The Last Mile of the Unified Ledger: Connecting Bank-Internal Tokenised Deposits to Project Agorá

Kyungeun Kim
Hana Institute of Technology, Hana TI

Abstract

Project Agorá, convened by the BIS and the Institute of International Finance, demonstrated settlement of tokenised commercial-bank deposits and central-bank reserves on a shared platform with seven central banks and more than 40 regulated financial institutions. Connections to external infrastructures were intentionally deprioritised, although the architecture can accommodate them. This paper examines one such connection: the vertical boundary between an Agorá-derived shared platform and a bank's internal token ledger. Assuming that both token records represent the same deposit liability, the paper develops an issuer-operated bridge. The bridge prepares the source and destination before recording a durable trigger that marks technical finality. It checks that the amounts recorded on the two token ledgers, together with amounts removed from the source but not yet recorded at the destination, equal a liability total supplied from outside the bridge. It also limits the amount of funds that can become unavailable during a transfer, separates operational authority and produces records for independent supervisory verification.

Five experiments on a single-bank prototype examined liability conservation and cross-ledger reconciliation, cancellation before the trigger and recovery after it, controls on unavailable funds, independent verification using recorded evidence, and local operating performance. Under those conditions, technical controls maintained accounting consistency, supported recovery from the specified interruptions, limited the amount of unavailable funds and enabled independent verification. Performance findings apply only to the tested prototype.

The evidence supports a policy framework for vertical interoperability. Accounting conservation does not ensure fund availability: after the trigger, value may remain fully accounted for while the transfer principal can neither use it nor cancel the transfer. Law, account terms, the rulebook and operating arrangements must therefore establish the identity of the liability and its authoritative record, the legal effect of the trigger, exposure limits and completion duties, separated powers and independent supervisory verification.

Keywords: tokenised deposits; vertical interoperability; payment-system interoperability; Project Agorá; cross-ledger reconciliation; settlement finality; fund availability; supervisory verification

1. Introduction

1.1 The unresolved vertical interoperability gap

Project Agorá's prototype established the horizontal direction of interoperability: settlement between banks across jurisdictions. The project brought together seven central banks and more than 40 regulated financial institutions [1, p. 5]. In subsequent testing, live transactions were settled across 17 scenarios [2], [3]. One category left outside the test perimeter was interoperability with external infrastructures. Connections to domestic RTGS and core banking systems were "intentionally deprioritised" and not tested, although the architecture could accommodate them [1, p. 82]. This paper examines that unresolved boundary from the perspective of a participating commercial bank. It focuses on the connection between the bank's internal tokenised-deposit system and an Agorá-derived shared platform (§1.2).

At this platform–internal-ledger boundary, existing messaging networks, issuer-centred burn–mint systems and general-purpose orchestrators could technically be used; §4.1 compares them against the requirements of this connection. This paper describes the connection as vertical because it links a single bank's own ledger to the shared platform rather than one bank to another. The term *vertical bridge* applies only when two conditions hold: participation is asymmetric, and the token records on both ledgers represent the same liability of the same issuer.

First, participation is asymmetric: the bank retains issuer control over its tokenised deposits but joins the platform under common rules it does not unilaterally set [1, pp. 19, 25, 34, 57]. The platform, in turn, has no role in governing the bank's internal ledger. The asymmetry concerns participation only; transfers run in both directions (§4.3). Second, the two token records must represent the same liability of the same issuer; otherwise, they are separate claims that may not remain at par (§6.1).

The missing **last mile** is the bridge between the two token representations. The BIS unified-ledger vision describes a common venue where tokenised money and assets coexist on a programmable platform [4, p. 94]. Connecting a bank's internal token ledger to the shared platform allows deposits recorded internally to be re-recorded on the platform and used for settlement there. Without that connection, only the money and assets recorded directly on the platform fall within the venue's scope.

The bridge does not replace core banking: the model treats the bank's core liability ledger as the source of the authoritative total T, not as a bridge endpoint (§§3.1, 4.4). This paper's prototype does not test live production integration; instead, the paper specifies the bridge design and examines its correctness, finality, access to funds and operational evidence. In this paper, *depositor* means an institutional account holder whose Bank K deposit is represented on either ledger, such as another bank or a corporate entity. *Transfer principal* means the party for whose account the re-recording occurs: either Bank K acting on

its own account or such a depositor. This term identifies the party to whom the transfer is attributable, rather than the operational role that executes it (§4.2).

1.2 Motivating evidence: bank-internal tokenisation

The gap is not hypothetical. Banks participating in, or pursuing initiatives related to, Agorá have operated, piloted or announced internal tokenised-deposit systems. Examples include Citi Token Services [5], HSBC's Tokenised Deposit Service [6], J.P. Morgan's JPMD [7], UBS Digital Cash [8], Hana Financial Group's deposit-token initiative [9], and BNY's permissioned-chain deposit tokens [10]. Korea's Project Han River and Switzerland's legally binding blockchain-based bank-deposit payment provide further evidence of institutional experimentation [11], [12].

These systems remain fragmented across technical and institutional models, from U.S. banks' own private, permissioned platforms [5], [10] to Korea's central-bank-led pilot and linked public–private infrastructure initiative [11], [13]. They therefore operate as **walled gardens**: participation in a shared payment platform does not, by itself, make a bank's internal tokenised deposits available on that platform. This fragmentation motivates the paper's configuration-specific question: when one bank connects its internal token ledger to a shared platform, how can the identity of the liability, finality, access to funds and supervisory evidence be preserved across the boundary?

1.3 Contributions

The paper organises its contribution around four policy questions: how are the ledgers connected; is the amount preserved; when can the transfer principal use the funds; and who is responsible?

- **C1 — Vertical bridge design.** It specifies the bridge structure and state transitions connecting a shared settlement platform to a bank's internal token ledger (§4).
- **C2 — Liability identity and aggregate conservation.** It assumes that the two token records represent one bank liability and tests whether the total remains conserved across approved issuance and redemption events, with bridge value in flight accounted for (§3.2, §4.4, §5.2 and §6.1).
- **C3 — Finality and access to funds.** It designates the durably recorded `ARMED`→`TRIGGERED` transition as the technical finality boundary, measures value unavailable to transfer principals before and after finality, and proposes the admission limit `P` and exposure limit `C` (§§3.3, 4.1–4.3, 5.3–5.4 and 6.2).
- **C4 — Authority separation and supervisory evidence.** It separates preparation, verification, trigger, execution, pause or cancellation, and audit powers, and provides independently checkable receipts and append-only evidence (§3.4, §§4.2 and 4.5, §5.5 and §§6.3–6.4).

1.4 Paper organisation and method

Using a design-science method [14], the paper develops a bridge design, evaluates its technical controls and derives policy requirements from the findings and their limits. The analysis combines a formal model and invariant proof with five prototype experiments, while treating legal and institutional conditions separately from experimentally tested properties.

Section 2 reviews the background and related work. Sections 3–4 define the model and bridge design, and Section 5 reports the five experiments (E1–E5). Section 6 translates the findings into legal, governance and supervisory requirements (R1–R5). Sections 7–8 state the limitations and conclusion.

2. Background and Related Work

2.1 Policy and economic foundations

Three policy foundations frame the vertical bridge: liability identity, the distinction between finality and access to funds, and operational accountability.

Liability identity and the unified ledger. Bearer-style private money tokens can trade away from par [15, pp. 1–2]. A similar risk arises when a bank liability is represented on two ledgers and the destination token becomes a separately tradable claim. Locking the source can keep the total amount available for use unchanged, but does not prove that both records represent the same liability or remain at par. This paper therefore treats bridge burn and mint as rerecording: the record moves without creating a second liability (§§4.1, 6.1). BIS likewise treats singleness—the exchange of different forms of money at par—as a condition for a viable monetary system [16, pp. 77–79]. The amounts recorded on the shared-platform ledger and the bank's internal ledger, together with any source-burned amount awaiting destination recording, must equal Bank K's authoritative tokenised-deposit liability total T (§§3.2, 4.4).

BIS's unified-ledger concept combines tokenised money and assets on a common platform while allowing links to other ledgers and existing systems through coordination and governance [4, pp. 94, 104–105]. This bridge applies that logic between an Agorá-derived platform and Bank K's internal ledger without creating a parallel claim. A later BIS report links singleness to redemption at par in central-bank money and places tokenised commercial-bank deposits and jurisdiction-specific reserve ledgers within Agorá's coordinated architecture [17, pp. 81, 84]. For this paper, the relevant implication is that singleness depends not only on the shared platform but also on the integrity of its links to external ledgers, including a participating bank's internal ledger.

Finality and access to funds. Technical confirmation does not necessarily constitute legal settlement completion. Agorá distinguishes the settlement trigger from later asynchronous ledger updates [1, p. 65, fn. 32]. In this paper's bridge, funds become unavailable at source lock; after the trigger, the transfer

cannot be cancelled while destination recording remains incomplete. The paper therefore treats finality, operational completion and fund access as separate policy questions (§§3.2–3.3, 4.1–4.3, 6.2–6.3).

Operational accountability and resilience. The FSB identifies interconnectedness, functional concentration and operational fragility as tokenisation vulnerabilities [18, pp. 14–20]. These risks can grow with connectivity, transaction volume and institutional dependence [18, pp. 2, 20]. BIS–CPMI finds that existing infrastructure risks persist under tokenisation but may appear differently [19, pp. 4, 25]. These concerns support separated authorities, attributable state changes and independently verifiable supervisory evidence (§§3.4, 4.5, 6.3–6.4).

2.2 Project Agorá: architecture and settlement model

Project Agorá is designed as a programmable multi-currency platform for tokenised commercial-bank deposits and central-bank reserves in a two-tier system [1, pp. 7–9]. The payment coordinator deployed on the unifying ledger manages the sequence and state of each payment [1, p. 30]. This paper uses only the public report's principles as platform-side inputs [1, pp. 10, 35, 40–41, 65].

Four inputs matter.

Visibility and token authority are bounded. Noto limits transaction contents to relevant parties while the issuer can see token state [1, pp. 35–36]. Paladin's reference documentation—not the Agorá report—adds that its notary validates and submits transactions and may restrict minting [20]. Pente limits workflow visibility to designated groups; the bridge's token endpoint relies on Noto [1, p. 35]. These boundaries inform the roles and evidence in §§3.4 and 4.5.

