twilight

Money clears the border. Trust gets detained.

Privacy, permissions and proof in interoperable finance

Dr Ksenia Shnyra · Lewis Tuff

research@twilight.co

ABSTRACT

A payment can leave one institution, cross a network and a jurisdiction, and arrive in seconds. What made it trustworthy does not arrive with it.

Whether the customer was screened, whether the asset was eligible, whether the receiver can prove either to its examiner: each is settled at origin and reopened on arrival. Current market activity, regulatory developments and recent BIS projects point to one pattern.

> Institutional tokenized volume concentrates inside perimeters where controls remain intact; once an asset crosses a boundary, those controls become harder to rely on.

BIS Project Mandala shows that privacy-preserving compliance proofs can be generated, while Project Tamga is exploring how those proofs can be verified across systems and jurisdictions. Yet we found no supervisory framework in the US or major international regimes under which a verified proof may stand as sufficient examination evidence that an obligation was met.

The proof is getting closer to becoming portable, but regulatory reliance is still stalling. To move beyond the current gap, we propose a narrow, supervised pilot to test when a verified proof should be accepted for regulatory reliance.

The pattern in the volume

$357bn
Broadridge repo per day, June 2026 — up 68% year on year

$3tn
Processed by Kinexys since launch

$350bn
Canton per day, across 700+ institutions

Institutional digital settlement is already a production infrastructure. Broadridge reported $357bn of repo a day in June 2026, up 68% year on year;[1] Kinexys has processed over $3tn since launch;[2] Canton reports $350bn a day across 700+ institutions.[3] What that volume has in common matters more than its size: it sits inside perimeters where one operator answers every question an institution needs answered.

That operating pattern is not new. Silvergate told the FDIC in 2021 that its settlement network had run “over 300,000 transactions” worth “in excess of $400.0 billion” in the first half of that year alone; the network closed in March 2023 as the bank failed.

Broadridge's platform serves 20 of 24 US primary dealers, yet those assets cannot reach other chains. Canton's EVM layer is still pre-mainnet as of August 2026. Even the scaled platforms show a ceiling: Broadridge's daily volume has run flat between $350bn and $384bn for three consecutive quarters after its growth run.[4] Where systems must connect, progress slows significantly. Even though SIFMA's cross-network proof of concept concluded in December 2024, it still did not move into production.

