with the legal claim rather than the token

A tokenised private-share project should begin by defining the investor's enforceable claim. The token may itself be the security, update the issuer's authoritative ownership record, evidence an entitlement held through a custodian, notify an off-chain registrar, or provide contractual exposure to another security. These structures can look similar on a screen while producing different rights, risks and remedies.

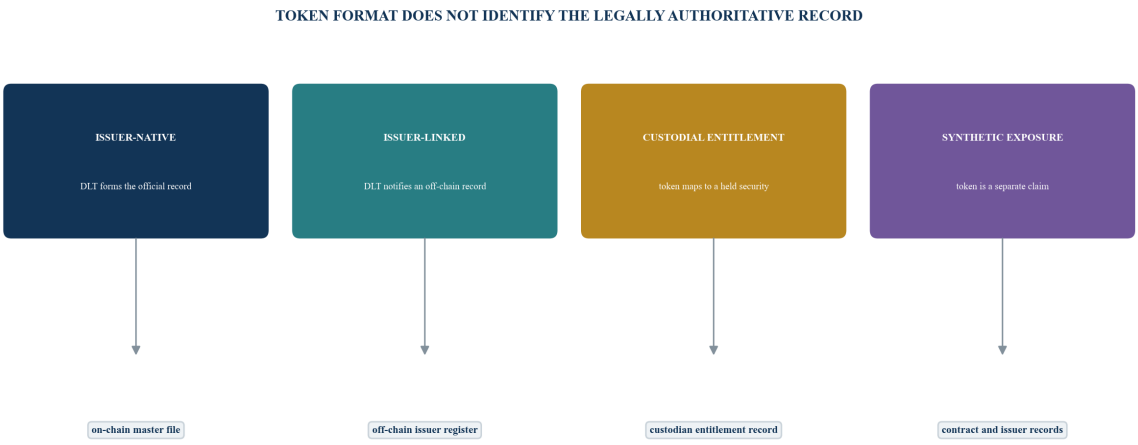
The US Securities and Exchange Commission staff's January 2026 statement describes issuer-sponsored and third-party tokenisation models. An issuer or its agent can integrate distributed ledger technology into the master securityholder file. Another issuer-sponsored model can leave the authoritative record off-chain and use an on-chain transfer as a notification to update it. A third party can issue a tokenised security entitlement backed by a security held in custody, or issue its own security providing synthetic exposure. The statement also notes that federal and state law govern the activities, transactions and relationships involved.

The design question is therefore: what legally changes when the token moves? A blockchain entry can be technologically final while the issuer's register, custodian account, transfer-agent record or governing documents still show no valid ownership change. Conversely, a legally effective transfer can be recorded through a ledger that forms part of the official books.

The control framework documents one authoritative answer for each state. It identifies the security, issuer, governing law, legally authoritative record, registered and beneficial holder, token issuer, platform operator, transfer agent or registrar, custodian, intermediary, wallet controller, cash provider and dispute forum.

Tokenisation can improve workflow and evidence. It cannot replace transaction-specific legal analysis. The implementation record should explain what the technology does, what the law recognises, what human or institutional acts remain required and how inconsistencies are resolved.

Figure 1. Four tokenisation models and the legally authoritative record



Classification and legal effect require instrument- and jurisdiction-specific advice.

2. Classify the model before designing the operating process

Model classification determines the control perimeter. An issuer-native security can make the distributed ledger all or part of the master securityholder file. In that structure, a valid ledger transfer may change the official ownership record, subject to the governing documents and applicable law.

An issuer-linked notification model leaves the master file off-chain. The token movement sends an instruction or evidence to the issuer or agent. Ownership changes when the off-chain record is validly updated. The process needs an explicit pending state between on-chain transfer and issuer recognition.

A custodial entitlement model inserts a third-party issuer or custodian between the investor and the underlying private share. The token holder may own a security entitlement or beneficial interest rather than become the registered shareholder. The operating design should expose the custody chain, segregation, insolvency treatment, voting, distributions, substitutions, fees and redemption rights.

A synthetic model creates a separate instrument whose value references the private share. The token holder may have no ownership or entitlement in the referenced company. Counterparty credit, collateral, valuation, termination and disclosure become central. Marketing language should not blur exposure to a share with ownership of that share.

Classification cannot rely on product names such as digital equity, on-chain stock or tokenised share. The analysis should read the instrument terms, corporate approvals, shareholder record, platform rules, custody agreement, wallet terms, transfer-agent process and cash arrangements together.

Table 1. Model-classification and control consequences

Model	Investor's immediate claim	Authoritative ownership record	Critical control
issuer-native	issuer security	DLT master file or integrated component	valid on-chain issuance and transfer
issuer-linked	issuer security after recognised update	issuer or agent's off-chain record	reconcile token events to registration
custodial entitlement	claim through custodian or intermediary	entitlement record plus underlying custody record	preserve one-to-one backing and holder rights
synthetic exposure	contractual claim against token issuer	contract, token ledger and reference data	disclose no underlying ownership and manage counterparty risk

The matrix is a decision aid and does not determine legal characterisation.

