MatchPoint Research Working Paper No. 2026/T26

Tokenisation and AI: The Programmable-Finance Stack

A governed asset-to-cash architecture for Gulf infrastructure investors and family-office portfolios

Prepared by Matchpoint Partners
Author attribution pending CK approval
August 2026

ABSTRACT

Background. Tokenisation can place asset rights, lifecycle events and settlement instructions into programmable records; artificial intelligence can assist document extraction, monitoring, reconciliation and exception handling. Neither technology determines legal rights, regulatory status, settlement finality or investment merit. **Objective.** This paper develops a governed programmable-finance stack for A4 infrastructure and digital-infrastructure investors and A2 family-office CIOs and heads of alternatives. **Approach.** The analysis reviews 40 primary, authoritative and clearly labelled sources available through 1 August 2026 across tokenised money and assets, market infrastructure, Gulf regulation, property law, smart-contract security, AI and operational resilience. **Findings.** A durable stack begins with verified rights and authorised data, connects them to controlled token records, identity, custody, lifecycle logic and a suitable settlement asset, and keeps AI within reviewable operational roles. Institutional pilots demonstrate selected technical and operating capabilities; they do not establish universal commercial scale, liquidity or return. **Implications.** Investors should gate each use case through legal, regulatory, settlement, reconciliation, security, model-risk and operating tests before capital or client exposure. All worked inputs are unverified illustrative management assumptions; attributed Matchpoint or client revenue, cash cost reduction, loss reduction and alpha remain USD 0 until approved observed evidence exists.

Highlights

Purpose. The stack links verified asset and cash-flow rights to controlled records, settlement, operations and evidence.

Users. A4 infrastructure investors and A2 family-office allocators share diligence controls while retaining distinct mandates and authority.

Architecture. Rights, identity, token state, lifecycle logic, custody, settlement, reconciliation, AI assistance and human decisions remain traceable.

Release gate. Legal effect, regulatory perimeter, cash leg, code security, key recovery, interoperability, model governance and fallback require approval.

Economics. Productivity and revenue claims require approved observed evidence; illustrative scenarios carry no attributed value.

JEL Classification: E42, G12, G15, G23, G28, G32, L86, O33

Keywords: tokenisation, artificial intelligence, programmable finance, infrastructure, digital infrastructure, family office, real-world assets, smart contracts, delivery versus payment, tokenised deposits, digital securities, custody, interoperability, model risk

1. INTRODUCTION

Tokenisation is often described as a change in the form of an asset. That description is incomplete. A token can be a digital record of an entitlement, an instruction, a security, a claim on money, evidence of control, a receipt, or an identifier with no independent legal effect. The value of a programmable-finance system therefore depends on the chain connecting the underlying right, the authoritative record, the permitted holder, the lifecycle rule, the settlement asset, the accounting entry and the evidence retained after an event.

Artificial intelligence adds a second layer. It can extract terms from source documents, classify incoming evidence, reconcile records, identify exceptions, monitor operating data, draft review material and help service investors. It can also introduce unsupported extraction, data leakage, opaque model logic, unstable automation and excessive reliance on a vendor. AI should operate within the rights and controls of the financial arrangement. It should not create ownership, regulatory permission, settlement finality, investment suitability or decision authority.

This paper addresses **Tokenisation and AI: The Programmable-Finance Stack** for two Matchpoint Partners target audiences. **A4 Infrastructure and Digital-Infrastructure Investors** include infrastructure funds, digital-infrastructure funds, project investors and infrastructure lenders evaluating Gulf data centres, fibre, towers, energy, utilities and related real assets. **A2 Family-Office CIOs and Heads of Alternatives** include single-family offices, multi-family offices, private banks and external asset managers allocating to funds and direct opportunities across the GCC, United Kingdom, Switzerland, Singapore and the European Union. A4 investors originate, finance, monitor and exit assets. A2 investors govern allocation, liquidity, custody, concentration and manager oversight. Both need to know what the token represents, how cash moves, who controls the system and what happens when a component fails.

The governing question is: **how can tokenisation and AI improve asset administration and investment operations while preserving enforceable rights, trusted money, human authority and auditable control?** The answer is a governed programmable-finance stack. The stack begins with legal and economic rights, creates a controlled digital object that faithfully references those rights, restricts access and transfer, coordinates the asset and cash legs, services lifecycle events, reconciles every authoritative record and routes uncertainty to accountable humans.

The Financial Stability Board found that adoption of tokenisation remained very low in 2024 while identifying potential vulnerabilities in liquidity and maturity mismatch, leverage, asset quality, interconnectedness and operational fragility [1]. The Bank for International Settlements describes tokenisation as a way to combine messaging, reconciliation and asset transfer on programmable platforms anchored in trusted money [2-3]. The Eurosystem's exploratory work involved 64 participants, more than 40 trials and experiments, and over 200 transactions with a reported aggregate value of EUR 1.59 billion; the work included both actual central bank money trials and experiments using mock settlement [4]. These institutional results demonstrate selected capabilities within defined test arrangements. They do not establish universal production readiness, lower total cost, secondary liquidity, legal equivalence across jurisdictions or superior investment returns.

Market-infrastructure principles remain relevant when technology changes. The Principles for Financial Market Infrastructures address legal basis, governance, settlement finality, money settlements, custody, operational risk, access and transparency [5]. CPMI and IOSCO guidance for stablecoin arrangements emphasises that a transfer function can resemble financial market infrastructure and requires analysis against the relevant principles [6]. IOSCO's recommendations for crypto and digital-asset markets and decentralised finance address conflicts, market abuse, custody, cross-border activity, operational risk, disclosure and identification of responsible persons [7-8].

The Gulf perimeter is activity-specific. The Central Bank of the UAE's in-force Payment Token Services Regulation covers issuance, conversion, custody and transfer of payment tokens within its scope [11]. The Dubai Financial Services Authority defines Investment Tokens by reference to securities, derivatives and substantially similar rights and obligations, and its updated Crypto Token framework took effect on 12 January 2026 [12-13]. Abu Dhabi Global Market provides a DLT Foundations framework while requiring separately regulated financial activities to have the necessary permission [14]. Dubai Land Department launched a regulated real-estate tokenisation pilot in 2025 and announced a controlled secondary-resale phase for February 2026 [15-16]. These regimes and projects are not interchangeable. A use case needs a written perimeter analysis for the asset, activity, entity, location, client and settlement arrangement.

The paper defines a **programmable-finance stack** as the governed set of legal, data, identity, token, custody, settlement, workflow, AI, reconciliation and oversight components through which a right can be created, held, transferred, serviced and extinguished. The definition is technology-neutral. A permissioned ledger, a public network, a conventional database or a hybrid can support parts of the stack. The selection follows requirements and evidence.

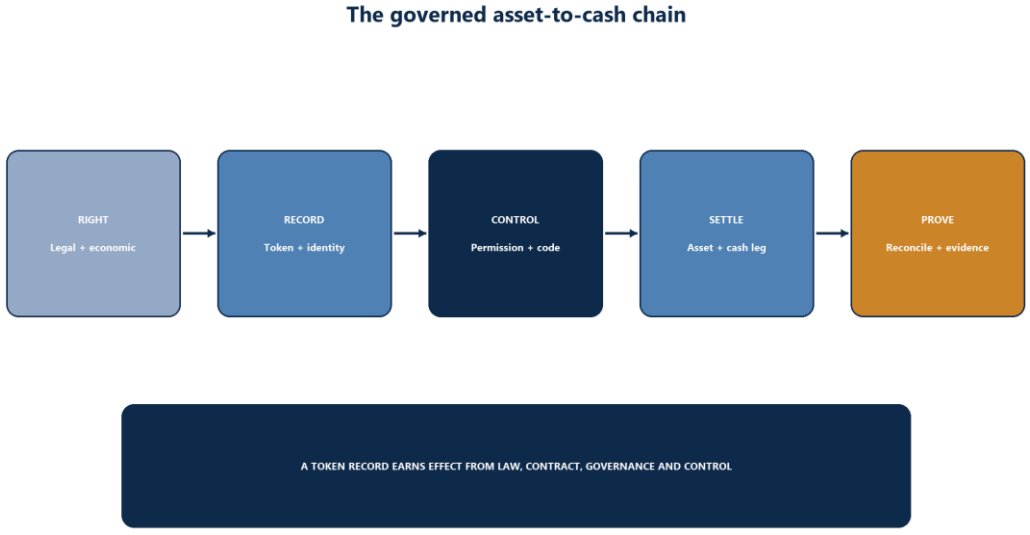

Figure 1. The governed asset-to-cash chain

Source: Matchpoint evidence framework; tokenisation, settlement and legal context [1-19].

The contribution is a practical framework. It provides:

- an A4 and A2 decision perimeter;
- a rights-to-record taxonomy;
- a minimum programmable asset object;
- a before-and-after operating workflow;
- a controlled architecture for identity, custody, token state, settlement and reconciliation;
- a bounded role for AI in extraction, monitoring and exception operations;
- lifecycle and release gates;
- unverified illustrative infrastructure and family-office scenarios;
- an evidence-gated productivity and value bridge; and
- a ninety-day adoption roadmap.

The analysis reviews 40 primary, authoritative and clearly labelled sources available through 1 August 2026. Regulatory applicability depends on entity, jurisdiction, licence, activity and client. Academic smart-contract studies are reported within their technical settings. No approved observed Matchpoint or client evidence was supplied for T26 revenue, cash cost reduction, loss reduction or alpha. Those attributed values therefore remain USD 0.