Settlement follows a defined sequence. Agorá locks assets, delegates authority and issues an atomic settlement trigger; later updates may remain asynchronous [1, pp. 22, 50–51, 65]. This paper adopts the durable trigger record as its technical cancellation boundary (§§4.1–4.3).

The platform token records an existing deposit relationship. Agorá's legal analysis treats tokenisation as a record of the existing balance, not a source of independent rights [1, pp. 58–62]. This paper adopts same-liability identity across the internal and platform records as a modelling condition.

Technical and legal finality differ. Applicable rules and jurisdictional law determine legal completion; PFMI informs the relevant standard [1, p. 65, fns. 30, 32]. The design leaves the trigger's legal effect to the rulebook and law (§6.2).

2.3 Central bank interoperability experiments

Official-sector experiments use three models: a common venue, cross-system exchange or synchronisation, and institutional integration. Table 1 shows why none matches this same-liability vertical bridge.

Table 1. Official-sector experiments compared with the same-liability vertical bridge.

Project	Setting and mechanism	Why the configuration differs
mBridge	Common ledger and central-bank validators for multiple CBDCs	Multiple central-bank issuers; no bank-internal token ledger
Mariana	Bridges and AMM between domestic and transnational wCBDC environments	Cross-system exchange, not one liability re-recorded
Meridian FX	Synchronisation operator and APIs between RTGS and external ledgers	Distinct-currency legs, not two representations of one assumed bank liability
Jura	Third-party DLT, subnetworks and dual notaries for EUR/CHF wCBDCs	Two currencies and central-bank issuers
Helvetia II	Core-banking, central-bank payment and DLT asset-system integration	Core-banking integration; this paper starts from an existing internal token ledger
This paper	**Issuer-operated shared-platform–internal-ledger bridge**	**One bank liability preserved across two ledger records**

mBridge and Jura are multi-currency, multi-issuer arrangements, whereas Mariana exchanges wCBDCs between domestic and transnational environments through bridges and an AMM [21, pp. 4, 12–13, 25–26], [22, pp. 3–4, 24–27], [23, pp. 3, 10, 16, 18–20], [24]. Their policy problem is coordination among sovereign issuers, not one bank's control of two records of the same claim.

Meridian FX provides a close orchestration precedent: its API-based operator coordinates RTGS and external-ledger settlement without its own RTGS account or credit and liquidity risk [25, pp. 5, 12–15]. Meridian coordinates distinct-currency settlement legs, whereas this paper coordinates re-recording between two ledger representations of one assumed Bank K deposit liability.

In test environments, Helvetia II linked the SDX DLT platform and the SIC central-bank payment system to participating banks' core-banking systems, where wCBDC transactions were booked and reconciled [26, pp. 11, 13, 17–18, 28–29]. This paper instead assumes that a participating bank already operates

an internal token ledger and examines how that existing platform can connect to the shared platform.

2.4 Industry interoperability initiatives

Issuer-specific systems. J.P. Morgan's Kinexys and JPMD, Citi Token Services, HSBC's Tokenised Deposit Service and UBS Digital Cash show that banks already operate, pilot or plan issuer-specific tokenised-deposit platforms and services [27], [5], [6]–[8]. These cases establish the demand for and existence of the bank-side endpoint assumed here.

Horizontal frameworks. Kinexys–DBS explores tokenised-deposit transfers between two banks' on-chain ecosystems [28]. RLN places issuer balances on a shared ledger; RSN extends that partitioned model to multi-asset and cross-network settlement, while leaving atomicity and reconciliation unresolved [29, Technical Report, pp. 11–12]. The proposed TCH network likewise explores interoperability standards and implementation [30]. These initiatives provide coordination and settlement precedents, but remain focused on interbank or shared infrastructures.

Vertical-adjacent systems. HKMA's EnsembleTX pilot completed a cross-bank transfer, a horizontal use case [31], [32]. Kinexys–Canton announced plans for phased integration of native issuance, transfer and near-instant redemption of JPMD [33], but did not answer the paper's four policy questions on ledger connection, conservation, fund access and accountability.

2.5 Cross-chain interoperability: theory and practice

Computer-science research develops interoperability mechanisms and verification methods; applied research examines failures, controls and system designs.

Theoretical mechanisms and verification. Atomic swaps define atomic exchange of distinct assets [34]; MPHTLC extends this to multiple co-owners and assets and addresses joint-ownership collusion [35]. Zakhary et al.'s cross-chain atomic commitment provides lineage for §4.1's issuer-coordinated commit [36]. Surveys classify interoperability architectures and security properties [37], [38]. Verification taxonomies distinguish local, external and native models, with later work adding optimistic verification through a challenge period [39], [40]. These categories inform §4.1.

Empirical evidence from bridge systems. Xscope systematises bridge failures underlying G1 [41]. From more than 10 million transfers, Count of Monte Crypto derives an invariant in which cumulative outflow equals cumulative inflow minus costs, uses it for retrospective detection and online auditing, and proposes announce-then-execute control [42].

System and design precedents. Axelar's ITS Hub is designed to track bridged balances only when no minter is set [43], [44]. CCTP combines issuer-

centred burn–mint and one-time destination nonces for native USDC across peer chains [45]. He [46] classifies tokenised-deposit interoperability architectures by settlement instrument, ledger topology and intermediary role; Model III is a liquidity-provider-mediated own-liability structure. Together, these precedents cover balance tracking, issuer attestation, replay protection and liability topology.

This paper applies that accounting problem to preserving one bank liability across a shared platform and the bank's internal token ledger.

2.6 Research gap and scope

Existing research provides orchestration, issuer-centred burn–mint, bridge accounting and native-liability structures. These are useful building blocks for moving or exchanging tokens across ledgers, but cannot be applied unchanged to this configuration. Figure 1 summarises that boundary.

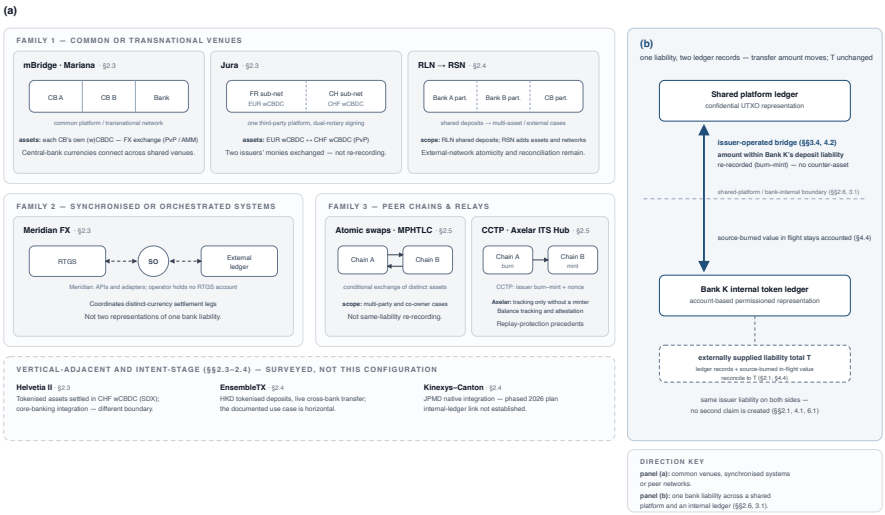

Figure 1. Interoperability settings and paper scope. Panel (a) groups common-venue, synchronised and peer-chain approaches and marks adjacent cases. Panel (b) shows Bank K re-recording an amount of one liability between an Agorá-derived shared platform and its internal ledger; the two ledger balances and source-burned in-flight value reconcile in aggregate to T (§3.2).

Sections 3–5 define this setting and test the bridge; Section 6 derives rulebook and supervisory requirements.

3. System model, roles, and goals

Section 2 identified the configuration-specific gap. This section defines the protected liability, bridge boundary, transfer risks, authority and the four goals addressed in Sections 4–5.

3.1 Scope

This paper models a vertical bridge between an Agorá-derived shared platform and Bank K's internal token ledger, not the production Agorá platform. Bank K is a hypothetical participating bank that issues the deposit liability. The prototype uses a permissioned EVM internally, but that choice does not define the model.

Four records matter: the shared-platform token ledger, Bank K's internal token ledger, BridgeBook's bridge-control record, and the issuer liability record that supplies the authoritative total T. The first two represent value; BridgeBook records transfer state and evidence; the issuer liability record provides the accounting anchor. Section 4 assigns their interfaces and operational authority.

The bridge boundary excludes both the internal ledger's connection to core banking and the process that produces T. The model treats T as externally supplied and examines the part of one Bank K liability re-recorded between the token ledgers. Figure 2 locates this boundary.

The model assumes durable records, deterministic ledger finality and externally supplied T. It examines outages, retries, incomplete evidence and operational delay/withholding. It does not guarantee legal finality, completion against issuer-wide collusion or deliberate non-cooperation, detection of off-BridgeBook activity, or recovery from validator halt or ledger reorganisation. Sections 4–7 retain these limits.

3.2 One liability, two ledger representations

T denotes Bank K's tokenised-deposit liability represented across the two token ledgers. A bridge transfer leaves T unchanged: burn and mint move an amount already included in T from one representation to the other. Authorised issuance or redemption is different. Bank K adds or subtracts the same amount from both the relevant token-ledger balance and T; §4.4 states the resulting conservation property.

The model covers only **Configuration A**, in which both tokens record the same liability of the same issuer [1, pp. 58–62]. The bridge changes that liability's record location; it neither creates nor exchanges a separate claim. The analysis therefore asks three separate questions: Is T conserved? Which event makes the transfer final? Can the transfer principal use the amount before destination recording? An accounting equality answers only the first.