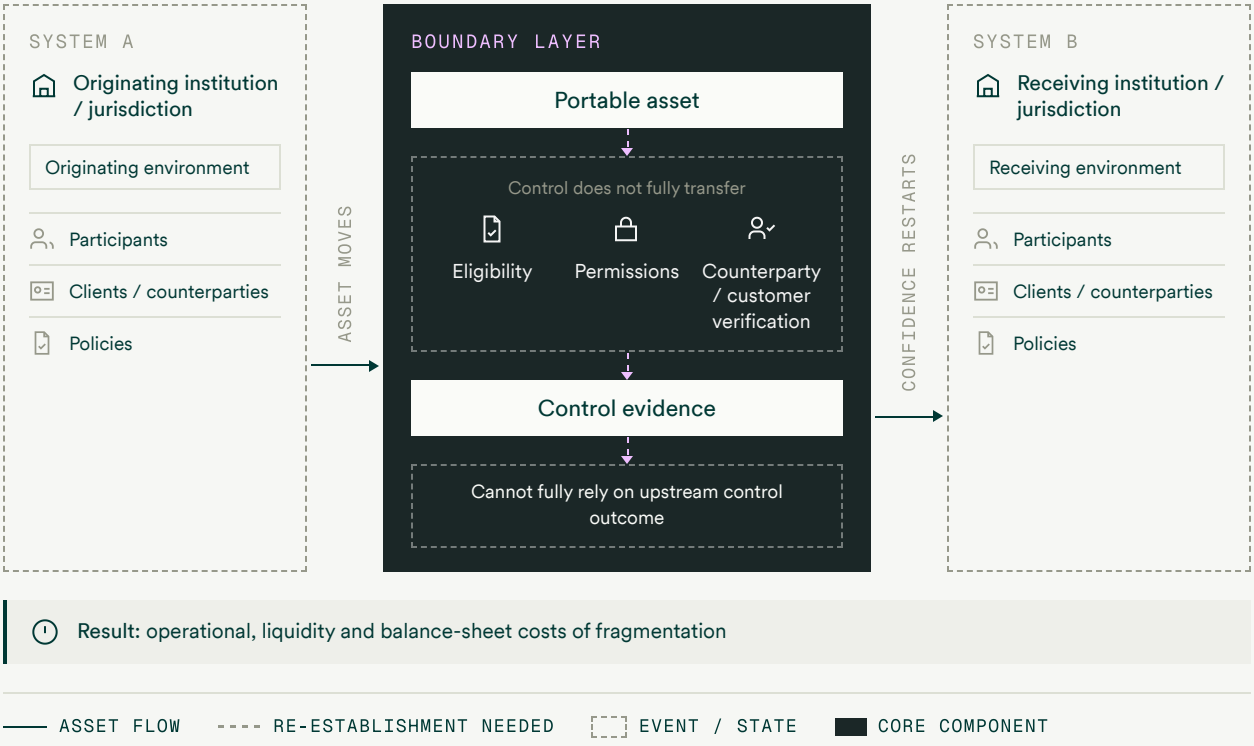
A natural experiment is running in public, and its two arms are easy to compare. On public chains, where the parties carry no regulatory obligations, value moves between systems continuously — one protocol, Circle's CCTP, carried an estimated 60% of bridged volume in early 2026.[5] Regulated institutions have the same movement layer available to them and barely use it: their cross-system volume, as distinct from the closed-perimeter volume described above, rounds to zero. Neither arm is constrained by the ability to move an asset. What separates them is whether the mover must answer for the controls attached to it.

The economic upside of integration is clear: CHIPS settles about $2tn of payments a day using roughly $96bn of funding, meaning each dollar of liquidity supports more than $20 of settlement. NSCC's netting shows the same compression from the other direction: $519tn of gross obligations reduced to $9tn settled in a year.[6] Economies like that exist only where one system sees all the obligations.[7]

The value of integration is not just speed; it is the ability to reuse liquidity rather than strand it at each boundary. Every boundary that forces institutions to re-establish controls gives up some of that leverage. Which raises the central question: why is the boundary costly to cross when the assets can cross it easily?

FIG. 01 **Trust boundary**

The asset can increasingly move. Trust has to be re-established.



02

Why the boundary holds

Four explanations are commonly offered by market practitioners; each falls short against the evidence.

01 **Legal construct.** Law does not fully explain why the boundary persists. SIFMA's legal workstream found no legal barrier, yet the cross-network project still did not ship.[8]

02 **Gaps in technology.** Technology does not fully explain it. The movement layer already works: VanEck's VBILL fund moves across four chains.[9]

03 **Mandates.** Mandates do not fully explain it. Dodd-Frank swaps clearing took roughly five years to reach 70% of eligible flow, while inside-perimeter volume has scaled without waiting for a rule.[10]

04 **Commercial incentive.** Commercial incentives can reinforce the boundary, but they do not fully explain it. Operators may have limited incentive to make controls portable beyond their own networks where interoperability reduces switching costs or weakens network effects. Yet incentive alignment alone has not been enough: USDF was a consortium whose members wanted interoperation and still failed to reach production, and the regional banks joining bank-governed networks name control, not economics, as the reason they chose a members-only system. Nor is the demand hypothetical: 44% of more than 300 institutions surveyed by ISDA and GDF expect to accept tokenized money market funds as collateral,[11] and firms such as HQLAx have built businesses around solving the frictions created when collateral cannot move efficiently across systems.[12]