2. WHAT IS BEING TOKENISED?

2.1 The token is one record in a rights system

A sound design begins with a sentence that can be tested: **the token represents X, against Y, under Z law and documents, with these holder rights, restrictions and remedies**. Without that sentence, a technical team can build a transferable object before the sponsor has resolved the economic and legal object.

The Law Commission's digital-assets work distinguishes digital objects from the rights or things to which they may be linked and supports legal recognition of certain digital assets as property [18]. The UK Jurisdiction Taskforce's legal statement analyses cryptoassets and smart contracts under English law while stressing that consequences depend on facts and legal arrangements [19]. UNCITRAL's Model Law on Electronic Transferable Records uses technology-neutral concepts of identity, integrity and control for records that are functionally equivalent to transferable documents or instruments [17]. None of these sources makes every token a security, title document, deposit or property right. They demonstrate why the mapping must be explicit.

Possible object	What the token may record	Authoritative evidence	Central diligence question
Digital security	Share, note, fund unit or derivative right	Issuance documents, register, law	Does the token constitute or update the legally authoritative record?

Possible object	What the token may record	Authoritative evidence	Central diligence question
Beneficial interest	Contractual or trust interest in an asset vehicle	Trust, nominee, subscription and register records	What rights exist against trustee, nominee or issuer?
Asset participation	Economic exposure under a contract	Participation agreement and payment waterfall	Is the holder exposed to the asset, issuer or both?
Payment token	Claim or instrument used for payment	Issuer terms, reserve and regulatory status	Who owes redemption and how is value protected?
Electronic document	Transferable record such as an electronic bill	Applicable law, reliable system and control	Does functional equivalence apply to this instrument?
Digital receipt	Evidence that an off-chain event occurred	Source-system record and verification	Is the token evidence, or is it the right itself?
Governance token	Voting or protocol participation	Constitution, charter or contract	Are votes binding and who implements them?
Identifier	Reference to an asset or data object	Authoritative registry and mapping	Can the mapping change without token-holder consent?

2.2 Four layers of truth

A project should distinguish four layers:

1. **Legal truth:** the rights, obligations, remedies and governing law created by legislation and documents.
2. **Registry truth:** the record designated as authoritative for holder, quantity, status and restrictions.
3. **Operational truth:** the systems used for identity, payments, servicing, accounting and reporting.
4. **Ledger truth:** the current state recorded by the selected token or distributed-ledger system.

The layers can be aligned. They are not automatically identical. A blockchain transaction may be final under protocol rules and reversible under a court order or contractual correction process. A token transfer may be technically valid and legally restricted. A corporate action may be recorded on-chain while payment occurs through conventional accounts. A custodian's books may determine a client's beneficial position while an omnibus wallet is the on-chain holder.

Mismatch	Example	Consequence	Required control
Legal versus ledger	Transfer to an ineligible holder	Defective or restricted holding	Eligibility check, freeze and correction procedure
Registry versus ledger	Issuer register not updated	Disputed ownership or servicing	One authoritative-record rule and reconciliation
Cash versus asset	Token delivered before funds are final	Principal or replacement-cost exposure	Coordinated DvP and settlement-finality analysis
Custody versus ledger	Key moved without client-book update	Client asset mismatch	Wallet-to-books reconciliation and dual control
Oracle versus source	Incorrect project milestone submitted	Wrong distribution or covenant state	Signed source, challenge window and override
AI versus document	Extracted clause changes a threshold	Incorrect automated rule	Human approval against source passage

2.3 Rights-first token specification

The specification should be approved before code. It should state the issuer or obligor, the underlying asset, holder entitlement, seniority, cash-flow formula, voting rights, information rights, transfer restrictions, eligible holders, issuance authority, redemption or maturity, default treatment, dispute forum, registry status, custodian structure, tax responsibilities and amendment process.

The European Union DLT Pilot Regime permits defined DLT market infrastructures under specific permissions and conditions [9]. MiCA regulates specified crypto-assets and service providers while financial instruments remain within other EU financial-services law [10]. The DFSA Investment Token definition similarly focuses on the rights and obligations represented [12]. Classification follows substance, jurisdiction and activity. The project should not begin with a marketing label such as real-world asset, utility token or digital twin and treat the label as a legal conclusion.

3. THE A4 AND A2 DECISION PERIMETER

3.1 A4 infrastructure and digital-infrastructure investors

A4 investors can use programmable records across origination, construction, operations, financing, transfer and exit. A data-centre investment, for example, can involve land or lease rights, construction contracts, equipment, grid connection, power purchase arrangements, capacity reservations, customer contracts, insurance, debt, hedging and operating accounts. Tokenising one economic interest does not compress these relationships into a single asset.

The most credible near-term use cases are bounded and evidence-rich:

- controlled investor or lender registers;
- project-document and obligation records;
- permissioned transfer of notes or participation interests;
- milestone evidence and drawdown workflows;
- cash-flow allocation and distribution calculations;
- collateral or asset-register references;
- consent and voting workflows;
- secure reporting and data-room entitlements; and
- reconciliation among issuer, agent, custodian, administrator and investor.

Common A4 questions include:

- Which legal right is represented and where is it enforceable?
- Does the digital record control the register, or mirror another register?
- Which infrastructure milestone can change a payment, draw or distribution?
- Who verifies the physical and contractual event supplied to the ledger?
- Which form of money settles the transaction and when is it final?
- Can keys, permissions and service operations survive an incident or vendor failure?
- How are lenders, investors, regulators, courts and insolvency officials accommodated?

3.2 A2 family-office CIOs and heads of alternatives

A2 investors encounter tokenisation as allocators, direct investors, co-investors, note holders, fund investors or clients of a private bank or external asset manager. Their starting point is the investment mandate. The technology can change access, denomination, servicing or transfer mechanics. It does not establish suitability, diversification, liquidity, custody quality or fair value.

Common A2 questions include:

- Is the holding a direct asset, security, fund interest, note, participation or contractual claim?
- Which entity owes the payment, and what assets support the obligation?
- What rights exist if the platform, issuer, custodian or key provider fails?
- Does a displayed secondary market have committed liquidity, executed volume or only indications?
- How are valuation, fees, taxes, sanctions and source-of-wealth controls handled?
- Can the family office consolidate the asset into accounting, risk and performance systems?
- Which committee approves allocation, custody, concentration and exceptions?

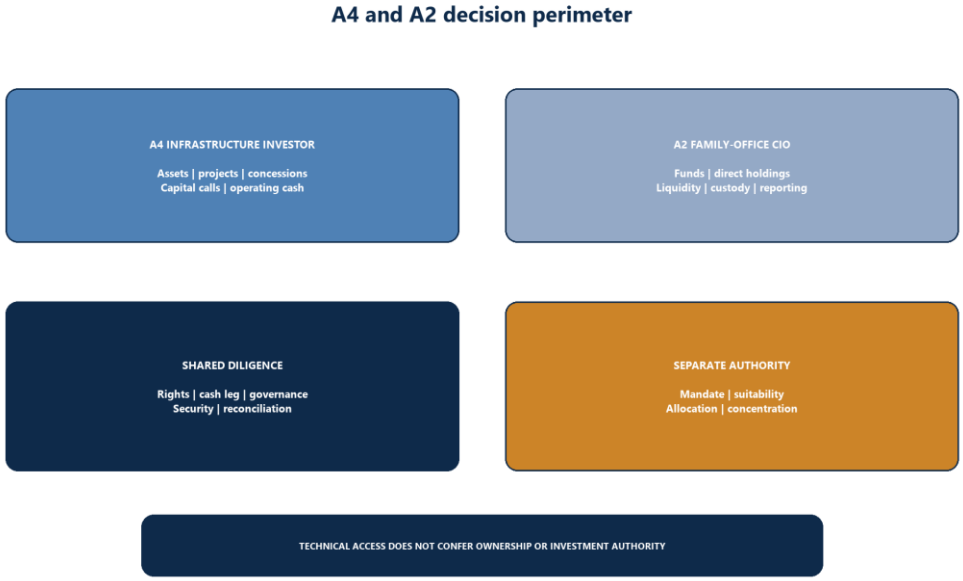

Figure 2. A4 and A2 decision perimeter

Source: Matchpoint ICP and decision-rights framework.

3.3 Shared diligence and separate authority

Dimension	A4 investor	A2 family office	Shared gate
Primary objective	Finance and govern an infrastructure asset	Allocate and preserve family capital	Defined investment and operating purpose
Underlying evidence	Project, concession, contract and operating data	Offering, manager, custodian and portfolio data	Verified source and rights mapping
Decision authority	Investment committee, lender or asset board	CIO, investment committee or family governance body	Named authority and limits
Token use	Issuance, monitoring, servicing or transfer	Subscription, holding, transfer and reporting	Lifecycle design
Cash concern	Draws, debt service, revenue and distributions	Funding, income, redemption and liquidity	Settlement and reconciliation
Failure concern	Project, operator, oracle, code and counterparty	Issuer, platform, custodian, key and liquidity	Recovery and fallback
AI concern	Source extraction and operating monitoring	Diligence, reporting and exception review	Human approval and model governance

An adviser working across capital providers, issuers and technology vendors should set the engagement perimeter and conflicts process before data or transaction design. Access to a token dashboard does not establish entitlement to confidential asset information. A shared platform does not merge fiduciary duties, client classifications or investment authority.

4. THE PROGRAMMABLE ASSET OBJECT

4.1 Minimum object model

Programmability requires structured objects. The token identifier is only one field. A minimum object should connect the digital record to the source right and to every controlled lifecycle event.