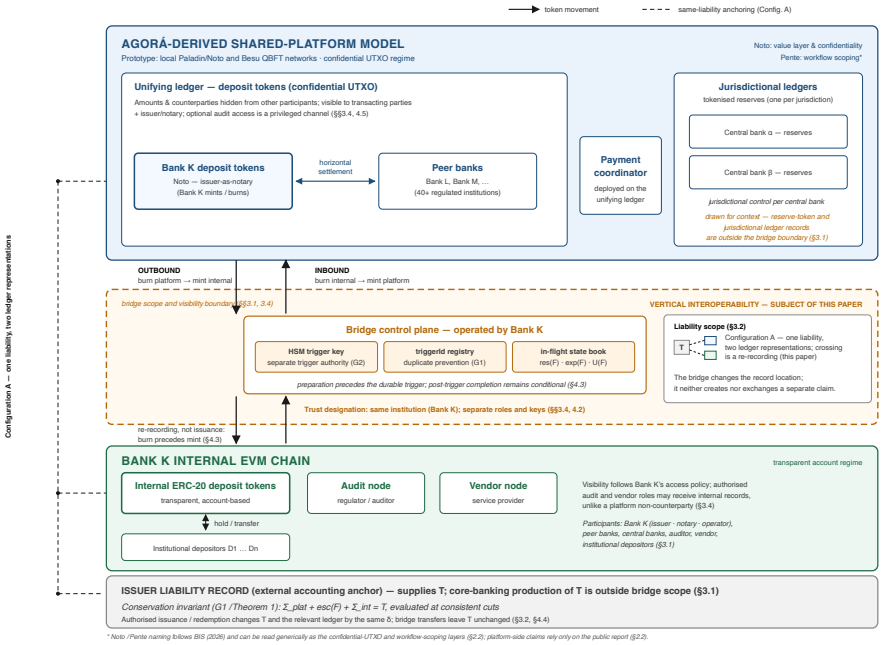

Figure 2. Architecture and scope. Bank K's bridge connects a confidential-UTXO shared-platform model to its account-based internal EVM ledger. BridgeBook records the transfer; the issuer liability record supplies T. Core banking is the accounting anchor, not an endpoint, and jurisdictional ledgers provide context only. The shared-platform layer is adapted from [1, Fig. 9]; the other layers are this paper's additions.

3.3 States and policy measures

The central policy distinction is that preserving T does not ensure access to funds during an incomplete transfer. Each transfer follows the same recorded phases in either direction:

$$\texttt{PREPARING} \to \texttt{LOCKED} \to \texttt{ARMED} \to \texttt{TRIGGERED} \to \texttt{BURNED} \to \texttt{CLOSED}.$$

The phases have the following policy meanings:

- `PREPARING` — The bridge admits the request and checks conditions before locking funds.
- `LOCKED` — The source locks or escrows the amount; cancellation remains possible.
- `ARMED` — Destination readiness is recorded; cancellation remains possible.
- `TRIGGERED` — The finality decision is durably recorded; cancellation is no longer permitted.

- `BURNED` — The source representation is removed, but the destination has not yet recorded its replacement.
- `CLOSED` — Destination recording is complete; the transfer leaves all in-flight measures.

`ARMED`→`TRIGGERED` is technical finality: cancellation is possible before it; afterwards, only conditional forward recovery is permitted.

For platform-to-internal transfers, the platform locks and burns and the internal ledger records the destination amount; the reverse direction swaps those ledger roles (§4.3).

Figure 3 maps these phases to the accounting and unavailable-value measures defined below.

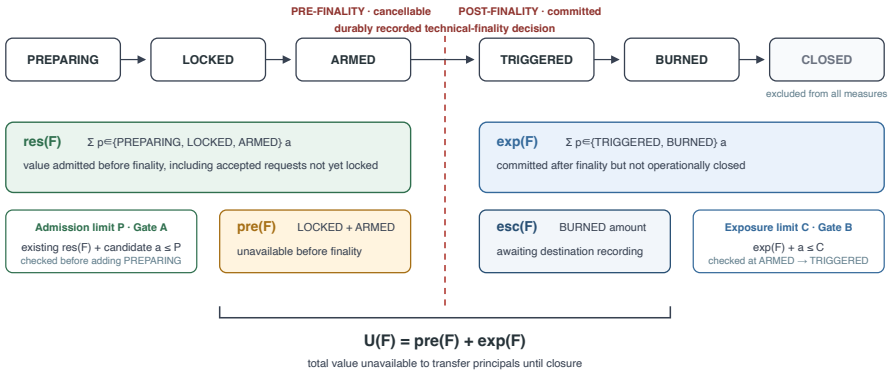

Figure 3. Transfer phases and policy measures. The durable `ARMED`→`TRIGGERED` decision separates cancellable from committed transfers. P caps admitted pre-finality value $\mathrm{res}(F)$, and C caps committed-but-unclosed value $\mathrm{exp}(F)$. $\mathrm{pre}(F)$ and $U(F)$ measure unavailable value; $\mathrm{esc}(F)$ is the `BURNED` accounting subset (§4.3).

Let F be the in-flight transfer records, each with amount a and phase p:

$$\mathrm{esc}(F) = \sum_{p \in \{\texttt{BURNED}\}} a, \quad \mathrm{pre}(F) = \sum_{p \in \{\texttt{LOCKED},\texttt{ARMED}\}} a,$$

$$\mathrm{exp}(F) = \sum_{p \in \{\texttt{TRIGGERED},\texttt{BURNED}\}} a, \quad U(F) = \mathrm{pre}(F) + \mathrm{exp}(F),$$

$$\mathrm{res}(F) = \sum_{p \in \{\texttt{PREPARING},\texttt{LOCKED},\texttt{ARMED}\}} a.$$

esc(F) is accounting escrow: the `BURNED` amount is absent from both token ledgers while destination recording is pending. It is not the source ledger's operational lock or escrow. pre(F) and exp(F) divide unavailable value at finality; $U(F)$ is the total. res(F) includes `PREPARING` because admission consumes capacity, while pre(F) excludes it because funds remain usable. At Gate A, F is the existing set before adding the candidate. Section 4.3 applies the limits, Section 5 measures unavailability, and §4.4 distinguishes conservation from access to funds.

3.4 Roles and authority separation

Bank K is the issuer authorised over both representations and therefore operates the bridge. A1–A3 define ordinary visibility, which provides the baseline against which G4 and E4 assess independent reconstruction from additional supervisory evidence. A4 and the notary separate orchestration from enforcement to avoid unchecked control by one role.

Table 2 makes these observation and authority boundaries explicit.

Table 2. Observation positions and operational authorities in the bridge model.

Class	ID or role	Holder	Permitted visibility	Bridge authority
Observation	A1	Platform non-counterparty	Information available to a non-party, not transaction contents	None
Observation	A2	Transaction counterparty	Its own transaction details	None
Observation	A3	Bank K or its authorised observer	Records allowed by Bank K's internal access policy	None
Operation	A4 — orchestrator	Bank K	Both bridge endpoints and BridgeBook	Process authorised requests and sequence, delay or withhold eligible transfers

Class	ID or role	Holder	Permitted visibility	Bridge authority
Enforcement	Notary	Bank K	Platform-token state and transaction-specific evidence	Approve or refuse platform burn or mint and consume transfer identifiers; cannot initiate transfers or set release order

These boundaries need not correspond to distinct institutions.

Bank K supplies the cross-ledger control plane. A4 coordinates eligible transfers, while distinct authorities approve triggering, cancellation, pause and restart (§4.2). Supervisors oversee and read records rather than execute transfers (§6.3). An external provider must rely on Bank K's attestations or receive delegated access to its private flows and liability controls, and therefore acts under Bank K's authority. Bank K controls its internal ledger and platform token contract, not the platform [1, p. 57].

Paladin defines the Noto notary as validating and submitting token operations and potentially holding exclusive mint authority [20]. In the Agorá model, the participating bank issues its deposit tokens, controls the applicable asset contract and sees their state [1, pp. 36, 57]. The model assigns both functions to Bank K, but separating the notary from A4 through distinct authority, keys and verification paths is this paper's internal-control design (§4.2); institutional separation is not required.

This allocation cannot prevent Bank K from delaying or withholding an eligible transfer. It makes state-changing actions attributable and allows the rulebook to assign responses and review. Completion remains conditional on recovery and continued operation (§§4.2, 6.3–6.4).

3.5 Goals

The liability, risks and authority defined above yield four design and evaluation goals:

- **G1 — Liability and execution integrity.** Conservation holds at every reachable state; each bridge-leg destination record follows one finalised source-side burn for the same transfer and amount; and no transfer creates more than one destination-side value movement. Completion after a transient failure remains conditional on safe retries and component recovery.
- **G2 — Finality-bound recovery.** The durable `ARMED`→`TRIGGERED` decision is technical finality. Cancellation is allowed only before it; afterwards,

only conditional forward recovery is permitted. Legal effect depends on the applicable rulebook and law.

- **G3 — Controlled unavailability.** If every relevant transition passes the gates and aggregate updates are serialised, pre-finality reservation remains within P and post-finality exposure within C, including under concurrent requests.
- **G4 — Independent verifiability.** An authorised verifier can check transfer state, responsible role and ledger evidence without relying solely on the orchestrator's assertion.

These goals are conditional properties of the specified transition system. They do not determine legal finality, production values for P, C or τ, or responsibility allocation; Section 4 states the technical conditions, Section 5 tests them and Section 6 addresses the institutional choices.

4. Bridge Design

Section 3 defined the protected liability, risks, authority and G1–G4. Section 4 turns those definitions and goals into design choices that Section 5 tests.

4.1 Design alternatives and selection

The shared-platform token record and Bank K's internal token record represent the same Bank K liability, and Bank K supplies the authoritative total T. The comparison therefore asks which approach preserves that liability's identity while allocating bridge authority clearly and making its exercise independently reviewable.

The comparison applies four requirements:

- **Controlled linkage.** A unique triggerId binds the source-ledger action, destination-ledger action and supporting evidence to the same transfer, allowing an authorised reviewer to verify that they match.
- **Ordered execution.** Preparation precedes the durable trigger, and the source representation is burned before the destination representation is minted [1, pp. 22, 65].
- **Same-liability re-recording.** A bridge transfer changes where one liability is recorded; it does not create a new claim [1, pp. 58–62].
- **Technical and legal finality remain separate.** The durable trigger record is the technical boundary. Its legal effect depends on the rulebook and applicable law [1, p. 65, fns. 30, 32], [47].

Table 3 applies these requirements to six approaches. For each, it asks whether it preserves one liability, provides a clear owner of the commit-or-cancel decision, works without changing the shared platform and leaves evidence for independent review.

Table 3. Six design approaches under the same-liability constraint.