The actual barrier lies in a fifth, sharper reality: the same asset, under the same law, from the same issuer, behaves differently on either side of a trust boundary. VBILL supplies the comparison. It moves across four chains, but its collateral eligibility is venue-specific: the token travels and the permission does not. Issuer, law and technology are held constant and only the boundary varies — as close to identification as this market permits. What changes at the crossing is not the asset, the law governing it, or the rails carrying it, but whether the controls attached to it are recognized on the other side. The failure is not in the movement of the asset but in the controls meant to move with it, and in whether they are recognized when they arrive.[13]

Those controls reduce to three questions a regulated institution's risk, compliance and operations functions must answer together.

01 **Who may see it?** Financial activity is confidential by default. A bank owes its clients discretion about their positions and its counterparties discretion about its own. Whatever carries the asset must carry that discretion.

02 **Who may act on it?** A restricted security may pass only to qualified buyers. A sanctioned party may not receive payment. A custodian may release assets only on proper instruction. These permissions are legal obligations expressed as software, and they bind wherever the asset goes.

03 **Who can prove what happened?** After the fact, an auditor, an examiner or a court must be able to establish what moved, when, to whom, and under whose authority. Evidence is a property of the system that holds the record.

One technical distinction runs under everything that follows, and it decides what a supervisor can verify. Access-control privacy holds data in cleartext and governs who may query it; when the access control fails, everything is exposed at once. Hardware-enforced privacy decrypts inside secure enclaves on validator machines; it fails with the hardware, and the failure is the same total exposure, as researchers showed in 2022 by extracting one such network's master decryption key through a processor vulnerability. Mathematically enforced privacy differs in kind: the ledger and its intermediaries hold only commitments and ciphertexts, so a breach yields no transaction contents — though even these systems leak timing and relationship patterns at boundaries. Only the third gives a supervisor something it can verify without taking custody of the data behind it.

> “A shared ledger does not require shared data. Privacy controls enable data sharing only when necessary and approved by participants, rather than by default.”
>
> BIS — PROJECT AGORÁ

Confidentiality breaks on public ledgers, where pending transactions can expose transaction intent or sensitive details before execution. The BIS's Project Agorá, run with seven central banks and more than forty financial institutions, reached the conclusion that the remedy is architectural. The work is advancing to real-value testing.[14]

Permissions break because they enforce only within the perimeter where they were written: at custodian boundaries, the guarantee degrades into manual repair. SEC filings show transfers failing when KYC records lapse. And proof was hard long before the blockchain: US repo became measurable at $12.6tn a day only once the OFR's collection began, on estimates that had missed roughly $700bn. The failure has a published price. The syndicated loan market's own documents charge for settlement delay, with compensation accruing at daily SOFR plus a spread adjustment of 11.448 basis points;[15] average par settlement still ran at roughly 22 days in early 2025,[16] on secondary volume that passed $1tn on a trailing-year basis in early 2026.[17]

> Tokenization as practiced today adds a second ledger to reconcile rather than removing one.

Even the largest tokenized money fund keeps its authoritative register off the chain: Franklin's on-chain fund discloses that its transfer agent “maintains the official record of share ownership”, with public blockchain networks running alongside traditional book-entry records. A holder reading the chain and an examiner reading the register are looking at two different documents. ICMA's primary-market work reaches the blunt conclusion that without standardized data models, distributed-ledger systems simply process inconsistent data faster. All three controls are foundational, but proof is where the constraint becomes most acute: what can now be demonstrated technically still exceeds what supervisors are prepared to recognize.[18]