3. Define the digital security master

The security master connects the token identifier to the legal instrument. It records the issuer's legal name and jurisdiction, security class, series, authorised and issued quantity, nominal value, currency, rights, seniority, conversion terms, voting, dividends, information rights, pre-emption, transfer restrictions, legends, governing documents, corporate approvals and authoritative register.

The token layer adds network, contract address, token standard, issuance transaction, decimals, supply controls, wallet rules, administrative keys, upgrade powers, pausing, burning, recovery, allowlists and bridge or interoperability arrangements. Each technical field should map to a legal purpose and an accountable owner.

One token should not silently represent several legal classes. A legal class should not appear as several token contracts without a reconciliation rule. Migrations and upgrades require a controlled

mapping from the old identifier to the new one, including frozen or lost tokens and pending transfers.

Supply integrity requires three reconciliations: authorised shares to issued shares; issued shares to the authoritative holder record; and that holder record to token supply. Treasury shares, cancelled units, locked allocations, fractional interests, options, warrants and convertible claims require separate states. A token burn may not legally cancel a share until required corporate acts and records are complete.

The master also records where personal identity is held. SEC staff guidance on transfer agents contemplates blockchain records for wallet addresses, balances, ownership percentages, share quantities, purchase dates and transaction identifiers while personal and non-public information remains within proprietary systems. The architecture should connect those records without publishing protected data unnecessarily.

4. Separate identity, wallet control and legal ownership

A wallet address is a technical destination. It does not by itself establish the legal identity, capacity, authority or eligibility of the person controlling it. The holder model should bind the wallet to a verified natural or legal person, relevant beneficial owners, representative authority, investor classification, jurisdiction, sanctions and financial-crime results, tax status, permitted activities and confidentiality obligations.

The binding can expire. Corporate ownership, directors, signatories, investor classification or sanctions status can change. Wallet keys can be delegated, compromised, recovered or held by a custodian. A current identity record therefore needs validity dates, event triggers, review history and the specific wallets and roles covered.

Private shares often have issuer-specific eligibility restrictions. Employees, existing shareholders, competitors, sanctioned persons, retail investors, residents of specified jurisdictions or transferees lacking issuer consent may be restricted. A general platform allowlist can be insufficient because eligibility depends on the individual instrument and transaction.

Lost-key and succession processes expose the difference between control and ownership. If a verified owner loses a private key, the system needs a legally supportable process to freeze, cancel, reissue or redirect the token while preserving the authoritative ownership record. Death, incapacity, insolvency, court orders, secured claims and estate administration can also require intervention outside ordinary token transfers.

Privacy design should minimise disclosure. Identity, tax, financial-crime and beneficial-ownership data can remain off-chain with controlled attestations on-chain where lawful and suitable. The record should explain who can resolve the attestation, how revocation works and what happens when the identity service fails.

Figure 2. Identity, wallet and ownership binding

Data placement is illustrative and remains subject to privacy and recordkeeping requirements.

5. Preserve transfer restrictions as executable controls

Private shares can carry contractual, constitutional, statutory and regulatory restrictions. Common controls include board consent, rights of first refusal, pre-emption, co-sale, lock-ups, employee-plan conditions, holding periods, legends, permitted-transferee definitions, information requirements and jurisdictional selling restrictions.

The token contract can automate parts of the process. It can restrict transfers to approved wallets, enforce quantity limits, require approval signatures, pause movement or direct transactions through a controlled venue. Automation should reflect the governing documents accurately and support amendments.

Some judgements remain off-chain. A board may exercise discretion. A right of first refusal may require notice, valuation, time periods and documentary evidence. A permitted-transferee definition can require legal interpretation. A regulatory exemption can depend on facts that change by holder, communication and transaction.

The transfer rulebook should identify every condition, source document, decision owner, evidence, sequence, system enforcement and override authority. A smart contract rule without a legal source can create arbitrary blockage. A legal restriction without technical enforcement can allow an on-chain movement that the issuer refuses to recognise.

Rules need version control. New financing rounds, amendments, shareholder agreements, restructurings and changes of law can change transferability. Historic transactions should remain traceable to the rule set in force at the time.

Table 2. Transfer-restriction control matrix

Restriction	Off-chain evidence	Possible on-chain control	Completion evidence
board consent	resolution or delegated approval	approval signature or transfer gate	register updated after consent
holder eligibility	identity and classification record	instrument-specific wallet allowlist	eligible holder linked to wallet
right of first refusal	notice, response and expiry record	timed transfer lock	waiver or completed process
quantity constraint	cap table and available position	balance and order limit	no excess issue or transfer
selling restriction	current legal and compliance analysis	jurisdiction and channel gate	route-specific approval retained
lock-up or legend	governing document and dates	time lock with controlled override	authorised release recorded

Conditions vary by issuer, instrument, holder, route and jurisdiction.