Design approach	How it works	Why it does or does not fit Configuration A	Decision
1. No transfer-time control	Uses API calls and retries, or reconciles the ledgers later [42], [48]	If a response is lost, no authoritative record says whether to complete or cancel. Later reconciliation detects the problem only after the transfer event	Not sufficient as the bridge control
2. Claim-changing design	Locks the original and issues another token, or supplies destination liquidity [15], [40]	Creates another claim or an exchange against inventory. This paper requires the same Bank K liability merely to change recording location	Outside Configuration A
3. Conditional exchange	Uses time or hash conditions to exchange assets [34], [35]	Designed to exchange distinct assets, not to re-record one issuer liability	Different transaction problem
4. External verification	Uses relayers, multisig/MPC, light clients or zk proofs to verify messages or ledger state [37], [38], [49], [39], [40]	Can strengthen evidence checking, but Bank K must still provide the private ledger facts and T; it also adds access and governance requirements	Does not remove issuer dependence
5. Cross-ledger commitment	Coordinates prepare and commit operations on both ledgers [36]	Requires prepare/commit interfaces on the shared platform that Bank K cannot impose	Unavailable without platform changes
6. Issuer-operated orchestration	Bank K coordinates native lock, trigger, burn and mint operations; Agorá and CCTP provide related precedents [1, pp. 22, 35, 65], [45]	Bank K already controls both representations and T, can own the commit-or-cancel decision and can separate roles and evidence internally	Adopted

Table 3 is specific to this configuration, not a general ranking of interoperability mechanisms. A single-ledger design also falls outside the comparison because it removes the two-ledger problem rather than solving it.

Crucially, Bank K supplies T and private ledger facts. External verification

may strengthen evidence checking, but it cannot establish T independently of Bank K. The issuer-operated approach therefore places the commit-or-cancel decision with Bank K while preserving claim identity. Section 4.2 divides that authority across roles and evidence. The rulebook and applicable law determine irrevocability, incomplete-transfer status, completion responsibility and insolvency treatment (§§6.2–6.3).

4.2 Bridge components and authority separation

An issuer-operated design does not mean that one process should hold every power. The architecture uses the four record layers in §3.1 and separates operational authority across five components and roles:

- **BridgeBook** stores transfer state, receipts and pre- and post-finality reservations. Aggregate limits require a shared, serialised budget record; implementation and evaluation appear in §§5.1 and 5.4.
- **The orchestrator** coordinates the workflow and requests the trigger decision.
- **The Gateway** locks, burns and mints on the internal ledger and records used outbound identifiers.
- **The notary** is a separately keyed Bank K verification role, not an external institution. It verifies platform-token operations and, for inbound minting, the internal burn evidence and one-time identifier.
- **The HSM trigger key** authenticates the finality decision and is separated from transaction-submission keys. The execution role has no direct authority to approve that decision.

Table 4 states the resulting authority and evidence requirements.

Table 4. Operational authority and evidence by bridge stage.

Stage	Responsible role	Permitted action	Evidence retained
Request screening	Compliance	Approve or reject before funds are locked	policy decision and request record
Lock and prepare	Execution operator	Lock the source amount and confirm destination readiness	source-lock and readiness evidence
Trigger	Trigger authority	Record and sign the technical-finality decision	durable trigger record and HSM signature
Burn and mint	Execution operator and notary	Execution operator submits ledger actions; notary verifies the required platform or burn evidence	burn certificate, used-identifier record and finalised ledger evidence

Stage	Responsible role	Permitted action	Evidence retained
Cancel or pause	Rulebook-authorised operator	Release and cancel before finality, or pause new admissions; a supervisor may require escalation without executing transfers	source-release receipt, cancellation or pause record, authority and reason
Audit and reconciliation	Read-only auditor or supervisor	Compare BridgeBook, both ledgers and the issuer liability record; no transaction execution	append-only log and reconciliation report

Production must separate compliance, trigger approval, execution and audit so that no operational role can complete a transfer and erase its evidence. The prototype separates roles and keys; institutional independence remains a production governance requirement. The design reuses native platform functions and requires no change to shared contracts. With these roles assigned, §4.3 applies the same finality and exposure rules in either direction.

4.3 Bidirectional protocol and unavailable-funds controls

The prototype tests the shared policy lifecycle using Noto's confidential UTXO commitments and an account-based ERC-20 token on EVM. A Noto-source lock may combine commitments, lock a, and return excess as unlocked change; an EVM-source transfer escrows exactly a. Completion records a as an account credit or new Noto commitment. This maps amounts, not individual UTXOs, to account entries. Because other token systems may represent ownership and state differently, the design does not claim a universal mapping. Its contribution is the common identifier, finality boundary, P/C reservation, conservation and evidence lifecycle applied to this pairing.

P caps admitted pre-finality value and C caps committed but incomplete value. Gate A checks P before locking; Gate B checks C before the durable trigger and moves a atomically between them.

Table 5 applies these gates and phase rules to both transfer directions.

Table 5. Bidirectional protocol and unavailable-funds controls.

Phase	Platform → internal	Internal → platform	Policy control and effect
PREPARING	Check platform source and internal destination	Check internal source and platform destination	Gate A requires $\mathrm{res}(F) + a \leq P$ and destination evidence within a rulebook-defined freshness threshold
LOCKED	Noto creates a locked commitment for a and returns unlocked change	Gateway escrows exactly a	The transfer principal cannot use a; the amount remains reserved under P
ARMED	Gateway records destination readiness	BridgeBook records readiness for notary-verified platform minting	The transfer remains cancellable and charged against P
TRIGGERED	Durable trigger decision	Same durable trigger decision	Gate B requires $\exp(F) + a \leq C$ and moves state and reservation atomically from P to C
BURNED	Noto burns the locked a	Gateway burns escrowed a and produces evidence	The amount remains charged against C; age monitoring begins
CLOSED	Gateway records an account credit of a	Notary verifies the burn, consumes the identifier and approves a new Noto commitment of a	Destination recording completes and C is released

Figure 4 shows the resulting sequence and representation translation in each direction.

Gate A reserves P before locking; rejection leaves source funds unaffected. Gate B atomically releases P, acquires C, and records TRIGGERED. Its failure requires release and cancellation or an ARMED hold that remains in P and $U(F)$. Pre-finality cancellation releases the source lock and P; C is released only at CLOSED.

The Gateway or notary rejects a completed value-moving action that reuses the transfer identifier, while unfinished steps may be retried. Recovery first

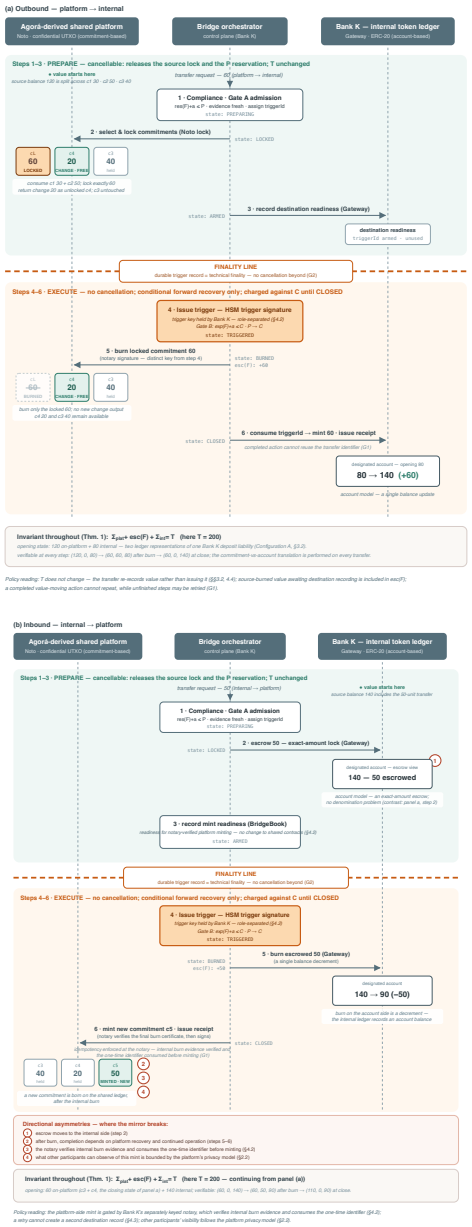

Figure 4. Bidirectional protocol and representation translation. Panels (a) and (b) show the two translation directions. The durable trigger record marks technical finality; legal effect depends on the rulebook and law. Gate A limits pre-lock admission and Gate B moves the transfer to C. Thereafter, only conditional forward recovery is permitted. Burn precedes mint, T remains unchanged and amounts are illustrative.

reconciles BridgeBook with both ledgers and then resumes from the durable phase [48]. Exactly-once completion remains conditional on correct verification, component recovery and continued operation; the protocol cannot compel completion against deliberate withholding.

The age threshold τ is a supervisory alert, not a legal completion promise. If a BURNED record exceeds τ, policy may pause new triggers and require escalation. The rulebook must identify who may pause or resume admission and what evidence is required. These properties hold only while every transfer passes the relevant controls and the records remain durable.

4.4 Properties and limits of the transition model

The accounting condition is

$$\textbf{INV}: \qquad \Sigma_{\text{plat}} + \text{esc}(F) + \Sigma_{\text{int}} = T.$$

In plain terms, Bank K's liability must remain on one token ledger or as source-burned value awaiting destination recording. Under the model assumptions and enforcement conditions stated in §§3–4, the following theorem holds.

Theorem 1 (Conservation component of G1).
If **INV** *holds initially, it continues to hold after every permitted transfer, cancellation, retry, issuance and redemption transition.*

Locking leaves the total unchanged; burn moves value into $\text{esc}(F)$; mint moves it to the destination ledger; and authorised issuance or redemption changes the ledger and T together. Each permitted transition therefore preserves **INV**.

Three policy implications are separate from the equation:

- **Execution and finality remain conditional.** A destination mint must match one final burn and identifier—G1's execution-integrity clause, tested in E2 (§5.3), not proved here. After the trigger, cancellation ends; completion depends on forward recovery and operator cooperation.
- **Conservation is not access to funds. INV** may hold while $U(F) > 0$, so value can be fully accounted for while the transfer principal cannot use it.
- **Exposure bounds require complete enforcement.** If every relevant transfer passes both Gates and aggregate reservations are serialised, then $\text{res}(F) \leq P$ and $\text{exp}(F) \leq C$.

These properties cover only the permitted transition model. They neither prevent activity outside BridgeBook nor determine legal finality or force completion. Because the guarantees are conditional, supervisors need evidence that the required actions, limits and roles were actually observed.