Proof, verification, and reliance

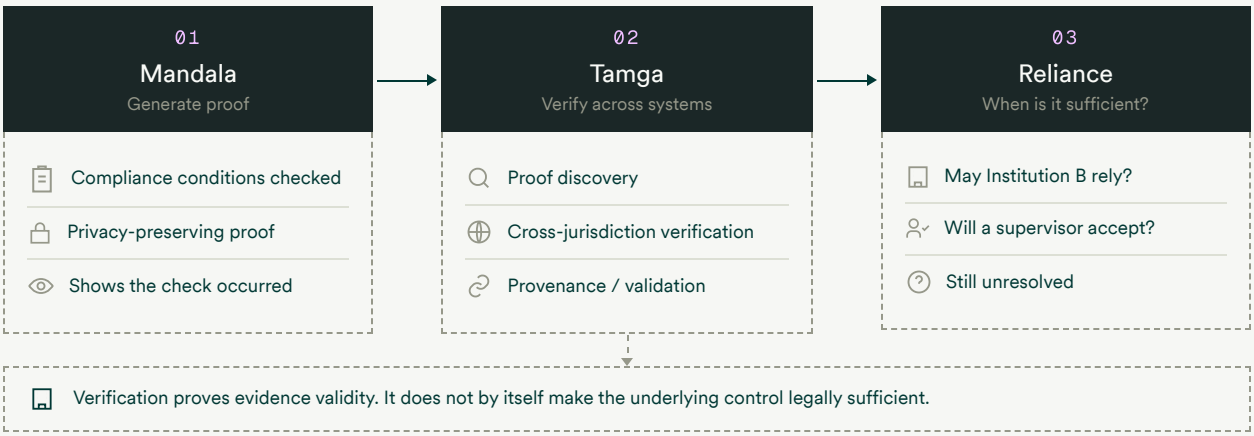
Cryptography answers the first two of those questions — who may see it, and who may act on it. Project Mandala demonstrated that jurisdiction-specific compliance requirements can be checked within a transaction, producing proof the check occurred without exposing the record. Project Tamga explores how proofs created under different systems and jurisdictions can be verified elsewhere.[19]

Mandala: Can I prove it?
Tamga: Can you verify it?

Neither can answer what a regulated institution must settle first: can I rely on it?

FIG. 02 **Proof, verification, reliance**

Mandala proves. Tamga supports cross-system verification, Regulation decides whether to rely.



Conceptual progression of capabilities, not an integrated architecture. Mandala and Tamga are separate BIS projects; neither resolves the policy question of regulatory reliance.

PROCESS FLOW SUPPORTS / ENABLES INFORMATION / STATE CORE COMPONENT

A valid proof is not a true fact, a true fact is not a trusted control, and a trusted control is not sufficient evidence.

Cryptography proves a computation over specified inputs; it cannot establish that those inputs were true, that the rule captured the right obligation, or that the issuer's controls were sound.

Verification settles provenance; reliance is a separate judgment, and it is the supervisor's.

None of this is blocked on the technology. Each of the three controls is already implemented in live or supervised environments. The access-control architectures that carry today's institutional volume are in production — Fnality, for example, has held central-bank funds for release on cryptographically authenticated instruction under a Bank of England settlement-finality designation since December 2024[20] — while the privacy-preserving cryptographic architectures have been proven in supervised pilots and are moving toward production. No cryptographic-privacy architecture yet carries production settlement volume at the scale of the access-control platforms. The remaining gap is increasingly one of engineering, governance and institutional design — who holds escalation authority, how revocation propagates across systems, and under what conditions another institution or supervisor can rely on the resulting control outcome — rather than one of basic technical feasibility.