6. Build a transfer state machine

A robust process exposes the states between commercial agreement and final ownership. The sequence can include indication, eligibility review, information permission, order, matching, execution, consent request, right-of-first-refusal process, documentation, funding, token lock, cash confirmation, on-chain movement, register update, settlement finality and post-settlement reconciliation.

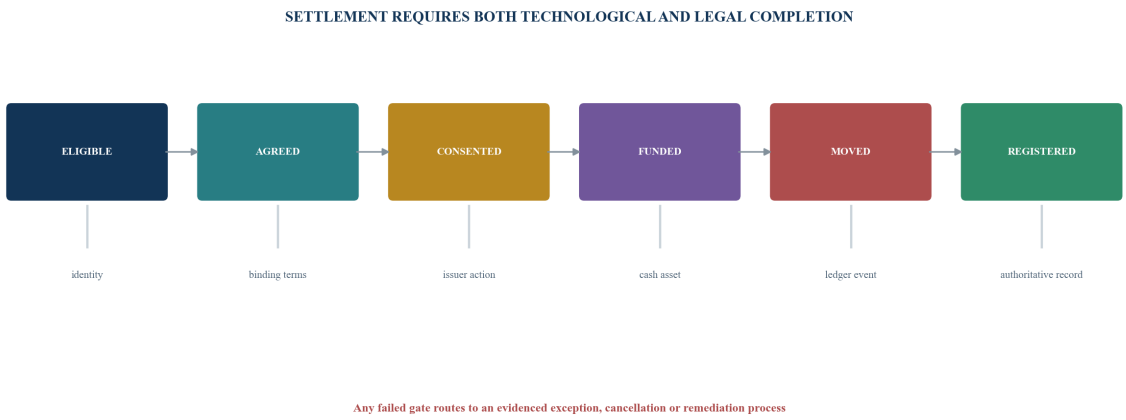
The state machine prevents premature claims. A transaction can be commercially agreed while legally conditional. A token can be locked without being transferred. A blockchain transaction can be confirmed while the issuer update remains pending. Cash can be received without effective delivery.

Each state needs entry criteria, exit criteria, evidence, owner, service level, cancellation route and exception path. The system should preserve amendments and failed attempts. Timestamps need a common standard so the full sequence can be reconstructed.

The authoritative state should be clear to participants. If the platform says settled while the issuer register says pending, the discrepancy should generate an immediate exception. If a transaction can be reversed or corrected through administrative keys, the conditions and authority should be disclosed and governed.

Legal finality requires a defined point at which ownership and payment become irrevocable and unconditional under the applicable framework. A count of blockchain confirmations is a technology measure. It should be connected to the legal finality analysis rather than substituted for it.

Figure 3. Tokenised private-share transfer state machine



States are illustrative and require transaction-specific design.

7. Design the cash leg and delivery-versus-payment

Tokenising the security does not automatically tokenise money. The cash leg may settle through a bank transfer, commercial-bank money, central-bank money, e-money, stablecoin or another settlement asset. Each choice introduces different credit, liquidity, redemption, safeguarding, operational and legal-finality considerations.

Delivery-versus-payment aims to link delivery of the security to payment so one leg does not complete without the other. Both legs can operate on one platform, on connected ledgers or across token and account-based systems. The design should document the conditional logic, timeouts, failure states and finality point.

The Bank for International Settlements has described the potential for shared programmable platforms and central-bank settlement assets to reduce risks and costs. It has also noted that tokenisation does not remove settlement-failure risk and that interaction with account-based systems remains important. Liquidity requirements can increase when transactions settle gross or cash is fragmented across platforms.

The UK Digital Securities Sandbox allows approved firms to test issuance, trading and settlement using developing technology under a regulated framework. The Bank of England's 2026 updates allow applications for specified stablecoins meeting minimum requirements as settlement assets in the sandbox. Approval and limits remain firm- and stage-specific.

Private-share projects should resist a false choice between instant and safe. Prefunding can reduce principal risk while increasing liquidity cost. Atomic settlement can remove one exposure while concentrating dependence on code, network availability and the settlement asset. The business case should measure these trade-offs.

Table 3. Cash-leg and settlement design choices

Cash model	Potential benefit	Principal dependency	Control question
bank transfer	familiar rails and records	cut-off times and reconciliation	when is cash irrevocably available?
commercial-bank token	programmable bank claim	issuer and platform access	what claim and redemption right exists?
central-bank settlement	strong monetary anchor	permitted infrastructure and participation	can the transaction access the rail?
stablecoin	programmable and extended-hour transfer	backing, redemption, safeguarding and price	is the asset acceptable through failure?
prefunded escrow	visible funds before delivery	trapped liquidity and escrow authority	who releases or returns the funds?
cross-platform DvP	connects existing systems	interoperability and timing	what occurs if one platform completes first?

Settlement assets and arrangements require jurisdiction- and participant-specific analysis.

8. Treat settlement finality as a legal and operational control

The finality analysis should identify when the security transfer and payment become irrevocable and unconditional, which law governs each leg, which system rules apply, and what insolvency, court order, fraud, mistake or cyber event can still affect the outcome.