4.5 Supervisory evidence and evaluation plan

Supervision needs records of what the bridge actually did, not only the orchestrator's account.

In this paper, an independent reconciler is a read-only process separate from the orchestrator. Using only exported records from both token ledgers, BridgeBook and the issuer liability record, it reports missing or unmatched entries. It cannot execute transfers, and its findings depend on the completeness of the export.

The evidence should answer four questions:

1. **Authorisation and reconciliation.** What transfer, amount and policy were authorised, and do BridgeBook, both ledgers and the issuer liability record reconcile?
2. **Status and delay.** Is the transfer cancellable or committed, how old is it, and what do its $\mathrm{pre}(F)$, $\exp(F)$, $U(F)$ and reservation histories show?
3. **Exactly-once execution.** Do source and destination records match by identifier, amount and destination, with valid signatures, receipt and used-identifier evidence?
4. **Accountability.** Which role acted or rejected the request, and does each exception have a signed record of its action, reason and policy?

The rulebook should specify access, export frequency, confidentiality and retention. Public disclosure is unnecessary, but continuing access requires an independent node or external replication. Evidence supports reconciliation and attribution; it does not prevent misconduct, force completion, prove issuer-wide completeness or assign legal responsibility.

Table 6 maps G1–G4 and the operating envelope to E1–E5 and states each evaluation question.

Table 6. Goals and experiments in plain language.

Goal	Experiment	Evaluation question
G1 — Liability and execution integrity	E1, E2	Does recorded value reconcile to the authoritative liability total, can cross-layer gaps be detected, and do retries avoid duplicate value movement?
G2 — Finality-bound recovery	E2	Can a transfer be cancelled before finality and, after finality, recovered exactly once under the tested interruptions?
G3 — Controlled unavailability	E3	When must the limits be checked, how much value remains unavailable, and what rejection or cancellation cost follows?
G4 — Independent verifiability	E4	Can exported evidence determine whether any transfer is incomplete and reconstruct totals, histories, receipts and responsible roles?
Operating envelope	E5	What latency, throughput and notary-verification cost were observed in the prototype? These are not production-capacity estimates.

5. Implementation and Evaluation

5.1 Prototype and evaluation scope

We built a single-bank prototype connecting an Agorá-derived platform to Bank K's internal token ledger. It implements the two token ledgers, BridgeBook and the issuer liability record; that record supplies T, while production of T by core banking is outside scope. Role-separated credentials, an issuer/notary verifier, signed receipts and ledger evidence support independent ex post verification.

Measurements used local Paladin/Noto and Besu QBFT networks, with both ledger legs reaching finality through Byzantine fault-tolerant (BFT) consensus. The measurements provide a laboratory baseline under Configuration A; they are not estimates of production capacity. Multibank and non-EVM deployments were not tested.

5.2 E1 — Liability conservation and reconciliation

E1 tested 100 transfers, 50 in each direction, with endpoint outages and an orchestrator restart. A separate read-only invariant checker reconstructed T from five authorised issuance and redemption events and evaluated §4.4's conservation invariant at 546 consistent snapshots, using bridge states backed by verified ledger evidence. All transfers reached `CLOSED`. At every snapshot, the

platform, source-burned in-flight and internal records summed to T; all final receipts linked destination mints to burns without liability-lineage errors.

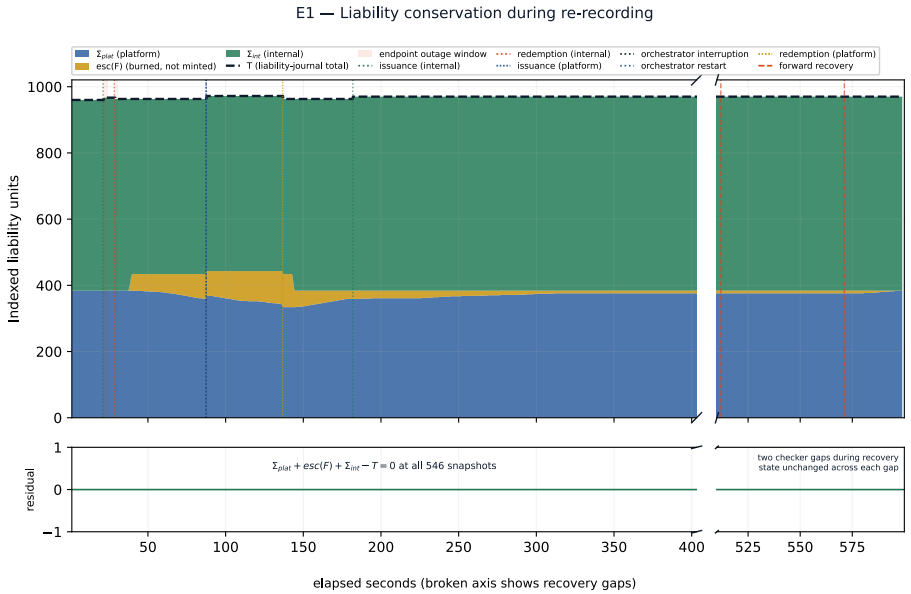

Figure 5. Conservation during re-recording: all 546 snapshots reconciled to T. The broken axis discloses two gaps in the invariant checker's observations during recovery; durable bridge state was unchanged across each.

Reconciliation was tested against four discrepancies involving mints or burns without matching BridgeBook or issuer liability records. Ordinary workflow checks missed all four, while the §4.5 file-only reconciler detected them by comparing both token ledgers, BridgeBook and the issuer liability record. Cross-layer reconciliation detects unrecorded issuance and unmatched ledger events, but does not prevent them and depends on complete exports.

E1 therefore supports conservation only within the recorded workflow; it does not establish legal identity or record completeness. The rulebook must designate the authoritative source of T and require reconciliation across both token ledgers, BridgeBook and the issuer liability record. The experiment does not determine how core banking produces T, access to funds during an incomplete transfer or legal finality.

5.3 E2 — Finality boundary and recovery

E2 used the durable `ARMED → TRIGGERED` transition as the technical finality boundary. Four one-unit transfers covered both directions: one pre-trigger cancellation and one post-trigger hold followed by recovery in each direction. All

22 checks passed. Before the trigger, source-lock release restored spendable balance and allowed cancellation; after the trigger, cancellation failed and recovery was forward-only.

During the post-burn holds—2.546 seconds internal-to-platform and 5.134 seconds in reverse—the transferred unit remained accounted for in transit, keeping the inventory residual at zero, but was not yet spendable on the destination ledger ($U(F) = 1$). Recovery closed both transfers, returned $U(F)$ to zero and produced two valid offline receipts.

Figure 6 shows recovery after mint attempts failed during separate execution-client outages.

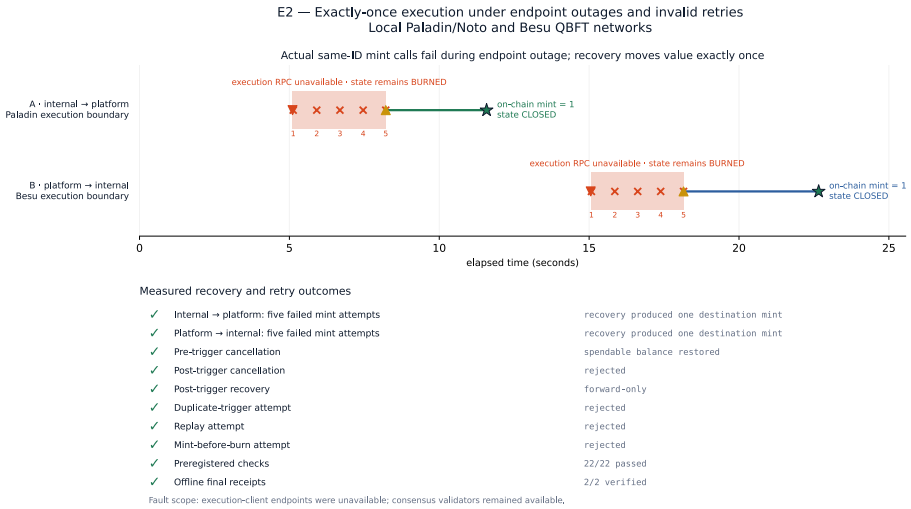

Figure 6. Post-burn recovery. Five mint attempts per direction failed safely during execution-client outages of about 3.1 seconds; recovery produced one destination mint per transfer. The tested duplicate-trigger, replay and mint-before-burn attempts were rejected.

The trigger separates reversible preparation failures from post-trigger completion duties. The rulebook must set the trigger's legal effect, completion deadlines, monitoring and responsibility for unavailable value. E2 did not test prolonged or malicious non-completion, selective notary rejection, validator halts, legal finality or production service levels.

5.4 E3 — Exposure-control comparison

E3 asked when limits must be checked to keep unavailable funds within a chosen bound. It compared four policies: no cap, review after finality, a check immediately before finality, and checks both before locking and before finality. Each policy was tested at $P = C$ of one, two and four units, with two one-unit offers

in each direction: four policies × three settings × two directions × two offers, giving 48 offers in total.

At $P = C = 1$, no cap and post-finality review let unavailable value reach two. A finality-stage check capped post-finality exposure at one but allowed two units to be locked; across both directions, two of four offers completed and two were cancelled. The two-stage check kept all unavailable-value measures at or below one; two offers completed and two were rejected before locking.

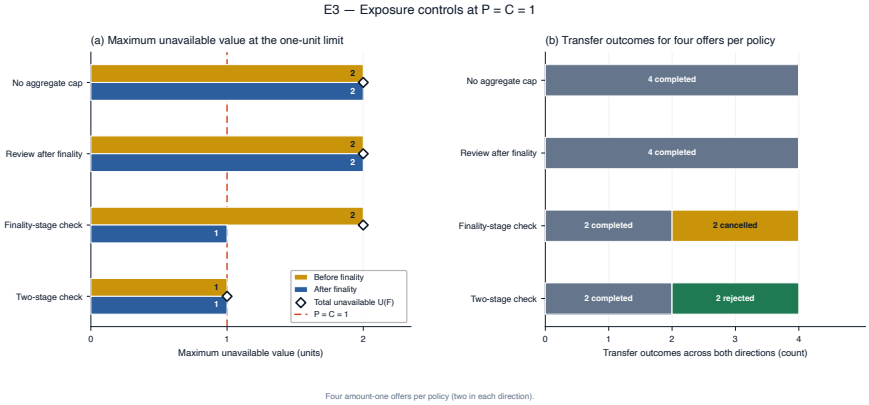

Figure 7. Exposure and outcomes at a one-unit limit. The finality-stage check capped only post-finality exposure; the two-stage check also capped total unavailability. Tests used one non-bypassing gateway and serialised aggregate state.