Object field	Minimum content	Approval owner	Failure if absent
Asset identity	Issuer, vehicle, project, instrument and unique identifier	Issuer or administrator	Wrong asset or duplicate supply
Source right	Document, clause, governing law and authoritative register	Legal owner	Unclear legal effect
Holder entitlement	Cash, vote, information, transfer and remedies	Issuer and counsel	Misstated investor rights

Object field	Minimum content	Approval owner	Failure if absent
Quantity and supply	Authorised amount, issued amount and unit	Issuance authority	Over-issuance or unit error
Eligibility	Investor type, jurisdiction, sanctions and mandate rules	Compliance and distributor	Ineligible transfer
State	Created, issued, restricted, pledged, frozen, redeemed or cancelled	Administrator	Invalid lifecycle transition
Cash-flow rule	Formula, currency, date, source and rounding	Finance or calculation agent	Incorrect payment
Permission	Who can issue, transfer, pause, amend and burn	Governance body	Excess privilege
Custody	Wallet, key model, books, beneficial owner and recovery	Custodian	Asset loss or books mismatch
Settlement	Money form, accounts, reservation, finality and fallback	Settlement owner	Principal risk
Evidence	Signatures, timestamps, source links and audit records	Control owner	Unprovable state
Version	Contract, code, model and data version	Change authority	Silent rule change

4.2 Identity and eligibility

Permissioned finance needs a reliable relation among legal person, account, wallet, role and entitlement. A wallet address alone does not show beneficial owner, signing authority, sanctions status, investor classification or mandate. The identity layer can use an approved credential, registry or account system. It should expose the minimum information required to execute a rule while keeping full evidence with the accountable provider.

Eligibility can change. A credential can expire. A beneficial owner can change. A sanctions status or residency can require review. The transfer rule should define whether a stale credential blocks, quarantines or routes a transaction for manual review. It should record which version of the rule and credential produced the result.

4.3 Permissions and privileged actions

Programmability concentrates authority in code paths and administrator keys. The design should enumerate privileged actions and separate initiation, approval and execution where material.

Privileged action	Minimum control	Evidence retained
Mint or issue	Authorised supply, signed instruction and dual approval	Issuance document, approval and transaction
Transfer override	Defined legal basis and independent approval	Reason, authority, prior and new state
Freeze	Permitted trigger, expiry and review	Trigger, owner, scope and review date
Upgrade	Tested code, impact assessment and notice	Diff, audit, approvals and rollback
Oracle replacement	Source validation and continuity plan	Prior source, new source and reconciliation
Key recovery	Identity proof, quorum and delay	Recovery request and approvals
Redemption	Entitlement, cash confirmation and burn control	Payment, register and final token state
Emergency pause	Defined incident threshold and named authority	Incident, duration, communication and restart

Smart-contract research has documented classes of implementation and semantic vulnerabilities. Luu and co-authors used symbolic execution to identify vulnerabilities in Ethereum contracts [27]. Kalra and co-authors developed a formal-analysis framework for safety and fairness properties [28]. Atzei and co-authors classified programming pitfalls and attack patterns [29]. The precise technologies and historical datasets differ from a current institutional implementation. The durable control lesson is that code execution can faithfully perform flawed logic. Business intent, legal constraints, formal properties, testing, independent review, upgrade control and incident response should be connected.

5. BEFORE AND AFTER OPERATING WORKFLOW

5.1 Before: fragmented asset administration

A conventional private-asset workflow can involve subscription documents, spreadsheets, administrator books, bank payments, email approvals, manual eligibility checks, separate custody records and periodic investor reports. Each

component may be controlled. Friction appears at the hand-offs. Parties re-key the same identity, asset, cash and allocation data. Settlement follows sequential confirmations. Corporate actions require repeated reconciliation. Exceptions can remain in email.

The World Bank's 2018 bond-i created, allocated, transferred and managed a bond through its lifecycle on a blockchain platform while cash settlement remained through conventional arrangements [20]. The European Investment Bank's 2021 digital bond used a public blockchain for bond tokens and a central-bank digital-currency representation for the issue-money leg within the transaction arrangement [21]. These examples show that asset and cash architecture can evolve at different speeds.

5.2 Controlled target workflow

A controlled target state establishes the right and authoritative register first, validates holder eligibility, creates or transfers the asset record, coordinates the cash leg, records finality, updates books and services the position from shared evidence. It keeps manual authority where interpretation, exception or legal action is required.

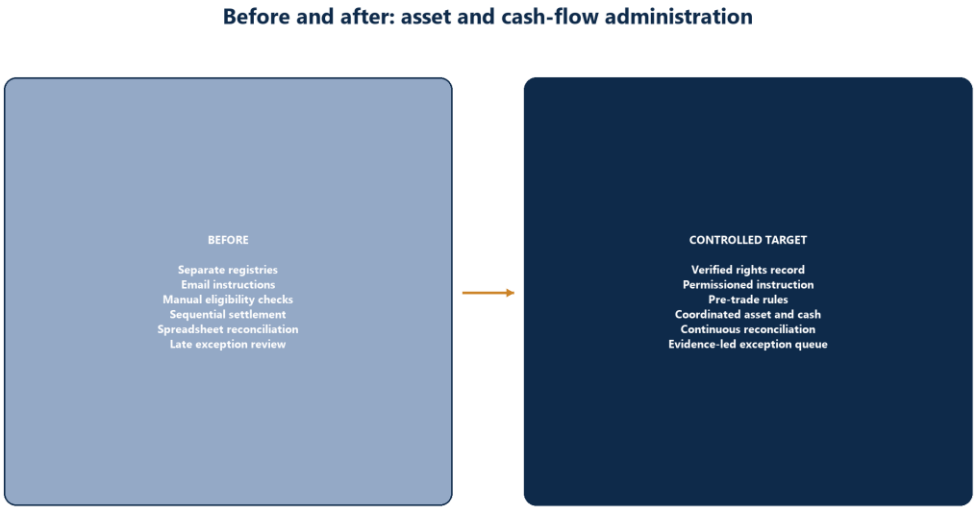

Figure 3. Before and after: asset and cash-flow administration

Source: Matchpoint operating-model framework; institutional pilot context [3-4,20-23].

Stage	Fragmented baseline	Controlled target	Release evidence
Onboarding	Repeated forms and files	Reusable approved identity reference	Identity-provider and privacy approval
Eligibility	Manual pre-transfer check	Rule plus human exception path	Rule tests and current credentials
Issuance	Separate document and register updates	Signed instruction linked to controlled mint	Supply and register reconciliation
Funding	Bank instruction after allocation	Reserved or coordinated cash leg	Finality and failure tests
Transfer	Sequential broker, custodian and registrar messages	Permissioned transfer with evidence	Legal effect and holder-book update
Servicing	Spreadsheet calculations and email notices	Controlled lifecycle calculation and notice	Independent calculation and exception review
Reporting	Periodic aggregation	Current position and evidence view	Books, ledger and cash reconciliation
Correction	Bilateral investigation	Governed correction or compensating entry	Legal authority and immutable audit trail

The target is not zero human involvement. The target is fewer unowned hand-offs, less duplicate entry, earlier exception visibility and a complete evidence chain. These outcomes require observed baseline and target measures before any productivity claim.

6. CONTROLLED STACK ARCHITECTURE

6.1 Layer 1: legal and product definition

The legal layer establishes the instrument, issuer, holder rights, register, governing law, offer and distribution perimeter, servicing obligations, insolvency treatment, dispute process and amendment authority. It also determines which events can be executed automatically and which require judgement or formal action.

The relevant authority depends on the case. CBUAE regulates Payment Token Services within the scope of Circular 2/2024 [11]. DFSA rules address Investment Tokens and Crypto Tokens in or from the DIFC [12-13]. ADGM's DLT Foundations framework provides a legal structure for certain DLT organisations while distinguishing financial activities requiring Financial Services Permission [14]. DLD's projects concern defined real-estate tokenisation arrangements in Dubai [15-16]. EU DLT and crypto-asset frameworks have their own perimeter [9-10]. The correct architecture therefore carries a jurisdiction and permission matrix rather than a generic regulatory-compliant flag.

Perimeter question	Required answer	Evidence owner
What is the asset or claim?	Legal classification and economic substance	Product counsel
Who issues or owes it?	Legal entity, capacity and authorisation	Issuer board and counsel
Where is the activity conducted?	Entity, client, system and marketing locations	Regulatory counsel
Who may acquire or hold it?	Investor, jurisdiction and distribution restrictions	Compliance
Who provides custody or transfer?	Provider, licence, client-asset model and delegation	Custody owner
What money is used?	Legal nature, issuer, redemption and regulatory status	Treasury and counsel
Which record is authoritative?	Register rule and correction authority	Registrar or administrator
What happens in insolvency?	Claim, segregation, control and enforcement analysis	Insolvency counsel

6.2 Layer 2: identity, permission and privacy

The identity layer maps approved legal persons to roles and technical accounts. It should support beneficial ownership, signing authority, investor classification, sanctions controls, jurisdiction, transfer eligibility and credential expiry. Personal data should be minimised, purpose-limited, protected and retained under the applicable regime. UAE federal, DIFC and ADGM data-protection regimes apply according to facts and location [36-38].

Public visibility can conflict with investor confidentiality. A design can keep transaction proofs or pseudonymous positions on a ledger while maintaining identity and sensitive documents in controlled systems. Pseudonymisation is not necessarily anonymisation. Linkage, wallet reuse, transaction patterns and external data can reveal an actor. A privacy impact assessment should cover participants, observers, validators, vendors, analytics providers and cross-border access.