Blockchain immutability is only part of the analysis. Administrative keys, contract upgrades, chain reorganisations, forks, validation failures, sanctions interventions or legal orders may affect the practical result. The platform should explain whether corrections occur through reversal, compensating entries, token cancellation and reissuance, or an off-chain ownership determination.

Cross-border arrangements can connect the issuer's corporate law, holder and intermediary jurisdictions, network or node locations, platform rules, custody law and cash-settlement framework. Conflicts rules and recognition should be analysed before live use.

The Basel Committee's cryptoasset framework requires clear, legally enforceable rights, obligations and interests in relevant jurisdictions and proper documentation of settlement finality for qualifying arrangements. The exact prudential treatment depends on the exposure and institution, yet the documentation discipline is useful for every project.

An exception register should distinguish technology completion, legal completion, cash finality and operational reconciliation. The oldest unresolved state, value at risk, cause, owner and remediation should reach management promptly.

9. Keep the authoritative register reconciled

Issuer-linked and custodial models rely on more than one record. The operating model should reconcile the token ledger to the issuer register, transfer-agent file, custodian account, entitlement ledger and total issued supply at defined intervals and after material events.

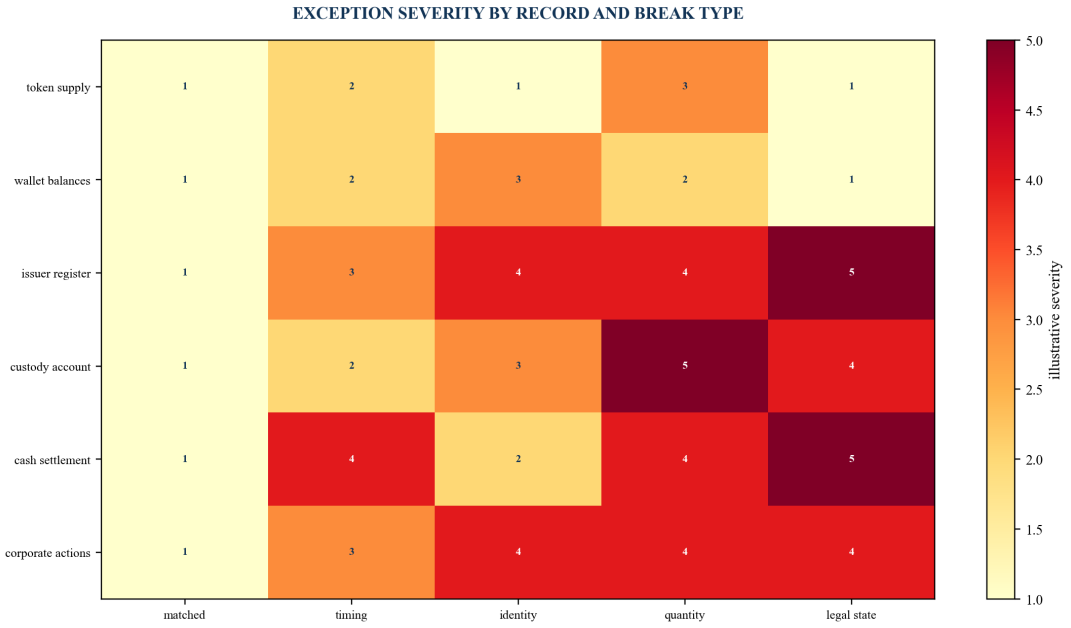
Reconciliation should work at holder and transaction levels. Aggregate supply can balance while individual holders are wrong. It should test opening positions, issuances, transfers, cancellations, freezes, burns, reissues, corporate actions, pending states and closing positions.

Breaks need cause codes. Timing differences, failed interfaces, incorrect identity mapping, decimals, duplicated events, chain reorganisations, unauthorised transfers, manual updates and corporate-action errors require different responses. A balancing adjustment without root-cause evidence can hide ownership risk.

The authoritative record hierarchy should be approved in advance. If systems disagree, the incident process identifies the record that controls the legal result, prevents further inconsistent transactions and preserves evidence. Corrections should be authorised, communicated and auditable.

Reconciliation also protects backing. A custodial entitlement token should not exceed the underlying security position or the quantity allocated to that token programme. Encumbrances, lending, collateral and substitutions should be visible. The holder needs clear disclosure of the custody and insolvency structure.

Figure 4. Record reconciliation and exception severity



Values and thresholds are illustrative management assumptions.

10. Rebuild corporate actions for the token structure

Private-company actions can include dividends, voting, information notices, pre-emption, rights issues, conversions, splits, consolidations, tenders, repurchases, mergers, drag-along, tag-along, compulsory transfers and liquidation proceeds. The token design should define how each event reaches the legally entitled holder.

Record dates are critical. The on-chain holder, registered holder and beneficial owner can differ. Pending or failed transfers can create competing claims. The event process should identify the controlling record and the cutoff time, including time-zone and network conventions.