Across all policy and limit settings, 44 of the 48 offers completed, two were cancelled and two rejected. All completions had valid evidence, no capacity reservation remained, and four restart tests closed without duplicate value movement or leaked capacity.

Among the tested policies, only the two-stage check kept both pre- and post-finality unavailable value within the one-unit limit. Tighter limits reduce exposure but increase rejection or cancellation. The rulebook must choose P/C and how rejected or cancelled transfers are handled. E3 did not test production capacity, multiple gateways, database or validator failure, bounded recovery time or malicious operation.

5.5 E4 — Independent supervisory verification

E4 asked whether an authorised supervisor could verify the bridge from exported files alone, using a read-only verifier without live access to the database, ledger RPC or orchestrator.

Table 7 lists the six supervisory targets and the evidence used to verify them.

Table 7. Supervisory targets verified from exported evidence.

Supervisory target	Evidence required
Liability total and residual	Ledger totals and issuer liability record
Current incomplete transfers and age	BridgeBook rows and transition logs
Oldest incomplete transfer	BridgeBook rows and transition logs
Pre-/post-trigger and total unavailable-value histories	Reservation and transition histories
Receipts and used identifiers	All 46 receipts and used-identifier records
Exception responsibility	Signed append-only exception log (10 records)

All transfers were complete when the files were exported. The two incomplete-transfer targets therefore returned empty results; they did not test the ageing of a transfer that remained incomplete.

Totals and histories alone were insufficient. Adding all 46 receipts and used-identifier records enabled receipt verification; every receipt and identifier passed. Adding a signed append-only exception log enabled exception attribution: all 10 records matched their identifiers, signatures and role and exception-code rules. Incomplete receipt and identifier records left receipt verification partial, while success-only logs could not establish exception responsibility.

E4 verified all six targets from the completed evidence export without live system access. It used records exported at one point in time and did not test continuous supervisory access, which would require an independent node or external replication. One implementation gap remains: receipt verification did not compare the authorised destination with the destination recorded on the ledger.

5.6 E5 — Prototype operating baseline

E5 used 130 transfers to locate the normal-operation bottleneck and measure the notary verification path's cost, providing a local operating baseline.

All transfers reached `CLOSED`; all 260 ledger receipts and 130 final receipts verified, with no errors or application retries. At concurrency one, median end-to-end latency was 5.241 seconds internal-to-platform and 5.204 seconds in reverse (99th-percentile values 6.348 and 5.943 seconds). Chain finality accounted for about 97–98% of the medians. The trigger operation itself had medians of 66.6 and 63.9 milliseconds; this technical timing is not a finding of legal finality. Full notary acceptance—including evidence verification and recording that the

transfer identifier had been used—had medians of 15.949 and 15.356 milliseconds, about 0.3% of single-transfer latency.

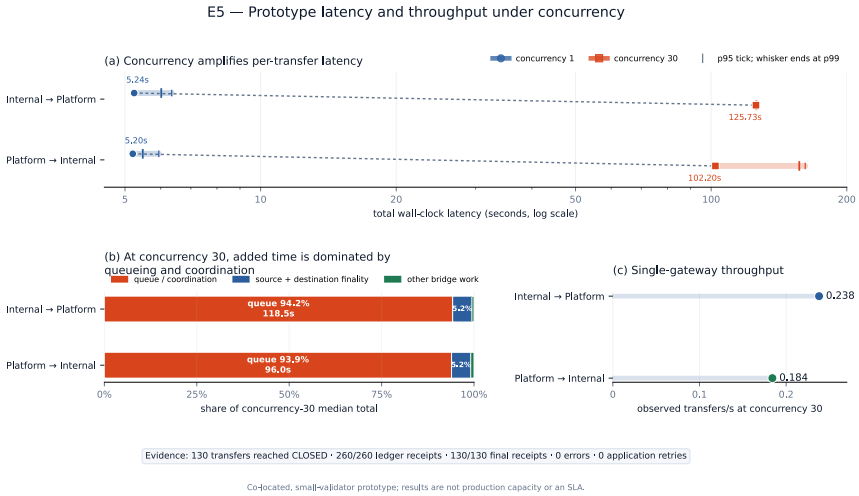

Figure 8. E5 operating envelope. At concurrency 30, median latency reached 125.7 seconds internal-to-platform and 102.2 seconds in reverse, while throughput was 0.238 and 0.184 transfers per second. Queueing and coordination accounted for about 94%; chain finality's smaller share reflects longer queues, not faster finality. This is a prototype implementation bottleneck, not a QBFT limit.

These co-located, small-validator results are not production capacity or an SLA. The run did not isolate the latency cost of the P/C gates, evidence export or recovery.

Section 6 derives legal, governance and supervisory requirements from these results and their limits.

6. Legal and Policy Implications

The technical results in Section 5 support a policy conclusion: the bridge can implement controls and produce evidence of their operation, but it cannot give them legal authority or allocate institutional responsibility. This section therefore identifies what applicable law, account terms, the rulebook and operating arrangements must establish before deployment. It moves from liability identity and record authority (§6.1), through finality and post-trigger completion responsibility (§6.2), to operational authority and supervisory verification (§6.3), before consolidating five minimum policy requirements and their limits (§6.4).

6.1 Liability Identity and Reconciliation

The bridge's accounting framework begins with a legal premise: the platform token and the internal token are records of the same Bank K deposit liability, not separate claims. This premise must be established by applicable law, account terms and system rules. The bridge code cannot create that legal identity; the conservation equation can only test whether the records remain consistent with it. If either token represents a separate claim, the analysis does not apply.

Once the same-claim premise is established, policy must distinguish the record that fixes the total liability from the records showing a transfer's progress. The issuer liability record supplies the authoritative total T. The two token ledgers show where the liability is represented, while BridgeBook records the transfer's progress. The rulebook should designate the authoritative source of T, require independent reconciliation across all four record layers, and assign responsibility for investigating, resolving and reporting discrepancies. Reconciliation should remain possible independently of the bridge operator.

Section 5.2 provides limited technical support for this framework: the recorded workflow preserved the total, while independent reconciliation detected the tested events outside that workflow. This demonstrates that the proposed control can reveal inconsistencies. It does not establish legal identity, prove that the issuer's records are complete or prevent activity outside BridgeBook. Whether the two representations continue to constitute the same deposit for insurance and resolution purposes remains a jurisdiction-specific legal question [18, p. 16], [29, Legal Report, pp. 75–76, 96].[1]

The policy implication is that both ledger records must refer to the same legally defined claim. The amounts recorded on the two ledgers, together with value recorded as in transfer, must reconcile to the authoritative total T. This requirement can show that value remains accounted for, but not whether the transfer principal can use the funds while the transfer remains incomplete. Section 6.2 addresses that separate question.

6.2 Finality, fund availability, and completion duties

Liability identity and reconciliation address whether value remains accounted for across the two ledgers. A separate policy question arises once a transfer passes the trigger: can the transfer principal use the funds before destination recording is complete? Sections 5.3–5.4 showed that conservation can hold while the answer is no, and that bounding this unavailable-funds exposure requires controls both before locking and immediately before the trigger. The policy concern is therefore not a brief processing delay itself, but that the transfer principal can no longer cancel while completion may remain uncertain. With-

[1] Reference [29] is a preliminary New York-law analysis of a different proof-of-concept structure. It is used only for general legal conditions, not as authority that its conclusions apply directly to this bridge.

out limits and completion duties, unavailable value can accumulate even while accounting remains correct.

Agorá provides the design starting point: applicable rules may give legal significance to an atomic settlement trigger although subsequent ledger updates are asynchronous [1, p. 65], [50, p. 16]. In this bridge, `ARMED → TRIGGERED` is only the technical boundary between cancellation and forward completion. Applicable law, account terms and the rulebook must determine whether it makes the bridge leg legally irrevocable. Whether that designation survives insolvency is a separate jurisdictional question [29, Legal Report, p. 44 and fn. 169]. It must be validated under the law governing the bridge and the underlying deposit relationship.

Policy must therefore pair the finality rule with availability protection. P limits value admitted before the trigger, C limits triggered-but-unclosed value, and τ identifies a `BURNED` transfer whose age requires escalation. The rulebook should assign a completion owner and deadline, require monitoring and status reporting, specify pause and restart authority, and provide restoration or compensation for prolonged delay. These values are policy choices, not prototype results; tighter limits reduce exposure but increase rejection or cancellation.

The experiments show that recovery and exposure controls are feasible under the tested conditions. They do not establish legal finality, a production service level or compulsory completion against deliberate withholding. Section 6.3 addresses the authority and evidence needed to apply these rules.

6.3 Authority, Operating Rules, and Supervisory Verification

The completion and exposure rules in §6.2 are effective only if the rulebook identifies who may apply, pause and review them. The bridge can separate keys, require signatures and preserve evidence so that actions are attributable. It cannot decide which institution should hold each power or bear legal responsibility.

The model places the control plane within Bank K because the bank controls the liability and its two ledger representations. Within that arrangement, compliance approval, trigger authorisation, ledger execution, notary verification, cancellation or pause, restart and audit remain distinct logical authorities. The rulebook should assign who may screen and lock a transfer, issue the trigger, execute the burn and mint, cancel before the trigger, pause new admissions, restart after failure, approve exceptions and rotate keys. No operational role should simultaneously approve the trigger, execute both ledger legs and control the evidence. Audit access should remain read-only. Any emergency supervisory power must be separately authorised rather than inferred from audit access.

This does not make bank-by-bank operation mandatory. Direct bank operation, vendor-supported hosting and shared services are institutional options. Any

provider with access to the bridge endpoints, BridgeBook or transfer sequencing occupies the corresponding trust role and must be governed accordingly. Whichever model is selected must preserve issuer accountability, separated keys and verification paths, attributable actions and evidence availability. E4 (§5.5) and E5 (§5.6) did not compare these operating models or test tenant isolation.