6.3 Layer 3: token state and lifecycle logic

The token layer records identifiers, balances, restrictions and lifecycle state. Widely used technical interfaces can improve portability, yet an interface standard does not establish business semantics. EIP-20 specifies a token interface for balances, transfer and approvals [25]. EIP-712 specifies typed structured-data hashing and signing [26]. An institutional implementation needs additional rules for issuance authority, eligible holders, corporate actions, correction, pause, upgrade, data retention and recovery.

State transitions should be finite and testable. A token should not move directly from any state to any other state. An issued token can become pledged or frozen under defined authority. A matured or redeemed token should not transfer. A cancelled issuance should preserve historical evidence. Every transition should record the initiating instruction, rule version, approvals and resulting register state.

6.4 Layer 4: custody and key operations

Custody architecture answers who controls the signing keys, how client entitlement is recorded, how instructions are authenticated, how assets are segregated, how keys are backed up or recovered and how the position survives provider failure. Institutional controls can include hardware security modules, multi-party computation, multi-signature approvals, whitelists, rate limits, time delays and independent books.

Custody model	Benefit	Material risk	Minimum diligence
Direct self-custody	Investor controls keys	Loss, compromise and weak succession process	Governance, recovery, security and operational capacity

Custody model	Benefit	Material risk	Minimum diligence
Regulated custodian	Professional control and books	Provider, sub-custodian and omnibus risk	Licence, segregation, liability, audits and recovery
Platform custody	Integrated user experience	Concentrated platform and conflict risk	Legal status, client assets, permissions and exit
Multi-party control	Reduced single-key dependence	Coordination, implementation and vendor risk	Quorum, liveness, recovery and independent testing
Hybrid	Role-specific control	Complex responsibility and reconciliation	End-to-end responsibility map

Family offices require succession-ready key governance. An investment cannot depend on one executive's device, seed phrase or undocumented vendor relationship. Infrastructure vehicles require continuity across a longer asset life than many technology firms. The operating plan should cover personnel change, custodian substitution, network migration and archival access.

6.5 Layer 5: cash and settlement

An asset transfer and payment are separate obligations until the arrangement connects them. Delivery versus payment seeks to make securities delivery conditional on payment. Payment versus payment applies the same principle to two currency legs. Atomic execution at a technical layer can reduce one form of principal risk while introducing dependence on platform rules, liquidity, availability and the legal status of the settlement asset.

The BIS unified-ledger work places tokenised central bank reserves, commercial bank money and tokenised assets in a common programmable architecture [2-3]. Project Agora's 2026 prototype joined eight central banks and more than 40 regulated institutions and demonstrated specified wholesale cross-border payment functions in its test setting [3]. The project states that it delivered a prototype and plans further real-value testing. Its results should not be converted into a claim that an A4 or A2 transaction can use the same arrangement today.

The Eurosystem trials and experiments explored wholesale central-bank-money settlement for DLT transactions [4]. CPMI-IOSCO principles favour settlement in central bank money where practical and available and require strict controls where commercial bank money is used [5]. A payment token can add programmability and requires analysis of issuer, redemption, reserves, supervision and settlement finality [6,11].

Settlement asset	Claim on	Key diligence	Typical residual risk
Central bank money	Central bank	Access, operating hours, system and legal finality	Availability and integration
Tokenised commercial bank deposit	Commercial bank	Deposit nature, bank risk, ledger and redemption	Bank credit and interoperability
Conventional bank transfer	Commercial bank	Payment finality, cut-off, matching and reversals	Timing and reconciliation
Regulated payment token	Token issuer	Licence, reserve, redemption, custody and acceptance	Issuer, run and market risk
Unbacked cryptoasset	Market value	Volatility, liquidity, custody and permissibility	Price, market and operational risk

6.6 Layer 6: oracle, workflow and reconciliation

Infrastructure finance depends on off-chain facts: construction completion, equipment delivery, grid connection, utilisation, customer acceptance, power consumption, insurance status and financial covenant values. An oracle does not make the fact true. It transports an assertion from a source into a decision system.

Every material oracle should have a named source, accountable signer, timestamp, evidence link, challenge period, correction method, fallback and liability allocation. High-impact events can require two independent sources or an approved professional certificate. A sensor can provide data and still require calibration, secure identity and exception handling.

DTCC's Smart NAV pilot explored distributing structured mutual-fund price and rate data across blockchain environments and emphasised standard roles, data routing and chain-agnostic delivery [23]. The result supports the proposition that trusted reference data can be made available to multiple programmable uses. It does not establish that any asset valuation or project fact becomes reliable simply because it is published on-chain.

Reconciliation remains a first-class layer. The stack should compare authorised supply, ledger balances, registrar positions, custodian books, beneficial-owner records, bank cash, general ledger, payments, fees and servicing events. A break receives an owner, severity, reason, ageing and resolution. A ledger described as a single source of truth can still disagree with the legal register, an external payment system or an incorrectly configured smart contract.

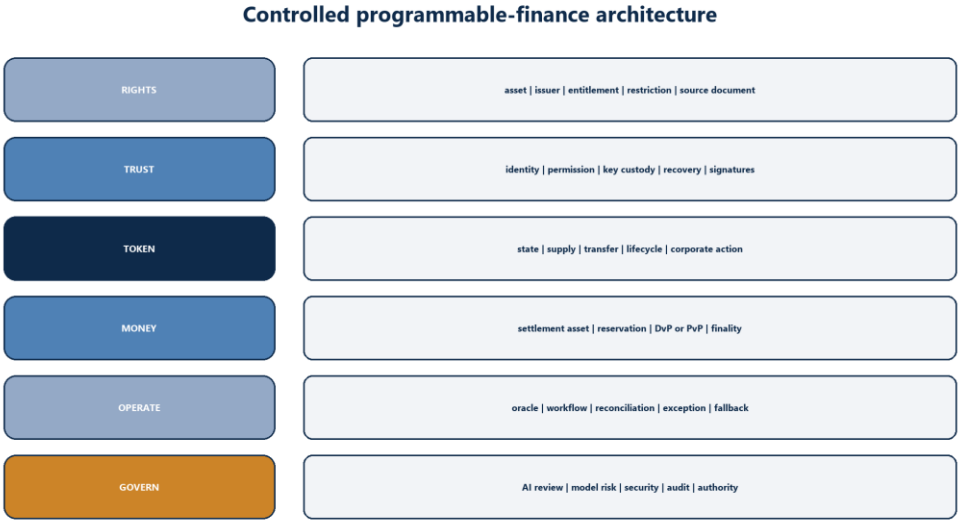

Figure 4. Controlled programmable-finance architecture

Source: Matchpoint architecture; market-infrastructure, security and governance context [1-14,24-40].

7. THE ROLE OF ARTIFICIAL INTELLIGENCE

7.1 Suitable assistance roles

AI can provide material operational assistance when source rights, intended use and review are defined. Suitable roles include:

- extracting candidate fields and clauses from offering, financing and project documents;
- comparing a structured term with the signed source passage;
- classifying notices, investor requests and operational evidence;
- matching bank, custodian, registrar and ledger records;
- detecting duplicate, missing, stale or unusual lifecycle events;
- monitoring project evidence and preparing exception packs;
- retrieving approved policies and producing a cited review draft;
- translating controlled communications while preserving the source text; and
- supporting service operations through bounded workflows.

The NIST AI Risk Management Framework organises AI risk management through Govern, Map, Measure and Manage functions [30]. The revised US interagency model-risk guidance emphasises risk-based governance, validation, monitoring and vendor-model responsibilities [31]. IOSCO's capital-markets AI report identifies use cases alongside model, data, third-party, concentration, cyber, manipulation and governance risks [32]. Applicability differs by institution and jurisdiction. The principles support a control record for AI functions in programmable finance.

7.2 Prohibited or separately authorised roles

The T26 architecture excludes autonomous authority over:

- legal classification or enforceability;
- investor eligibility or suitability exceptions;
- issuance beyond approved supply;
- movement of client assets or cash;
- smart-contract upgrade or emergency override;

- valuation approval;
- investment allocation, concentration or exit;
- lender enforcement or waiver;
- sanctions disposition; and
- regulatory, accounting, tax or legal conclusions.

An AI system can prepare evidence for these decisions. A named person or body with current authority approves the result. The system should technically prevent the AI service account from acquiring signing, minting, cash-transfer or upgrade privileges.

7.3 Document extraction requires a source-to-field control

Financial documents contain definitions, cross-references, schedules, amendments and negotiated exceptions. A language model can extract an apparently clear percentage from the wrong clause or miss that an amendment replaced it. Every material field should preserve:

Control field	Required content
Source identity	Signed document, version, date and hash or immutable reference
Passage	Exact page, clause or structured range supporting the field
Candidate value	Extracted text and normalised value
Confidence state	Accepted, uncertain, conflicted or missing
Reviewer	Named authorised person and timestamp
Rule effect	Which workflow or calculation uses the field
Change control	Amendment, impact, reapproval and effective date

The production rule should fail closed for a material missing or conflicted field. The workflow should create a review task and avoid silently selecting a convenient value.

7.4 AI monitoring and anomaly detection

AI can prioritise reconciliation breaks or operating anomalies. Evaluation should reflect the decision. A rare-event detector with high apparent accuracy can still overwhelm the team with false alerts. A text classifier can drift when document formats or counterparties change. A generative assistant can produce unsupported explanations.