Smart contracts can automate calculations and distribution instructions. The issuer or authorised agent still needs accurate event terms, funded assets, tax and withholding decisions, eligibility results, legal approvals and exception handling. Code should implement approved terms rather than infer them.

Voting requires identity and authority. A custodian or nominee may be the registered holder while token holders provide instructions. The system should manage notices, options, deadlines, partial elections, conflicting instructions, quorum, proxies and result evidence.

Mergers and restructurings can replace or cancel the underlying share. The token programme needs a controlled path to suspend transfers, determine entitlements, distribute consideration, burn or replace tokens and close the historic record. A token should not continue trading as though the old claim survives.

Table 4. Corporate-action operating controls

Event	Authoritative input	Token-layer action	Off-chain completion
dividend	board approval, record date and amount	snapshot and distribution instruction	funding, tax, payment and reconciliation
vote	notice, eligibility and voting rules	instruction capture and aggregation	registered vote and result evidence
conversion or split	approved terms and effective date	adjust or replace token units	update security and holder records
tender or repurchase	offer terms, elections and allocation	lock accepted tokens	payment, cancellation and register update
merger	transaction documents and entitlement	suspend, map or replace tokens	issue consideration and close old security
compulsory transfer	valid legal trigger and authority	freeze, cancel or redirect	record decision, remedy and notification

Entitlements and procedures depend on the legal instrument and holding structure.

11. Govern smart contracts and administrative powers

Smart contracts can enforce issuance limits, allowlists, transfer approvals, locks, distributions and recovery. Their power requires accountable governance. The control file should identify the code owner, deployer, administrators, signatories, upgrade authority, pause authority, recovery authority, oracle providers and emergency process.

Code review should connect requirements to implementation. Tests cover permitted and prohibited transfers, boundary quantities, expired permissions, concurrent events, lost keys, failed cash, corporate actions, contract upgrades and recovery. Independent security testing and remediation evidence should precede production use.

Administrative controls require segregation. A single individual should not be able to issue tokens, change eligibility, transfer assets and erase evidence. Multi-signature arrangements, hardware security, privileged-access monitoring, transaction limits and delayed high-risk actions can reduce misuse.

Upgrades can change investor rights or operational behaviour. The governing documents should specify when upgrades are permitted, what approval and notice apply, how dissent or exit works, and how historic states remain accessible. A code fork should not create two ungoverned claims on the same share.

External components add dependencies. Identity attestations, price oracles, bridges, custody APIs, cash tokens and cloud infrastructure need due diligence, service levels, incident notification,

continuity plans and exit routes.

12. Map the regulated-activity perimeter

Tokenisation does not remove the securities perimeter. Issuing, marketing, arranging, advising, dealing, operating a venue, custody, safeguarding, settlement, transfer agency, managing assets or operating collective arrangements can trigger different requirements.

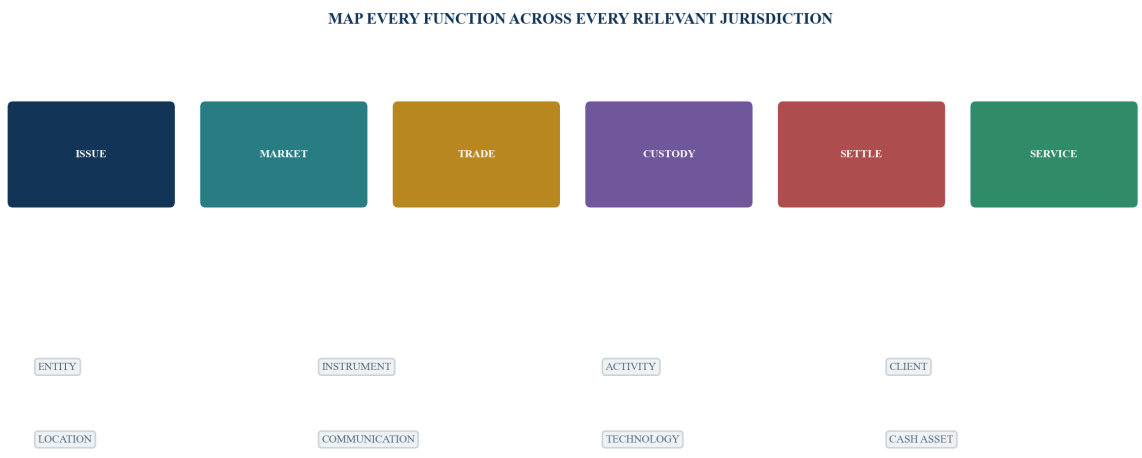
The DFSA's Investment Token framework applies to relevant activities in or from the Dubai International Financial Centre and defines Security and Derivative Tokens by reference to rights and obligations represented using distributed ledger or similar technology. ADGM guidance likewise addresses the regulatory treatment of tokens that are securities. Permissions remain activity-specific.

The European Union's DLT Pilot Regime provides a framework for DLT multilateral trading facilities, settlement systems and combined trading and settlement systems, with instrument and value conditions. National authorities authorise and supervise participants while ESMA coordinates and publishes relevant information.