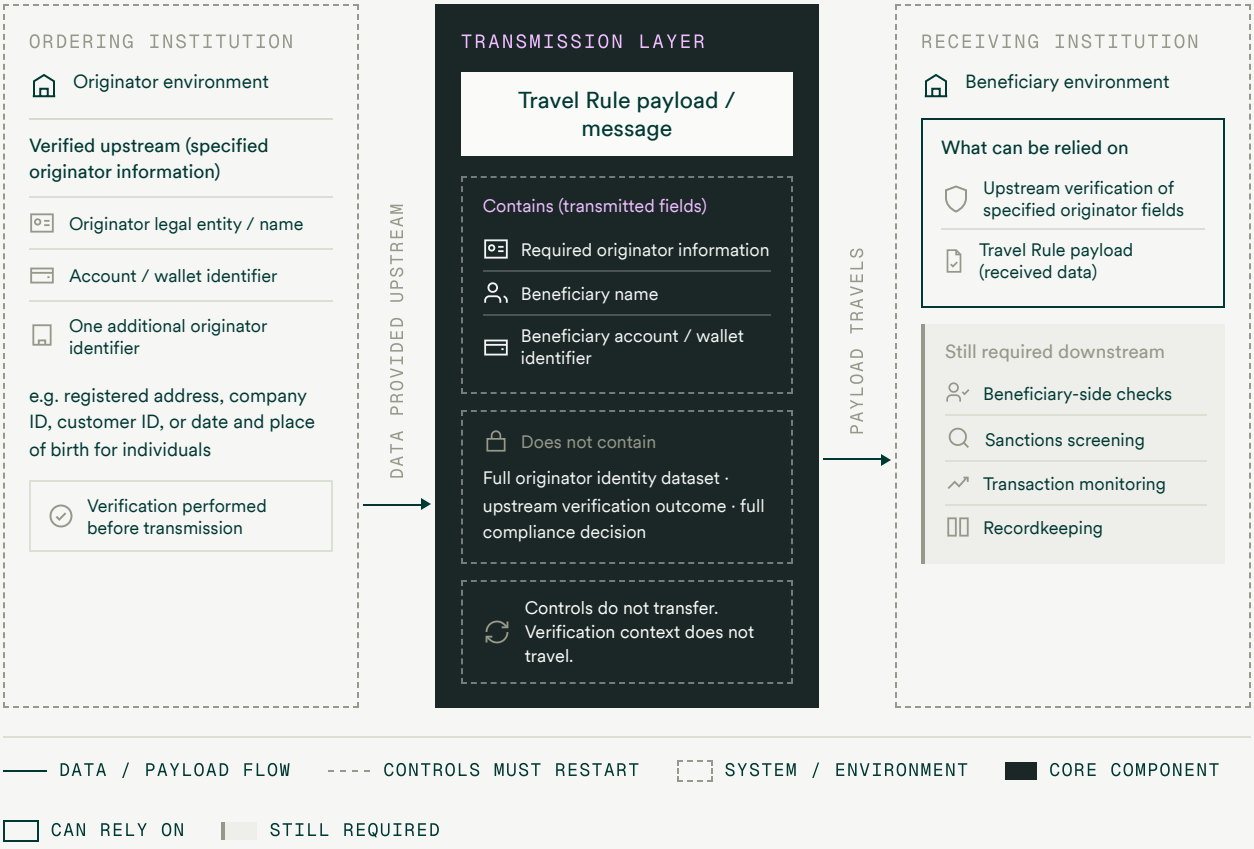
There are two precedents worth noting.

First, the 2022 amendments to SEC Rule 17a-4 accepted tamper-evident audit trails in place of write-once hardware, ending a standard that had held for twenty-five years. But that only recognizes proof that a record was not altered, not proof that an obligation was met.[21]

Second, the Travel Rule creates partial portability of verified identity data, not portability of the full compliance decision. The ordering institution verifies specified originator information and sends it with the transfer; the receiving institution can rely on that verification rather than re-check the same identity fields. But it still has to perform its own beneficiary-side controls, sanctions screening, transaction monitoring and recordkeeping. Some verified facts travel. The full compliance decision does not. The policy question is whether verifiable proof[22] can extend that existing reliance model to controls that today still have to be performed or evidenced again downstream.[23]

FIG. 03 **Travel Rule: partial portability**

Some verified facts travel. The full compliance decision does not.