E4 showed that supervisory verification required complete receipts, records showing that transfer identifiers had been used, and contemporaneous signed exception records; success-only logs were insufficient. These records support attribution, not prevention or allocation of legal responsibility. The rulebook must set the scope and frequency of access, confidentiality conditions and retention periods. Evidence should be read-only or independently exportable, while continuing access requires an independent node or external replication. E4 did not test minimised disclosure or continuous availability. E5 showed only that the prototype's full notary-acceptance path was not the measured bottleneck; it did not measure the cost of supervisory verification or establish a production service level. Section 6.4 consolidates these findings into minimum policy requirements and states their limits.

6.4 Policy Requirements and Limits

Sections 6.1–6.3 show that technical controls cannot produce legal or institutional outcomes on their own. Deployment therefore depends on five minimum requirements. These are a policy agenda, not a complete rulebook.

- **R1 — Liability identity and reconciliation.** Applicable law, account terms and system rules must establish that both token records represent the same issuer deposit liability. The rulebook must designate the authoritative source of T, require independent reconciliation of both token ledgers, BridgeBook and the issuer liability record, and assign responsibility for resolving and reporting discrepancies.
- **R2 — Finality rule.** The applicable framework must state whether and when the durable trigger makes the bridge leg irrevocable and how the underlying claim is treated after the trigger but before destination recording is complete. Any effect in insolvency must be validated under the governing law; the rulebook cannot create that protection by itself.
- **R3 — Availability and completion protection.** The rulebook must set the limits P and C and the age threshold τ for a `BURNED` transfer, together with a completion owner and deadline, monitoring and status-reporting duties, escalation procedures, and a route to restoration or compensation following prolonged non-completion.
- **R4 — Authority separation and accountability.** Trigger approval, token execution, cancellation, pause and restart, exception approval, key rotation and audit must be separately authorised and attributable. Direct, vendor-supported or shared operation may be used, but the selected model

must preserve issuer accountability and separated keys and verification paths. One operational role must not control the trigger, both ledger legs and the evidence.

- **R5 — Independent supervisory verification.** At the frequency specified in the rulebook, authorised supervisors or independent verifiers must be able to verify liability totals, incomplete transfers and their age, unavailable-value exposure, final receipts, use of transfer identifiers and exceptions. Evidence must be read-only or independently exportable. The rulebook must specify access scope, confidentiality, retention and how evidence remains available following an operational failure.

The prototype supports these requirements under the tested single-bank conditions but does not determine their legal effect, production parameters or preferred operating model. Technology can implement the controls and preserve evidence; law, the rulebook and operating arrangements must set limits and deadlines, assign responsibility and ensure continuity. Section 7 defines the remaining limits.

7. Contribution and Limitations

This paper tests one of several ways to connect two ledgers: a bridge operated under the issuing bank's authority that prepares both sides before triggering a transfer. It asks whether one deposit liability can remain accounted for, unavailable funds can be limited, and supervisors can verify the result. Under the tested conditions, the answer is yes. The limits below define the reach of that finding.

7.1 Implementation feasibility and operational limits

Under the single-bank test conditions, conservation, recovery, unavailable-value controls and independent verification were implemented and evaluated within one prototype. This establishes integrated feasibility, not production readiness. The prototype used small, co-located validator networks and one gateway that updated the aggregate state one transfer at a time. Recovery followed tested endpoint outages and selected process restarts because components returned and the operator continued. Consensus or database failures, competing gateways, prolonged outages, deliberate withholding or reordering, and cases in which the notary selectively rejected some requests were not tested. The P/C bounds likewise depended on every transfer passing the same controls and on aggregate updates being processed one at a time; production values for P, C, τ and recovery time remain to be set.

E4 reconstructed exported records at one cutoff, when no transfer was incomplete; its ageing result was therefore not a live test of prolonged non-completion. Minimised disclosure and continuous supervisory access were not tested. E5 is a local operating baseline, not an SLA or an estimate of production capacity. The

receipts did not verify that the destination in the authorised transfer instruction matched the destination recorded on the ledger. A production deployment must therefore retest the controls against its own infrastructure, fault model and operating arrangements.

7.2 Legal and Institutional Conditions

Technical feasibility does not determine the legal status of the two token records. The analysis assumes that both record the same Bank K deposit liability. Applicable law, account terms and system rules must determine whether they constitute the same claim, how it is treated in insurance, resolution and insolvency, and what legal effect attaches to the trigger. R1–R5 identify those required decisions; they are not experimentally validated legal rules.

The file-only reconciler described in §4.5 and tested in §5.2 detected all four tested events outside the recorded workflow that existing checks missed. This supports cross-layer detection, not prevention or completeness, because it depends on the exported records supplied to it. Signed evidence attributes actions to roles but does not allocate legal responsibility.

The experiments also did not compare direct bank operation, vendor-supported hosting or shared services. Multibank and non-EVM deployments, and the inferences available to an observer with access to both ledgers, likewise remained outside the experimental scope. Systems representing separate claims require different analysis.

The paper's contribution is an evidence-based policy framework for vertical interoperability. It shows how the required technical controls can be implemented and evaluated within one prototype and translates those results into legal, governance and supervisory requirements for deployment. Rather than prescribing one institutional model, it defines the requirements that any chosen model must satisfy. Section 8 states the resulting conclusion and priorities for deployment.

8. Conclusion and Priorities for Deployment

This paper addresses a specific last-mile problem: how a bank can re-record one deposit liability between its internal token ledger and a shared settlement platform. Under the tested single-bank conditions, an issuer-operated prepare-then-trigger bridge kept recorded value reconciled, recovered from specified interruptions without duplicate value movement, bounded unavailable value through two-stage controls and produced independently verifiable evidence. The contribution is not one isolated mechanism: these controls were implemented and evaluated within one prototype.

The policy implication follows from the difference between correct accounting and access to funds. A conserved total does not by itself protect a transfer principal who can neither use the funds nor cancel after the trigger. Deployment

therefore requires one coherent framework: both token records must represent the same legal claim and reconcile to T; the trigger must have a defined legal effect and be paired with exposure limits and completion responsibility; operational powers must be separated; and supervisors must receive independently verifiable evidence. Section 6.4 expresses this framework as R1–R5. Technology can implement the controls, but law, the rulebook and operating arrangements must give them effect, set their parameters and allocate responsibility.

Before deployment, institutions must test these controls in their intended infrastructure and turn the framework into binding legal, operational and supervisory rules. That work must set limits and service commitments, assign completion and remedy duties, select an accountable operating model, and ensure continuing and proportionate evidence access. An accountable connection between a shared platform and a bank's internal ledger requires accounting, finality, access to funds, authority and evidence to be designed together. From a participating commercial bank's perspective, the bridge is the last-mile interface to shared settlement infrastructure developed through collaboration among central banks and regulated financial institutions.

References

[1] Bank for International Settlements, *Project Agorá: A shared programmable platform for wholesale cross-border payments.* Basel: BIS, 27 May 2026. [Online]. Available: https://www.bis.org/publ/othp110.htm (accessed 30 Aug. 2026).

[2] Bank for International Settlements and Institute of International Finance, "Project Agorá shows how tokenisation can improve wholesale cross-border payments; work will advance to real-value testing," press release, 27 May 2026. [Online]. Available: https://www.bis.org/press/p260527.htm (accessed 28 Jul. 2026).

[3] BIS Innovation Hub, "Project Agorá — Real value testing," web page (undated). [Online]. Available: https://www.bis.org/about/bisih/topics/fmis/agora/rvt.htm (accessed 31 Jul. 2026).

[4] Bank for International Settlements, "III. Blueprint for the future monetary system: Improving the old, enabling the new," in *BIS Annual Economic Report 2023.* Basel: BIS, Jun. 2023, pp. 85–118.

[5] Citigroup, "Citi Token Services marks new milestone in delivering next gen transaction banking services to institutional clients," press release, 10 Oct. 2024. [Online]. Available: https://www.citigroup.com/global/news/press-release/2024/citi-token-services-marks-new-milestone (accessed 28 Jul. 2026).

[6] HSBC, "HSBC launches Tokenised Deposit Service for corporate cash management in Hong Kong," press release, 22 May 2025. [Online]. Available: https://www.about.hsbc.com.hk/news-and-media/hsbc-launches-tokenised-

deposit-service-for-corporate-cash-management-in-hong-kong (accessed 28 Jul. 2026).

[7] J.P. Morgan Payments (Kinexys), "First bank issues USD deposit token on a public blockchain," newsroom article, 12 Nov. 2025. [Online]. Available: https://www.jpmorgan.com/payments/newsroom/jpm-coin-usd-deposit-token-institutional-clients (accessed 28 Jul. 2026).

[8] UBS, "UBS successfully pilots blockchain-based multi-currency payment solution with UBS Digital Cash," press release, 7 Nov. 2024. [Online]. Available: https://www.ubs.com/global/en/media/display-page-ndp/en-20241107-ubs-digital-cash.html (accessed 28 Jul. 2026).

[9] Dunamu, "두나무, 하나금융그룹과 '기와체인' 활용 해외송금 서비스 검증 완료 [Dunamu completes verification of a GIWA-chain remittance service with Hana Financial Group]," press release (in Korean), 27 Feb. 2026. [Online]. Available: https://www.dunamu.com/news/1651 (accessed 7 Aug. 2026).

[10] BNY, "BNY extends digital cash capabilities for institutional clients," company news, 9 Jan. 2026. [Online]. Available: https://www.bny.com/corporate/global/en/about-us/newsroom/company-news/bny-extends-digital-cash-capabilities-for-institutional-clients.html (accessed 30 Aug. 2026).

[11] Bank of Korea, "디지털화폐 (CBDC) — 프로젝트 한강 [Digital currency (CBDC) — Project Han River]," web page (in Korean). [Online]. Available: https://www.bok.or.kr/portal/submain/submain/cbdc.do (accessed 7 Aug. 2026).

[12] Swiss Bankers Association, "Milestone for the Swiss financial center: Deposit token proof of concept successfully completed," press release, 16 Sep. 2025. [Online]. Available: https://www.swissbanking.ch/en/media-politics/press-releases/milestone-for-the-swiss-financial-center-deposit-token-proof-of-concept-successfully-completed (accessed 30 Aug. 2026).