The UK Digital Securities Sandbox enables approved firms to test notary, maintenance, settlement and trading-venue activities under temporarily modified requirements. A Gate 1 approval does not itself authorise live activity; the Bank of England dashboard records entrant stages and approval notices.

The perimeter map should cover entity, activity, instrument, client, communication, location, venue, custody and cash. It records the legal basis, permission, restriction, evidence, owner and review date. Cross-border distribution needs its own route-by-route analysis.

Figure 5. Tokenised private-share regulatory perimeter map



The map frames the analysis and does not determine applicable requirements.

13. Protect disclosure and investor understanding

Disclosure should explain the instrument before the technology. It states whether the investor owns the issuer's share, a security entitlement, a beneficial claim through a vehicle or custodian, or a separate synthetic instrument. It names the obligor and identifies the authoritative record.

The investor should understand transfer restrictions, eligible venues and wallets, custody, fees, corporate actions, voting, distributions, redemption, settlement asset, technology dependencies, administrative powers, conflicts, insolvency treatment, data use and remedies.

Marketing terms can create confusion. Fractional access does not necessarily produce liquidity. Twenty-four-hour technical availability does not mean the issuer, bank, registrar, compliance team or transfer process operates continuously. Faster ledger movement does not establish faster legal completion.

Performance and valuation require care. A token price can reflect a thin or fragmented venue, different rights, custody claims, fees, transfer restrictions or counterparty risk. Synthetic and custodial models should not be compared directly with the underlying share without adjustments.

Disclosure governance should record authors, evidence, approvals, versions, recipients and updates. Material changes to code, governance, custody, backing, settlement assets or legal structure can require revised information and holder communication.

14. Control data, privacy and cyber risk

A public or shared ledger can preserve transaction evidence while exposing addresses, balances and behavioural patterns. Pseudonymity may not prevent re-identification. The data architecture should classify personal, confidential, commercially sensitive and regulated information before deciding placement.

Off-chain stores often remain necessary for identity, beneficial ownership, tax, sanctions, source-of-funds, contractual documents, investor communications and legal opinions. On-chain references can support integrity if hashes, attestations and access controls are designed appropriately.

Data rights require operational procedures. Correction, restriction, retention, legal holds and deletion can conflict with immutable records. The design can minimise on-chain personal data and use revocable or updateable pointers, subject to legal advice.

Cyber scenarios include key theft, wallet compromise, malicious upgrades, oracle manipulation, bridge failure, denial of service, compromised administrators and fraudulent recovery. The response should link technology containment to legal ownership protection, communications, notification and transaction controls.

Continuity plans should address network or provider failure. Participants need a controlled fallback record, authority to suspend transfers, a recovery sequence and reconciliation before reopening. The issuer's ability to identify lawful holders should survive the failure of a particular interface or service provider.

Table 5. Critical tokenisation risks and response evidence

Risk	Immediate control	Authoritative evidence	Recovery objective
key compromise	freeze affected route and notify control owner	identity, holder and transaction records	restore lawful control without double claim
contract defect	pause governed functions	approved code, tests and incident record	remediate and reconcile every affected state
record mismatch	stop inconsistent transfer or servicing	defined record hierarchy and source files	align legal and technical ownership
cash-leg failure	prevent unmatched delivery	payment and finality records	return or complete both legs lawfully
provider outage	invoke continuity procedure	replicated record and operational logs	resume from reconciled state
privacy incident	contain access and preserve evidence	data map and disclosure record	meet legal duties and reduce further exposure

Response requirements depend on the incident, legal framework and adopted policy.

15. Validate the business case with complete economics

Tokenisation can reduce manual reconciliation, shorten processes, improve programmability and expand controlled access. These benefits should be measured against build, legal, regulatory, custody, identity, cyber, audit, integration, cash, governance and operating costs.

The baseline captures current time, people, errors, failed settlements, reconciliations, transfer completion, corporate-action effort, cash use and external fees. The target model then measures changes using comparable transaction populations.

Liquidity claims need evidence. Fractionalisation can increase the number of possible holders while restrictions, limited buyers, information asymmetry and issuer approval still constrain trading. A tokenised security can remain illiquid.

Capital and liquidity effects can move in both directions. Faster settlement can reduce exposure periods. Gross or prefunded settlement can increase cash requirements. Fragmented platforms can require duplicated liquidity and collateral.

The decision case should include downside scenarios: lower volume, delayed permissions, manual exceptions, a parallel legacy system, provider replacement, cyber remediation and wind-down. Management approves the model with explicit assumptions and review triggers.