The release scorecard should cover completeness, extraction accuracy by field, reason traceability, alert precision, missed material events, reviewer burden, segment performance, stability, override, latency and incident behaviour. Test sets should be independent of development data and include amendments, poor scans, multilingual documents, conflicting clauses, missing evidence and adversarial instructions embedded in source material.

7.5 Data, model and vendor boundaries

The AI control record should include intended use, prohibited use, model and version, provider, hosting, input data, retention, training use, access, evaluation, monitoring, incident process and exit. Proprietary services require evidence proportionate to their role. A vendor statement that data are secure or a model is accurate is not validation.

NIST's Secure Software Development Framework provides practices for preparing the organisation, protecting software, producing well-secured software and responding to vulnerabilities [33]. AI components should enter the same software inventory, secure-development, dependency, test, release and incident processes as other production components.

8. LIFECYCLE CONTROL

8.1 Creation and issuance

Creation begins after product, legal, regulatory, supply and technology approval. The issuance instruction should identify the authoritative source, quantity, currency, price, eligible recipient, cash condition and approvers. Code should enforce the authorised supply ceiling. The registrar and general ledger should reconcile after issuance.

An unallocated token, test token or failed transaction requires explicit treatment. Production and test networks should be separated. Addresses should be verified independently. A mint transaction should not be treated as a completed issue until holder eligibility, register state and cash condition are satisfied.

8.2 Holding, pledging and restriction

The holding phase includes custody, reporting, income, votes, notices, tax documentation, sanctions monitoring and changes in beneficial ownership. A pledge can restrict transfer while leaving economic ownership with the pledgor. The token state should reference the controlling legal arrangement and avoid representing a technical lock as a complete security-interest analysis.

8.3 Transfer and settlement

A transfer instruction should validate holder identity, recipient eligibility, available balance, restrictions, approvals, price or consideration, cash readiness and finality conditions. A rejected or expired transfer should preserve the attempted instruction and reason without changing ownership.

The EU DLT Pilot Regime creates a controlled legal path for authorised DLT market infrastructures in its scope [9]. IOSCO recommendations address custody, market integrity and operational risks [7-8]. A bilateral private transfer outside a trading venue has a different perimeter. The project should map every actor and activity rather than import an infrastructure label.

8.4 Servicing and corporate actions

Interest, distributions, calls, votes, conversions, waivers and information rights require a record date, eligible position, calculation source, tax treatment, payment instruction, exception process and proof. Programmable execution can reduce repeated manual steps. It can also distribute an error to every holder consistently. Independent calculation, tolerance checks and pre-release review remain appropriate for material payments.

8.5 Redemption, maturity and archival evidence

Redemption connects entitlement, payment and final token state. The system should prevent a token from being paid twice, transferred after redemption or destroyed before cash and register confirmation. The archive should retain the legal documents, approvals, transaction evidence, final holder record, payment proof, code and rule versions and resolved exceptions for the required period.

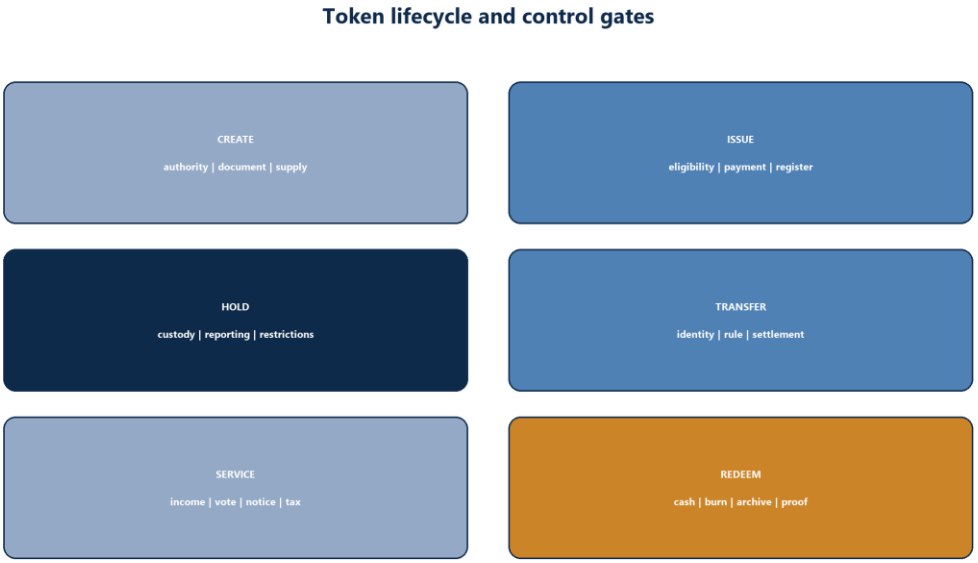

Figure 5. Token lifecycle and control gates
Source: Matchpoint lifecycle framework; rights and technical standards context [9-19,24-29].

9. RELEASE GATES AND FAILURE MODES

9.1 Legal and regulatory gate

The gate requires written answers on asset classification, issuer authority, offer and distribution, holder eligibility, register status, custody, payment, data, governing law, insolvency and dispute resolution. The answer should identify uncertainties and required approvals. A legal memorandum prepared for one structure should not be reused as a generic tokenisation opinion.

9.2 Settlement and reconciliation gate

The asset and cash legs should be tested under normal, delayed, partial and failed conditions. The team should know when each leg becomes final, which party carries exposure during any gap and how a mismatch is resolved. Reconciliation should detect excess supply, missing cash, duplicate instruction, wrong currency, stale position and books-to-ledger disagreement.

9.3 Security and privileged-access gate

The security gate covers code review, threat modelling, dependency inventory, key generation, storage, signing policy, segregation, privileged roles, upgrade, pause, recovery, penetration testing, monitoring and incident response. Smart-contract findings should be mapped to business invariants such as no unauthorised mint, no transfer to ineligible holder, no payment beyond entitlement and no silent upgrade [27-29].

9.4 Operational-resilience gate

The Basel Committee's operational-resilience principles address governance, operational-risk management, business continuity, mapping of interconnections, third-party dependency, incident management and resilient ICT [34]. The EU Digital Operational Resilience Act establishes requirements for in-scope financial entities on ICT risk, incidents, testing and third-party risk [35]. The precise legal application requires analysis. The operating design should still map critical operations, impact tolerances, dependencies, fallback and recovery.

Failure	Immediate risk	Detection	Controlled response
Ledger unavailable	Transfer or servicing interruption	Availability and queue monitoring	Manual fallback or deferred processing under policy
Settlement asset unavailable	Principal risk or failed completion	Cash-leg status	Cancel, reserve or reroute under approved rules
Oracle conflict	Wrong lifecycle action	Source comparison and tolerance	Pause affected action and human review
Key compromise	Unauthorised instruction	Signing anomaly and access alert	Pause, revoke, recover and investigate
Contract defect	Incorrect state transition	Invariant and reconciliation break	Pause, correction authority and controlled upgrade
AI extraction error	Wrong term or eligibility input	Source-to-field review and sampling	Reject output, correct and evaluate impact
Custodian failure	Access or client-asset uncertainty	Provider and books monitoring	Recovery, substitution and legal process
Vendor exit	Unsupported component	Contract and viability monitoring	Export, migrate and invoke continuity plan
Privacy incident	Unauthorised disclosure	Security and data monitoring	Contain, assess, notify and remediate as required

9.5 Market and investor-protection gate

Fractional denomination can widen access and create the appearance of liquidity. Liquidity requires willing buyers and sellers, permissible transfer, reliable pricing, market-making capacity, custody and settlement. A platform screen is not evidence of executable depth. The investment paper should distinguish contractual redemption, committed liquidity, historical executed volume, indicative quotes and no-liquidity assumptions.

The FSB's risk analysis and IOSCO recommendations support attention to leverage, interconnectedness, conflicts, custody, manipulation, disclosure and operational risk [1,7-8]. A family-office decision should include concentration, look-through exposure, valuation, fees, exit routes and downside under platform or issuer distress.

10. TWO UNVERIFIED ILLUSTRATIVE SCENARIOS

10.1 Scenario A: A4 digital-infrastructure participation

[Unverified illustrative management scenario.] A Gulf data-centre vehicle considers issuing a permissioned digital participation to professional investors. The participation references a contractual right to defined distributions from the vehicle. It does not convey title to the land, servers, customer contracts or power assets. The vehicle remains the obligor. Transfer is restricted to approved investors. Cash moves through regulated bank accounts. The token record coordinates the investor register and lifecycle notices.

The use case could be structured through the following evidence objects:

Object	Unverified illustrative design	Required real evidence
Underlying	Data-centre vehicle participation	Executed participation and vehicle documents
Cash flow	Defined distributable cash formula	Audited accounts, bank records and approved calculation
Milestones	Energisation, customer acceptance and capacity	Independent certificates and source-system evidence
Holder	Professional investor with approved credential	KYC, eligibility and beneficial-owner records
Token state	Issued, held, restricted, pledged or redeemed	Approved smart-contract specification and test evidence
Settlement	Bank-money subscription and distribution	Account, finality and reconciliation design
AI role	Extract terms, compare certificates, prepare exceptions	Evaluation and human approval record
Authority	Vehicle board, administrator and authorised signers	Delegations, permissions and governance documents

The scenario begins with a conventional legal instrument and register analysis. A token can then become the authoritative register, a legally recognised record or an operational mirror according to the approved structure. Project evidence reaches the workflow through signed sources. AI can compare a certificate with the required milestone and flag inconsistencies. It cannot declare construction complete, authorise a draw or move money.