[13] Korea Internet & Security Agency (KISA), "'블록체인 기반 예금토큰 결제 인프라 확산' 사업 발대식 개최 ['Blockchain-based deposit-token payment infrastructure expansion' project launch ceremony held]," press release (in Korean), 22 Jul. 2026. [Online]. Available: https://www.kisa.or.kr/402/form?postSeq=2618 (accessed 30 Aug. 2026).

[14] A. R. Hevner, S. T. March, J. Park and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, Mar. 2004, doi: 10.2307/25148625.

[15] R. Garratt and H. S. Shin, "Stablecoins versus tokenised deposits: Implications for the singleness of money," *BIS Bulletin*, no. 73, 11 Apr. 2023.

[16] Bank for International Settlements, "III. The next-generation monetary and financial system," in *BIS Annual Economic Report 2025*. Basel: BIS, Jun. 2025, pp. 77–114.

[17] Bank for International Settlements, "III. Anchoring trust in money: Innovation beyond stablecoins," in *BIS Annual Economic Report 2026*. Basel: BIS, Jun. 2026, pp. 77–121.

[18] Financial Stability Board, *The Financial Stability Implications of Tokenisation*. Basel: FSB, 22 Oct. 2024.

[19] Bank for International Settlements and Committee on Payments and Market Infrastructures, *Tokenisation in the context of money and other assets: Concepts and implications for central banks — Report to the G20*. Basel: BIS, Oct. 2024.

[20] Paladin (LF Decentralized Trust), "Noto — Notarized tokens," Paladin architecture documentation. [Online]. Available: https://lfdt-paladin.github.io/paladin/head/architecture/noto/ (accessed 14 Aug. 2026).

[21] Bank for International Settlements, Banque de France and Swiss National Bank, *Project Jura: Cross-border settlement using wholesale CBDC*. Basel: BIS, Dec. 2021. ISBN 978-92-9259-525-8 (online).

[22] BIS Innovation Hub, Hong Kong Monetary Authority, Bank of Thailand, Digital Currency Institute of the People's Bank of China and Central Bank of the United Arab Emirates, *Project mBridge: Connecting economies through CBDC*. Basel: BIS, Oct. 2022.

[23] BIS Innovation Hub, Banque de France, Monetary Authority of Singapore and Swiss National Bank, *Project Mariana: Cross-border exchange of wholesale CBDCs using automated market-makers — Final report*. Basel: BIS, Sep. 2023.

[24] Bank for International Settlements, "Project mBridge reaches minimum viable product stage and invites further international participation," press release, 5 Jun. 2024. [Online]. Available: https://www.bis.org/press/p240605.htm (accessed 28 Jul. 2026).

[25] BIS Innovation Hub, Bank of England, Banque de France, Banca d'Italia, Deutsche Bundesbank and European Central Bank, *Project Meridian FX: Exploring synchronised settlement in FX*. Basel: BIS, 24 Apr. 2025.

[26] BIS Innovation Hub, SIX Group and Swiss National Bank, *Project Helvetia Phase II: Settling tokenised assets in wholesale CBDC*. Basel: BIS, Jan. 2022. ISBN 978-92-9259-524-1 (online).

[27] T. Sookdeo, "Unlocking blockchain's potential with Kinexys Digital Payments," J.P. Morgan Payments Developer Portal, 7 Jan. 2025 (updated 18 Feb. 2025). [Online]. Available: https://developer.payments.jpmorgan.com/blog/guides/blockchain (accessed 12 Aug. 2026).

[28] DBS Bank and Kinexys by J.P. Morgan, "DBS and Kinexys by J.P. Morgan to develop framework for interbank tokenised deposit transfers across multiple blockchains," press release, 11 Nov. 2025. [Online]. Available: https://www.dbs.com/newsroom/DBS_and_Kinexys_by_JP_Morgan_to_develop_framewo

rk_for_interbank_tokenised_deposit_transfers_across_multiple_blockchains (accessed 28 Jul. 2026).

[29] Securities Industry and Financial Markets Association (SIFMA), *Regulated Settlement Network (RSN) Proof of Concept: Business Applicability Report; Legal Viability Report; Technical Feasibility Report*, 3 vols. New York: SIFMA, 5 Dec. 2024. [Online]. Available: https://www.sifma.org/research/white-papers/regulated-settlement-network-proof-of-concept (accessed 28 Jul. 2026). (Legal Viability Report prepared by Sullivan & Cromwell LLP.)

[30] The Clearing House, "Major financial institutions unveil bank-led on-chain money initiative," press release via PR Newswire, 5 Jun. 2026. [Online]. Available: https://www.prnewswire.com/news-releases/major-financial-institutions-unveil-bank-led-on-chain-money-initiative-302792661.html (accessed 12 Aug. 2026).

[31] Hong Kong Monetary Authority, "HKMA announces the new phase of Project Ensemble to support real-value transactions in tokenised deposits and digital assets," press release, 13 Nov. 2025. [Online]. Available: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2025/11/20251113-3/ (accessed 29 Jul. 2026).

[32] HSBC, "HSBC completes first live cross-bank transaction in EnsembleTX," press release, Hong Kong, 13 Nov. 2025. [Online]. Available: https://www.about.hsbc.com.hk/news-and-media/hsbc-completes-first-live-cross-bank-transaction-in-ensembletx (accessed 29 Jul. 2026).

[33] Digital Asset and Kinexys by J.P. Morgan, "Digital Asset and Kinexys by J.P. Morgan announce intention to bring USD JPM Coin (JPMD) natively to the Canton Network," press release, 7 Jan. 2026. [Online]. Available: https://blog.digitalasset.com/news/digital-asset-and-kinexys-by-j.p.-morgan-bring-usd-jpm-coin-jpmd-natively-to-canton (accessed 30 Aug. 2026).

[34] M. Herlihy, "Atomic cross-chain swaps," in *Proc. 2018 ACM Symp. Principles of Distributed Computing (PODC '18)*, Egham, U.K., Jul. 2018, pp. 245–254, doi: 10.1145/3212734.3212736.

[35] K. Narayanam, V. Ramakrishna, D. Vinayagamurthy and S. Nishad, "Atomic cross-chain exchanges of shared assets," in *Proc. 4th ACM Conf. Advances in Financial Technologies (AFT '22)*, Cambridge, MA, USA, Sep. 2022, pp. 148–160, doi: 10.1145/3558535.3559786. (arXiv:2202.12855.)

[36] V. Zakhary, D. Agrawal and A. El Abbadi, "Atomic commitment across blockchains," *Proc. VLDB Endow.*, vol. 13, no. 9, pp. 1319–1331, May 2020, doi: 10.14778/3397230.3397231.

[37] A. Augusto, R. Belchior, M. Correia, A. Vasconcelos, L. Zhang and T. Hardjono, "SoK: Security and privacy of blockchain interoperability," in *Proc. 2024 IEEE Symp. Security and Privacy (SP)*, San Francisco, CA, USA, 2024, pp. 3840–3865, doi: 10.1109/SP54263.2024.00255.

[38] R. Belchior, A. Vasconcelos, S. Guerreiro and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Comput. Surv.*, vol. 54, no. 8, Art. 168, 41 pp., Oct. 2021, doi: 10.1145/3471140.

[39] A. Bhuptani, "The interoperability trilemma," Connext blog (Medium), 1 Oct. 2021. [Online]. Available: https://blog.connext.network/the-interoperability-trilemma-657c2cf69f17 (accessed 29 Jul. 2026).

[40] M. Zhang, X. Zhang, Y. Zhang and Z. Lin, "Security of cross-chain bridges: Attack surfaces, defenses, and open problems," in *Proc. 27th Int. Symp. Research in Attacks, Intrusions and Defenses (RAID '24)*, Padua, Italy, Sep. 2024, pp. 298–316, doi: 10.1145/3678890.3678894.

[41] J. Zhang, J. Gao, Y. Li, Z. Chen, Z. Guan and Z. Chen, "Xscope: Hunting for cross-chain bridge attacks," in *Proc. 37th IEEE/ACM Int. Conf. Automated Software Engineering (ASE '22)*, Rochester, MI, USA, Oct. 2022, pp. 1–4, doi: 10.1145/3551349.3559520. (arXiv:2208.07119.)

[42] E. Liu, E. Luo, J. C. Yan, K. Izhikevich, S. Grant, D. Stefan, G. M. Voelker and S. Savage, "Count of Monte Crypto: Accounting-based defenses for cross-chain bridges," arXiv:2410.01107 [cs.CR], 1 Oct. 2024 (preprint).

[43] Axelar, "ITS Hub — Introduction," Axelar developer documentation. [Online]. Available: https://docs.axelar.dev/dev/amplifier/its-hub/introduction (accessed 6 Aug. 2026).

[44] M. Sheth, "ITS hub balance tracking should be applied when minter isn't set," GitHub issue #270, axelarnetwork/interchain-token-service, 8 Aug. 2024. [Online]. Available: https://github.com/axelarnetwork/interchain-token-service/issues/270 (accessed 6 Aug. 2026).

[45] Circle, "CCTP technical guide," Circle Developer Docs. [Online]. Available: https://developers.circle.com/cctp/references/technical-guide (accessed 18 Aug. 2026).

[46] Y. He, "New ledgers, old topology: A structural framework for tokenized deposit interoperability," working paper, SSRN 7167501, 23 Jul. 2026. [Online]. Available: https://ssrn.com/abstract=7167501.

[47] Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (CPSS-IOSCO), *Principles for Financial Market Infrastructures*. Basel: BIS, Apr. 2012. ISBN 92-9197-108-1 (online). Principle 8, pp. 64–66; Principle 17, pp. 94–100.

[48] P. Helland, "Idempotence is not a medical condition," *Commun. ACM*, vol. 55, no. 5, pp. 56–65, May 2012, doi: 10.1145/2160718.2160734.

[49] T. Xie, J. Zhang, Z. Cheng, F. Zhang, Y. Zhang, Y. Jia, D. Boneh and D. Song, "zkBridge: Trustless cross-chain bridges made practical," in *Proc. 2022 ACM SIGSAC Conf. Computer and Communications Security (CCS '22)*, Los Angeles, CA, USA, Nov. 2022, pp. 3003–3017, doi: 10.1145/3548606.3560652.

[50] Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (CPMI-IOSCO), *Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements*. Basel: BIS, Jul. 2022. ISBN 978-92-9259-578-4 (online). §3.4, pp. 15–17.