16. Build a decision-focused dashboard

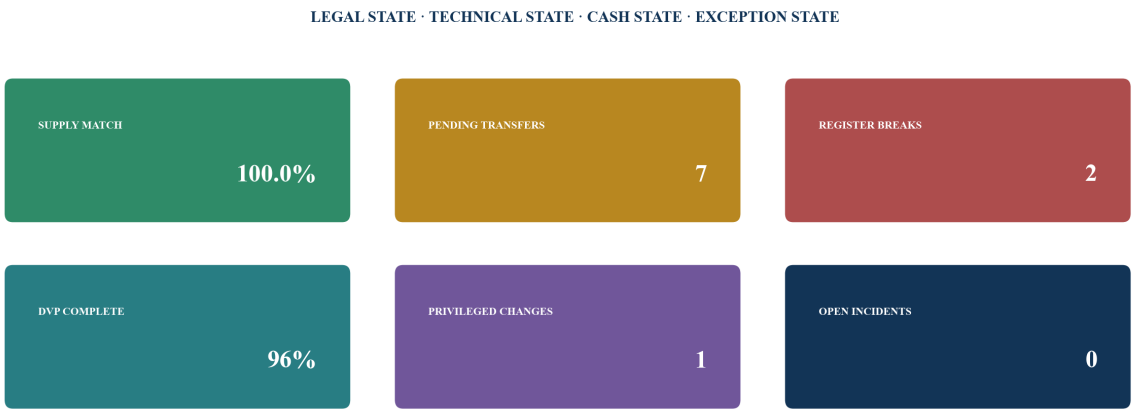
The dashboard should show whether the legally authoritative and technical states agree. Core measures include issued shares, token supply, backing, registered and beneficial holders, active wallets, pending transfers, consent age, cash status, reconciliation breaks, corporate-action exceptions, privileged changes and incidents.

Risk measures use denominators. Transfer failure rate should show failed transfers over attempted eligible transfers. Reconciliation ageing should show value and count. Corporate-action accuracy should use the complete eligible population. Liquidity measures should distinguish executable transactions from indications.

The board view should be concise: current model, live jurisdictions, instruments, holders, value, unresolved legal opinions, material exceptions, service availability, security incidents, compliance events and upcoming decisions.

Management should be able to trace every metric to records. Narrative commentary explains cause, impact, remediation, owner and due date. A green dashboard without reconciled ownership evidence provides false assurance.

Figure 6. Tokenised private-share control dashboard



Measures and thresholds are illustrative management assumptions.

17. Establish governance and evidence retention

The governing body approves the business purpose, token model, risk appetite, jurisdictions, holder types, authoritative record, cash model, material providers and wind-down approach. Delegated committees oversee implementation within documented authority.

Accountability spans legal, compliance, operations, technology, cyber, finance, tax, data, product, investor relations and corporate secretarial functions. The responsibility map distinguishes design, approval, operation, assurance and incident decisions.

The evidence file preserves instrument terms, approvals, legal analysis, permission mapping, code versions, tests, security reviews, identity design, service-provider diligence, reconciliations, disclosure, corporate actions, incidents and changes. Retention follows applicable requirements and legal holds.

Independent assurance tests the control design and operating evidence. Samples should include successful, failed, cancelled, recovered and corrected transactions. Testing should validate holder identity, restrictions, supply, backing, register updates, cash finality and exception closure.

Change governance covers new instruments, networks, jurisdictions, wallets, cash assets, contract upgrades, providers and transaction routes. Material changes reopen the relevant legal and operational analysis before release.

18. Run a ten-day tokenisation readiness diagnostic

Days one and two define the proposed instrument, commercial objective, jurisdictions, participants and current process. The team collects governing documents, cap-table records, product materials, architecture, provider contracts, workflows and available legal analysis.

Days three and four classify the token model and map the legally authoritative record, holder claim, rights, restrictions, identity layer, regulated activities, custody, cash and finality. Unresolved questions become named decision items.

Days five and six walk the full lifecycle: issue, distribute, transfer, register, settle, reconcile, service corporate actions, recover keys, handle incidents and wind down. Synthetic positive and negative scenarios test the intended controls.

Days seven and eight assess architecture, code governance, privileged access, data, cyber, continuity, providers and evidence. The team builds an on-chain/off-chain matrix and identifies manual dependencies.

Days nine and ten quantify the business case, rank gaps and present the decision. The output is a model classification, perimeter map, ownership and settlement control matrix, red-flag register, target workflow, economics and sequenced implementation plan.

19. Implement a thirty-day ownership and settlement office

Days one to five establish governance, workstreams, decision rights, document control and a single issue log. The team confirms the instrument and model boundary before building interfaces.

Days six to ten design the security master, holder and wallet binding, authoritative record hierarchy, transfer rules, state machine, cash leg and reconciliation. Legal and regulatory advisers resolve priority questions.

Days eleven to fifteen configure workflows, evidence fields, permissions, smart-contract controls, dashboards and exception routing. Provider responsibilities and service levels are incorporated.

Days sixteen to twenty execute end-to-end tests covering normal transactions, restricted holders, expired consent, failed cash, record breaks, lost keys, corporate actions, cyber incidents and recovery. Defects receive owners and retests.

Days twenty-one to twenty-five complete disclosure, operating procedures, training, continuity and launch criteria. Independent reviewers assess the high-risk controls.

Days twenty-six to thirty run a controlled rehearsal, close critical gaps, approve residual risks and decide whether to proceed, limit the scope, extend remediation or stop. The handover includes a ninety-day monitoring agenda.