The scenario should be stopped or redesigned if the rights cannot be stated clearly, the transfer perimeter is unresolved, cash and asset finality cannot be coordinated, the operating parties cannot reconcile positions, or the asset vehicle lacks a continuity plan longer than the technology contract.

10.2 Scenario B: A2 family-office allocation and reporting

[Unverified illustrative management scenario.] A family office evaluates a tokenised note that references a portfolio of Gulf infrastructure exposures. The note issuer promises payments under its terms. The family office does not directly own each project. A platform offers digital subscription, custody and periodic transfer windows. AI prepares a diligence summary and reconciles reported distributions.

The family office should separate five exposures:

1. the credit and structural risk of the note issuer;
2. the performance and valuation of the referenced portfolio;
3. the custody and key-control arrangement;
4. the availability and integrity of the platform; and
5. the actual liquidity of the permitted transfer mechanism.

Committee question	Unverified scenario input	Approval evidence required
Mandate fit	Classified as alternatives allocation	Current mandate and adviser review
Economic exposure	Portfolio-linked note	Terms, waterfall and underlying schedule
Downside	Issuer and asset losses possible	Stress analysis and legal priority
Liquidity	Periodic transfer window	Executed volume, eligible buyers and restrictions
Custody	Third-party digital-asset custodian	Licence, segregation, liability and recovery
Valuation	Administrator-provided NAV	Method, frequency, independence and challenge
AI output	Draft diligence and exception list	Source citations, validation and human sign-off
Concentration	Within proposed private-asset bucket	Verified consolidated portfolio data

The CIO should treat AI output as a review aid. Every material statement should link to the offering memorandum, custody terms, audited information or current regulatory evidence. Unknowns should remain unknowns. A recommendation should not be generated from missing documents or vendor marketing material.

11. WHAT INSTITUTIONAL EVIDENCE DOES AND DOES NOT SHOW

11.1 Evidence matrix

Institutional projects provide useful evidence when the claim is limited to what was tested. The World Bank bond-i demonstrated a legally binding bond lifecycle on a blockchain platform while documenting an off-chain cash leg in the

initial arrangement [20]. The EIB demonstrated a digitally native public-blockchain bond issuance with a central-bank-money representation in the issue settlement arrangement [21]. The Hong Kong Government's first tokenised green bond used a DLT platform for specified primary issuance processes and was settled through the relevant wholesale central-bank digital-currency arrangement [22]. DTCC Smart NAV demonstrated controlled publication of structured fund data for on-chain consumption [23]. Eurosystem work demonstrated wholesale settlement experiments and trials across a broad participant group [4]. Project Agora demonstrated a prototype for tokenised commercial-bank deposits and central-bank reserves in a multi-currency arrangement [3].

Evidence	Supported statement	Statement requiring additional evidence
Bond-i [20]	Bond lifecycle records can be operated on a blockchain in the documented structure	Every bond will settle faster or cost less
EIB digital bond [21]	Public-chain bond tokens and a central-money representation were used in the issuance arrangement	Public networks are suitable for every confidential asset
Hong Kong tokenised green bond [22]	A sovereign issuer completed specified tokenised primary-market processes	Tokenisation creates secondary liquidity or a pricing benefit
DTCC Smart NAV [23]	Trusted structured fund data can be delivered to multiple on-chain applications	All oracle data are correct or manipulation-resistant
Eurosystem work [4]	DLT transactions were tested and trialled with wholesale central-bank-money solutions	The tested solution is generally available to private projects
Project Agora [3]	A multi-currency wholesale prototype demonstrated specified programmable functions	Cross-border tokenised settlement is universally production-ready
DLD projects [15-16]	Dubai conducted a regulated real-estate tokenisation pilot and announced a controlled resale phase	The model applies to every property, investor or jurisdiction

11.2 Scale, liquidity and cost remain separate questions

A successful issuance proves that parties completed a transaction. Commercial scale requires recurring volume, participant capacity, resilience, legal certainty, integration, service operations and sustainable economics. Liquidity requires executable demand and supply. Cost improvement requires a measured baseline, equivalent service scope, transition cost, control cost and observed target performance.

Tokenisation can move costs rather than remove them. Registrar work can become identity, code, credential and reconciliation work. Manual settlement can become liquidity reservation and platform-integration work. A conventional custodian can be replaced by a digital-asset custodian with new key and sub-custody risks. Legacy and token systems can run in parallel for years.

11.3 Compliance remains attached to actors and activities

FATF's risk-based framework for virtual assets and virtual-asset service providers addresses licensing or registration, supervision, customer due diligence, travel-rule implementation and cross-border cooperation [24]. The precise application to a digital security, tokenised deposit, payment token or technology provider depends on the facts and national implementation. The stack should identify the obliged entity, information source, decision point, evidence and escalation for each financial-crime control. Embedding a rule in a smart contract does not transfer regulatory responsibility from the accountable entity.

12. PRODUCTIVITY, REVENUE AND INVESTMENT VALUE

12.1 Productivity must be measured at the accepted-output level

The sheet hook for T26 concerns productivity and revenue for the target business. The evidence standard begins with an approved baseline task and ends with accepted output. A faster draft that requires additional correction has not released capacity. A reconciliation alert that nobody resolves has not improved control. A token transfer that requires parallel manual processing has not reduced end-to-end work.

For a repeated process, define:

Released hours = accepted baseline hours - accepted target hours - incremental review and exception hours

The terms are measured over comparable volume and quality. Setup, migration, control, vendor and parallel-run costs remain separate. Released hours are capacity. Cash cost reduction requires an approved change in paid cost. Revenue requires a contract, invoice, collection and approved attribution.

Measure	Required evidence	T26 attributed value
Processing time	Time records for equivalent accepted outputs	Unverified; USD 0 attributed
Error or break rate	Defined population and independently checked exceptions	Unverified; USD 0 attributed
Settlement time	Final asset and cash timestamps under comparable conditions	Unverified; USD 0 attributed
Released capacity	Approved baseline, target and incremental control time	Unverified; USD 0 attributed
Cash cost reduction	Ledger, vendor and staffing evidence with approved counterfactual	USD 0
Revenue	Signed contract, invoice, collection and causal attribution	USD 0
Loss reduction	Observed incident or credit outcome and approved counterfactual	USD 0
Investment alpha	Approved methodology, benchmark and realised performance	USD 0

12.2 Unverified illustrative productivity bridge

[Unverified illustrative management assumptions.] Consider a monthly asset-servicing process with 100 position and cash records. Assume the baseline requires 30 hours, the controlled target requires 18 hours and additional exception review requires 4 hours. The illustrative released capacity is 8 hours for that month. This arithmetic is not an observed Matchpoint or client result. It creates no attributed cash saving or revenue. A real pilot would record accepted tasks, errors, rework, reviewer time and system cost before a claim is approved.

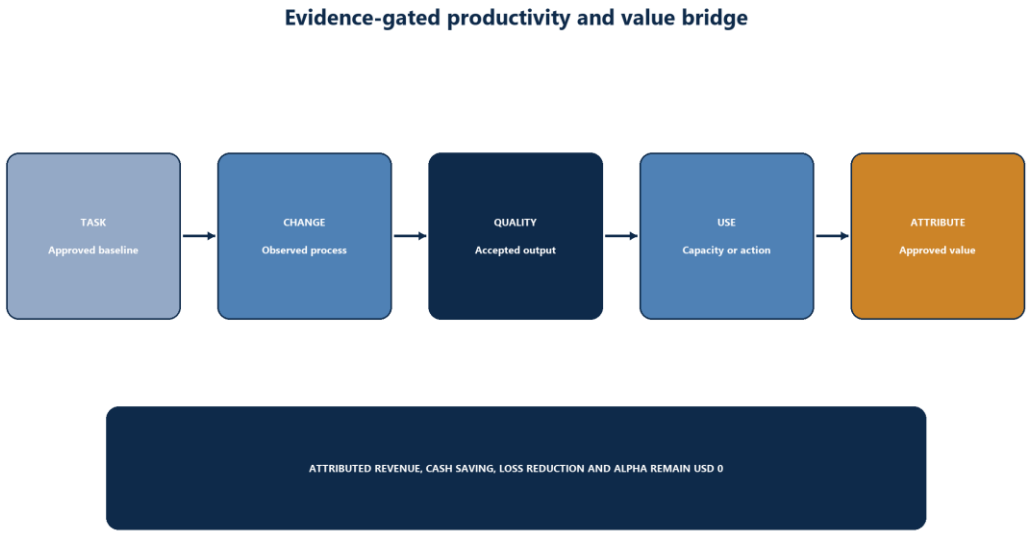

Figure 6. Evidence-gated productivity and value bridge

Source: Matchpoint business-case and attribution framework.

12.3 Revenue architecture for A4 and A2 businesses

Potential revenue mechanisms include issuance or administration fees, asset-management fees, custody fees, data services, origination, distribution and advisory work. Each mechanism requires a real customer, contract, delivery, billing, collection and allocation of direct and control costs. Token denomination can change access and does not prove additional demand. AI-assisted service can change response capacity and does not prove retention or pricing power.