Table 6. Thirty-day implementation-office deliverables

Workstream	Core deliverable	Acceptance evidence	Accountable owner
legal model	claim, record and finality memorandum	approved conclusions and open items	legal sponsor
instrument	security and token master	reconciled governing and technical fields	product owner
transfer	restrictions and state machine	scenario tests and documented exceptions	operations owner
settlement	cash and DvP design	both-leg finality and failure evidence	settlement owner
technology	governed contracts and interfaces	independent tests and access evidence	technology owner
launch	disclosure, procedures and dashboard	controlled rehearsal and signed decision	executive sponsor

Timing depends on scope, evidence, adviser availability and technology readiness.

20. Package work around decision-grade outcomes

A focused readiness diagnostic can determine whether a proposed token represents the intended legal claim and whether the ownership, transfer and settlement design is viable. The deliverables include model classification, on-chain/off-chain matrix, perimeter map, gap register, target workflow and implementation case.

An ownership-control build can establish the security master, holder and wallet binding, transfer restriction rulebook, authoritative record hierarchy and reconciliation. The outcome is a traceable record from legal instrument to token and holder.

A settlement workstream can design the cash leg, delivery-versus-payment sequence, finality analysis, exceptions and recovery. It can test whether both legs complete lawfully under normal and adverse scenarios.

A corporate-action and servicing workstream can map entitlements, record dates, voting, distributions, conversions, tenders and restructurings into governed workflows and smart-contract requirements.

A recurring control office can monitor supply, backing, register breaks, pending transfers, privileged changes, provider performance, incidents and regulatory developments. Each engagement should have written scope, evidence requirements, qualified advisers where required, acceptance criteria and measurable outcomes.

The commercial decision remains evidence-led. A project should proceed when the intended claim, authoritative record, permissions, restrictions, cash, finality, technology, economics and governance align. Tokenisation adds value when it improves a legally coherent transaction rather than decorating an unresolved one.

References

[1] US Securities and Exchange Commission, Divisions of Corporation Finance, Investment Management, and Trading and Markets. Statement on Tokenized Securities. 28 January 2026. https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

[2] US Securities and Exchange Commission, Division of Trading and Markets. Frequently Asked Questions Relating to Crypto Asset Activities and Distributed Ledger Technology. https://www.sec.gov/rules-regulations/staff-guidance/trading-markets-frequently-asked-questions/frequently-asked-questions-relating-crypto-asset-activities-distributed-ledger-technology

[3] US Securities and Exchange Commission. Private Secondary Markets. Updated 24 April 2026. https://www.sec.gov/resources-small-businesses/capital-raising-building-blocks/private-secondary-markets

[4] Financial Conduct Authority and Bank of England. PS24/12: Digital Securities Sandbox Joint Policy Statement and Final Guidance. Updated 3 December 2025. https://www.fca.org.uk/publications/policy-statements/ps24-12-digital-securities-sandbox-joint-policy-statement-final-guidance

[5] Bank of England. Digital Securities Sandbox. https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox

[6] Bank of England. Digital Securities Sandbox Dashboard. Updated 13 July 2026. https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox/digital-securities-sandbox-dashboard

[7] Financial Conduct Authority. The Future of Tokenisation: A Joint Vision from the Authorities for UK Wholesale Markets. 2026. https://www.fca.org.uk/publications/calls-input/future-tokenisation-joint-vision-authorities-uk-wholesale-markets

[8] European Securities and Markets Authority. DLT Pilot Regime. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/dlt-pilot-regime

[9] European Securities and Markets Authority. Q&A 1239: Issuance of DLT Financial Instruments. 2 June 2023. https://www.esma.europa.eu/publications-data/questions-answers/1239

[10] Dubai Financial Services Authority. DFSA Introduces Regulatory Framework for Investment Tokens. 25 October 2021. https://www.dfsa.ae/news/dfsa-introduces-regulatory-framework-investment-tokens

[11] Abu Dhabi Global Market Financial Services Regulatory Authority. Guidance on Digital Securities Offerings and Virtual Assets. https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-on-digital-securities-offerings-and-virtual-assets.pdf

[12] Bank for International Settlements. The Next-Generation Monetary and Financial System. 24 June 2025. https://www.bis.org/publ/arpdf/ar2025e3.htm

[13] Bank for International Settlements. On the Future of Securities Settlement. 1 March 2020. https://www.bis.org/publ/qtrpdf/r_qt2003i.htm

[14] Basel Committee on Banking Supervision. SCO60: Cryptoasset Exposures. https://www.bis.org/basel_framework/chapter/SCO/60.htm

[15] Committee on Payments and Market Infrastructures and International Organization of Securities Commissions. Implementation Monitoring of PFMI: Level 2 Assessment Report for UK Payment Systems and CSDs/SSSs. 16 April 2026. https://www.bis.org/cpmi/publ/d231.htm

About the Author

Chennakeshav Adya, Independent Researcher