The commercial pilot should therefore track funnel and operating evidence:

Stage	Evidence
Qualified opportunity	Identified customer, use case, authority, budget and timetable
Approved proposition	Legal perimeter, operating scope, price and responsibilities
Signed engagement	Executed contract and permitted claims
Delivered service	Accepted milestone and control evidence

Stage	Evidence
Billed	Invoice linked to the engagement
Collected	Bank or ledger evidence of receipt
Attributed	Approved causal record linking the work to the collection

12.4 Investment value is distinct from operating value

An infrastructure asset can produce investment return through income, growth, leverage, refinancing and exit. Tokenisation can influence access, administration, settlement and transfer. It does not change the underlying asset's operating cash flow unless it enables a separately evidenced operating or financing improvement. Any valuation premium or liquidity discount should be supported through observed transactions and risk analysis.

A2 committees should require the same asset-underwriting evidence for a tokenised exposure as for its conventional equivalent, plus the token stack risks. A4 sponsors should show how the digital arrangement affects the complete capital and operating system, including any new cost, dependency or legal uncertainty.

13. NINETY-DAY ADOPTION ROADMAP

Days 0-15: rights and perimeter

- Select one bounded asset, instrument or administrative workflow.
- State the right, obligor, holder entitlement and authoritative record.
- Map jurisdictions, entities, clients, activities and required permissions.
- Identify custody, cash, data and insolvency questions.
- Record prohibited claims and unresolved legal questions.
- Set investment and operating authority.

Gate 1: the object and perimeter are approved or the project stops.

Days 16-30: objects and control design

- Build the asset, holder, supply, state, cash-flow and evidence objects.
- Define identity, credential, privacy and eligibility controls.
- Enumerate privileged actions and approval quorums.
- Choose the authoritative register and reconciliation model.
- Specify the settlement asset, finality and failure states.
- Define AI intended use, prohibited use and human review.

Gate 2: every material state transition has an owner, authority, evidence and correction path.

Days 31-45: prototype build

- Configure a non-production token and identity environment.
- Implement supply, transfer, restriction, servicing and redemption states.
- Integrate approved test cash and oracle sources.
- Implement books-to-ledger and cash reconciliation.
- Create source-to-field AI extraction with citations.
- Log instructions, approvals, versions and exceptions.

Gate 3: the prototype has no live client asset, cash or decision authority.

Days 46-60: independent testing

- Verify smart-contract business invariants and technical security.
- Test ineligible, duplicate, stale, partial and failed transactions.
- Test key compromise, oracle conflict, vendor loss and ledger outage.
- Validate AI fields against independent labelled documents.
- Test privacy, access, deletion and cross-border-data controls.

- Reproduce reconciliation and evidence from source systems.

Gate 4: material findings are resolved, accepted with explicit controls or cause the project to stop.

Days 61-75: shadow operation

- Run the target process alongside the approved baseline.
- Prevent the prototype from moving live assets or cash.
- Measure accepted task time, error, break, review and exception rates.
- Compare AI outputs with authorised human results.
- Exercise incident, correction, rollback and manual fallback.
- Present A4 or A2 committee packs using verified evidence only.

Gate 5: the operating team demonstrates control within the selected scope and capacity.

Days 76-90: controlled live decision

- Reconfirm law, licence, documents, custody and settlement.
- Approve code, configuration, models, vendors and access.
- Set exposure, volume, client and transaction limits.
- Confirm fallback, recovery, insurance and communications.
- Train every role and test authority.
- Approve claims only from observed, reviewed pilot evidence.

Gate 6: named legal, compliance, investment, operations, security, model-risk and executive authorities approve a bounded live scope.

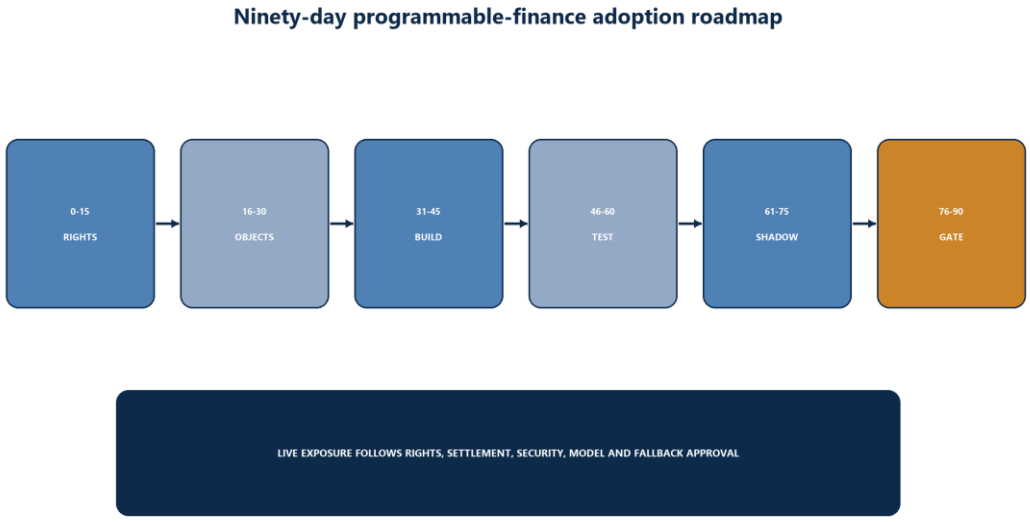

Figure 7. Ninety-day programmable-finance adoption roadmap

Source: Matchpoint implementation framework; governance and resilience context [30-40].

NIST Cybersecurity Framework 2.0 can support governance, identification, protection, detection, response and recovery across the stack [39]. CPMI's harmonised ISO 20022 data requirements for cross-border payments illustrate the importance of structured, consistent data semantics across institutions [40]. These references do not select a technology. They reinforce the need for governed information and resilient operations.

14. CLAIMS REGISTER AND LIMITATIONS

14.1 Permitted and unsupported claims

Claim	Evidence status	Permitted wording
Token records can support issuance and lifecycle administration	Supported in specified institutional arrangements [20-23]	Describe the exact arrangement and scope

Claim	Evidence status	Permitted wording
Programmable settlement prototypes can coordinate tokenised money and instructions	Supported in specified BIS and central-bank work [3-4]	Label prototype, trial or experiment status
AI can assist extraction, reconciliation and monitoring	Supported as capability under control frameworks [30-32]	Describe intended use and observed evaluation
Tokenisation creates liquidity	No general evidence	Report executed liquidity evidence for the specific market
Tokenisation lowers total cost	No approved T26 evidence	Measure complete comparable process and transition cost
AI removes the need for human authority	Outside intended use	Do not claim
The stack prevents fraud, loss or default	No approved evidence	Do not claim
Matchpoint or a client generated revenue or saved cash	No approved evidence	Attributed value remains USD 0
The stack generated investment alpha	No approved evidence	Attributed alpha remains USD 0
One regulatory analysis applies across the Gulf	Unsupported	Require entity, activity and jurisdiction analysis

14.2 Legal and regulatory limitations

The paper does not determine whether a specific token is a security, derivative, deposit, payment token, virtual asset, property interest, electronic transferable record or contractual claim. It does not determine licensing, offer, distribution, custody, settlement, tax, insolvency, data or accounting treatment. Those conclusions require current facts and accountable advisers.

14.3 Technical limitations

Distributed ledgers differ in governance, permission, consensus, finality, privacy, capacity, smart-contract capability and failure modes. Technical standards change. Code review reduces known risk and does not establish absence of defects. Off-chain sources, credentials, keys, vendors, bridges and interfaces can dominate end-to-end risk.

14.4 Empirical limitations

Institutional pilots use selected participants, assets, systems and legal arrangements. Reported transaction counts or values do not establish cost reduction, general availability, sustained throughput or market liquidity. The T26 scenarios and productivity calculation are unverified illustrative management assumptions. They should not be treated as forecasts or achieved results.

14.5 AI limitations

AI output can be incomplete, unsupported or unstable. Evaluation on one document population or workflow may not transfer. Provider and model changes can alter results. Human review can also be inconsistent. The operating system should measure both model and reviewer performance and retain the source evidence for every material result.

14.6 Commercial and causal limitations

Capacity, cash saving, revenue, loss reduction and alpha are distinct. Attributing an outcome requires an approved baseline, comparable target, observed use and causal method. Selection effects, market conditions, portfolio changes and parallel processes can explain differences. For T26, attributed Matchpoint or client revenue, cash cost reduction, loss reduction and alpha remain USD 0.

15. CONCLUSION

Tokenisation and AI can support a more structured asset-to-cash operating system. The durable capability is the governed chain from legal and economic rights through identity, token state, custody, settlement, servicing, reconciliation, AI assistance, human authority and retained evidence.

A4 infrastructure and digital-infrastructure investors can apply that chain to registers, financing instruments, milestone evidence, servicing and asset administration. A2 family-office CIOs and heads of alternatives can use it to strengthen diligence, custody, allocation, reporting and exception control. Each use case retains its own legal perimeter, investment mandate and authority.

The implementation sequence begins with the right and authoritative record. It then specifies the programmable object, permissions, cash leg, lifecycle and failure states. Code, AI and infrastructure are evaluated against business invariants and operating capacity. Institutional pilots provide credible evidence for selected capabilities. Production, liquidity, cost and return claims require separate observed evidence.

The release gate covers legal effect, regulatory perimeter, identity, custody, settlement finality, reconciliation, smart-contract security, AI governance, privacy, resilience, recovery and accountable decision rights. Commercial claims follow the same discipline. For T26, attributed Matchpoint or client revenue, cash cost reduction, loss reduction and alpha remain USD 0.

REFERENCES

[1] Financial Stability Board. (2024). The Financial Stability Implications of Tokenisation. https://www.fsb.org/2024/10/the-financial-stability-implications-of-tokenisation/
[2] Bank for International Settlements. (2025). The Next-Generation Monetary and Financial System. Annual Economic Report 2025, Chapter III. https://www.bis.org/publ/arpdf/ar2025e3.htm
[3] Bank for International Settlements. (2026). Project Agora: A Shared Programmable Platform for Wholesale Cross-Border Payments. https://www.bis.org/about/bisih/topics/fmis/agora.htm
[4] European Central Bank. (2025). Exploratory Work on New Technologies for Wholesale Central Bank Money Settlement. https://www.ecb.europa.eu/press/pubbydate/2025/html/ecb.exploratoryworknewtechnologies202506.en.html
[5] Committee on Payment and Settlement Systems and Technical Committee of IOSCO. (2012). Principles for Financial Market Infrastructures. https://www.bis.org/cpmi/publ/d101a.htm
[6] CPMI and IOSCO. (2022). Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements. https://www.bis.org/cpmi/publ/d206.htm
[7] International Organization of Securities Commissions. (2023). Policy Recommendations for Crypto and Digital Asset Markets: Final Report. FR11/23. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf
[8] International Organization of Securities Commissions. (2023). Policy Recommendations for Decentralized Finance: Final Report. FR14/23. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf
[9] European Union. (2022). Regulation (EU) 2022/858 on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology. https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng
[10] European Union. (2023). Regulation (EU) 2023/1114 on Markets in Crypto-Assets. https://eur-lex.europa.eu/eli/reg/2023/1114/oj?locale=en
[11] Central Bank of the UAE. (2024). Payment Token Services Regulation. Circular 2/2024. https://rulebook.centralbank.ae/en/rulebook/payment-token-services-regulation
[12] Dubai Financial Services Authority. (2021). Regulatory Framework for Investment Tokens. https://www.dfsa.ae/news/dfsa-introduces-regulatory-framework-investment-tokens
[13] Dubai Financial Services Authority. (2026). Updated Crypto Token Regulatory Framework. https://www.dfsa.ae/news/dfsa-implements-major-updates-crypto-token-regulatory-framework-enhancing-market-integrity-and-supporting-innovation-difc
[14] Abu Dhabi Global Market. (2023, amended 2026). Distributed Ledger Technology Foundations Regulations and Framework. https://www.adgm.com/dlt-foundations
[15] Dubai Land Department. (2025). Pilot Phase of the Real Estate Tokenisation Project. https://dubailand.gov.ae/en/news-media/dubai-land-department-launches-pilot-phase-of-the-real-estate-tokenisation-project
[16] Dubai Land Department. (2026). Phase II of the Real Estate Tokenisation Project. https://dubailand.gov.ae/en/news-media/dubai-land-department-launches-phase-ii-of-the-real-estate-tokenisation-project-enabling-resale-in-the-secondary-market-from-20-february/
[17] United Nations Commission on International Trade Law. (2017). Model Law on Electronic Transferable Records. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
[18] Law Commission of England and Wales. (2023, supplemented 2024). Digital Assets. https://lawcom.gov.uk/project/digital-assets/
[19] UK Jurisdiction Taskforce. (2019). Legal Statement on Cryptoassets and Smart Contracts. https://ukjt.lawtechuk.io/
[20] World Bank. (2018). World Bank Prices First Global Blockchain Bond, Raising A$110 Million. https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million
[21] European Investment Bank. (2021). EIB Issues Its First Ever Digital Bond on a Public Blockchain. https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain
[22] Hong Kong Monetary Authority. (2023). HKSAR Government Issues World's First Tokenised Green Bond. https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/02/20230216-3/
[23] Depository Trust and Clearing Corporation. (2024). Smart NAV Pilot Report: Bringing Trusted Data to the Blockchain Ecosystem. https://www.dtcc.com/-/media/Files/Downloads/DTCC-Connection/Smart_NAV-Report.pdf
[24] Financial Action Task Force. (2025). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html
[25] Ethereum Improvement Proposals. (2015). EIP-20: Token Standard. https://eips.ethereum.org/EIPS/eip-20
[26] Ethereum Improvement Proposals. (2017). EIP-712: Typed Structured Data Hashing and Signing. https://eips.ethereum.org/EIPS/eip-712
[27] Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart Contracts Smarter. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 254-269. https://doi.org/10.1145/2976749.2978309
[28] Kalra, S., Goel, S., Dhawan, M., & Sharma, S. (2018). ZEUS: Analyzing Safety of Smart Contracts. Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2018.23082
[29] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts. Principles of Security and Trust, 164-186. https://doi.org/10.1007/978-3-662-54455-6_8
[30] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1
[31] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, & Office of the Comptroller of the Currency. (2026). Supervisory Guidance on Model Risk Management. SR 26-2. https://www.federalreserve.gov/supervisionreg/srletters/SR2602.htm
[32] International Organization of Securities Commissions. (2025). Artificial Intelligence in Capital Markets: Use Cases, Risks and Challenges. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD788.pdf
[33] National Institute of Standards and Technology. (2022). Secure Software Development Framework Version 1.1. NIST SP 800-218. https://doi.org/10.6028/NIST.SP.800-218
[34] Basel Committee on Banking Supervision. (2021). Principles for Operational Resilience. https://www.bis.org/bcbs/publ/d516.htm
[35] European Union. (2022). Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector. https://eur-lex.europa.eu/eli/reg/2022/2554/oj
[36] United Arab Emirates. (2021). Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data. https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws
[37] Dubai International Financial Centre. (2020). Data Protection Law, DIFC Law No. 5 of 2020. https://www.difc.com/business/laws-and-regulations/legal-database/difc-laws/data-protection-law-difc-law-no-5-2020
[38] Abu Dhabi Global Market. (2021). Data Protection Regulations 2021 and Guidance. https://www.adgm.com/operating-in-adgm/office-of-data-protection/resources
[39] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. https://doi.org/10.6028/NIST.CSWP.29
[40] Committee on Payments and Market Infrastructures. (2023). Harmonised ISO 20022 Data Requirements for Enhancing Cross-Border Payments. https://www.bis.org/cpmi/publ/d218.htm

APPENDIX A. ASSUMPTIONS AND EVIDENCE REGISTER

Item	Status in T26	Required approval or evidence
Topic, ICPs, hook, visuals and length	Verified from Topic Tracker row 127	Tracker authority
Author	Matchpoint Partners; named-person attribution pending CK approval	CK approval
Worked A4 and A2 scenarios	Unverified illustrative management assumptions	Transaction, legal, investor and operating evidence
Architecture and control thresholds	Matchpoint framework; no live implementation evidence	Accountable owner approval and testing
Institutional results	Source-bounded to cited project reports	Preserve project scope and status
Productivity	No approved observed T26 evidence	Accepted baseline and target records
Revenue	No approved observed T26 evidence	Contract, invoice, collection and attribution
Cash cost reduction	No approved observed T26 evidence	Ledger and approved counterfactual
Loss reduction	No approved observed T26 evidence	Outcome and causal evidence
Alpha	No approved observed T26 evidence	Portfolio methodology and approved results

APPENDIX B. MINIMUM PROGRAMMABLE ASSET RECORD

1. Asset, instrument, issuer, obligor and vehicle identifiers.
2. Governing documents, law, jurisdiction and authoritative register.
3. Holder rights, obligations, restrictions, priority and remedies.
4. Authorised supply, issued supply, unit, currency and price basis.
5. Eligible holder, beneficial owner, credential and expiry.
6. Token state, lifecycle transition and current restrictions.
7. Custodian, wallet, key model, books and recovery procedure.
8. Cash-flow formula, calculation source, dates, tax and rounding.
9. Settlement asset, accounts, reservation, finality and fallback.
10. Oracle source, signer, timestamp, challenge and correction.
11. Code, contract, model, data and configuration versions.
12. Approval, transaction, reconciliation, exception and incident evidence.

APPENDIX C. RELEASE CHECKLIST

- Confirm the token's legal and economic object in one testable sentence.
- Confirm issuer authority and authorised supply.
- Confirm the authoritative register and correction process.
- Confirm the regulatory perimeter for every entity, activity and location.
- Confirm eligible holders, distribution restrictions and current credentials.
- Confirm custody, segregation, key control, recovery and succession.
- Confirm the settlement asset, finality, liquidity and failed-trade process.
- Confirm every oracle source, signer, challenge period and fallback.
- Verify smart-contract invariants, privileged actions, upgrade and pause.
- Verify books, ledger, register and cash reconciliation.
- Validate AI fields and alerts against independent source evidence.
- Confirm privacy, retention, access and cross-border-data treatment.
- Exercise outage, compromise, vendor exit, correction and manual fallback.
- Set exposure, volume and client limits.
- Record named legal, compliance, investment, operations, security and model authorities.
- Publish only claims supported by approved observed evidence.

APPENDIX D. GLOSSARY

Term	Meaning in this paper
AI	Statistical or computational methods used for extraction, classification, reconciliation, monitoring or language assistance
Atomic settlement	Coordinated execution in which linked legs complete together or fail together under the system rules
Authoritative register	Record designated by law or contract as determining the relevant holder or state
DvP	Delivery versus payment; conditional coordination of asset delivery and payment
Finality	Point at which transfer or settlement is legally and operationally irrevocable under the applicable arrangement
Oracle	Mechanism that supplies an external fact or assertion to a programmable workflow
PvP	Payment versus payment; conditional coordination of two currency legs
Smart contract	Code deployed to execute specified state transitions or rules on a supported system
Token	A digital record or object whose meaning depends on the associated legal, technical and operating arrangement