That partial-reliance precedent is the starting point for our legal search: we looked for a broader framework that lets one regulated institution rely on a verified control outcome produced elsewhere, and came back empty-handed.

The review spanned SEC rules, releases and no-action letters; federal banking guidance; FinCEN rulemakings; FATF Recommendations; and the EU AML package and MiCA, looking specifically for an instrument that lets a regulated entity rely on verified proof instead of reproducing the underlying data. We found none in securities, banking, or AML; attestation-conditioned relief, such as the CFTC's stablecoin-margin letters, does not meet that test.[24]

The close cases show how far supervisors have gone without taking the step. Where a US jurisdiction mandates proof of reserves, the instrument it chose is an auditor's attestation. Where a US supervisor has approved cryptographic disclosure — New York, for shielded withdrawals with viewing-key access, in 2020 — the evidence remains the records the key reveals, not the proof.[25] FinCEN has issued nothing on proof-based compliance under the Bank Secrecy Act. FATF has studied privacy-enhancing technologies for anti-money-laundering work and still requires transmission of the underlying data itself.[26] The EU's AML Regulation carries one pseudonymisation safeguard for inter-bank information sharing at Article 75(4)(e) and otherwise treats anonymity as a risk, banning anonymity-enhancing coins outright at Article 79; it has no mechanism for approving a privacy technology for compliance use.[27] This negative is our own finding, and we would welcome the counterexample.

The idea is not new. Auer proposed “embedded supervision” — automated supervisory verification drawn directly from distributed-ledger records — in 2019,[28] and legal scholars developed the same instinct as “embedded regulation”. Project Mandala put the research into a working system: compliance checked cryptographically before a transaction executes. The step the literature designed, and that no supervisor has taken, is the one after the transaction — accepting the proof in examination, as evidence, in place of the records it summarizes.

This is not for want of invitation. At the SEC's December 2025 roundtable, Chair Atkins described systems in which “a regulated platform can demonstrate that its users have been screened, without the ability to retain a permanent, person-by-person map of every payment, trade, or donation.” Proof-based approaches have therefore already entered the Commission's policy discussion, but no supervisory framework has yet defined when such proof is sufficient for regulatory reliance.[29]

Commissioner Peirce told the same room that “protecting one's privacy should be the norm, not an indicator of criminal intent.” Commissioner Uyeda asked, “Can tools such as zero-knowledge proofs provide verification tools while enhancing privacy rights?”[30]

The asymmetry is structural: the SEC granted Paxos's settlement system temporary clearing-agency registration in May 2026, demonstrating a regulatory pathway for novel infrastructure. No comparable framework yet defines when privacy-preserving proof can be accepted as sufficient supervisory evidence.[31]

It is a real choice with a running cost. Settlement lag is billed at SOFR plus a spread, and diligence is repeated institution by institution at $50,000 to $200,000 per vendor engagement.[32] Furthermore, this duplication is regressive: over the decade to 2024, the smallest banks devoted 11.0–15.5% of personnel expense to compliance against 5.6–9.6% at the largest — a gap significant at $p<0.01$ in all ten years.

One route is to pool the underlying data, recreating the confidentiality problem above at government scale. ESMA's July 2026 report records national authorities objecting to pooled repositories on cost, latency and cyber risk,[33] and the US banking agencies have moved the other way for their own files, adopting procedures in July 2026 for reviewing highly sensitive examination material on-site rather than transferring it onto agency systems.[34] Both are arriving at the same practice: leave sensitive records where they were made and examine them in place. The other route extends that practice across systems — let an institution establish compliance facts cryptographically, once, for the whole path, with the underlying records reachable on demand.[35]

11.0–15.5%

of personnel expense spent on compliance at the smallest banks, over the decade to 2024

5.6–9.6%

the same figure at the largest banks

A pilot that can fail

Recognition does not require rebuilding regulation around zero-knowledge proofs, but a standard narrow enough to supervise and general enough to reuse.

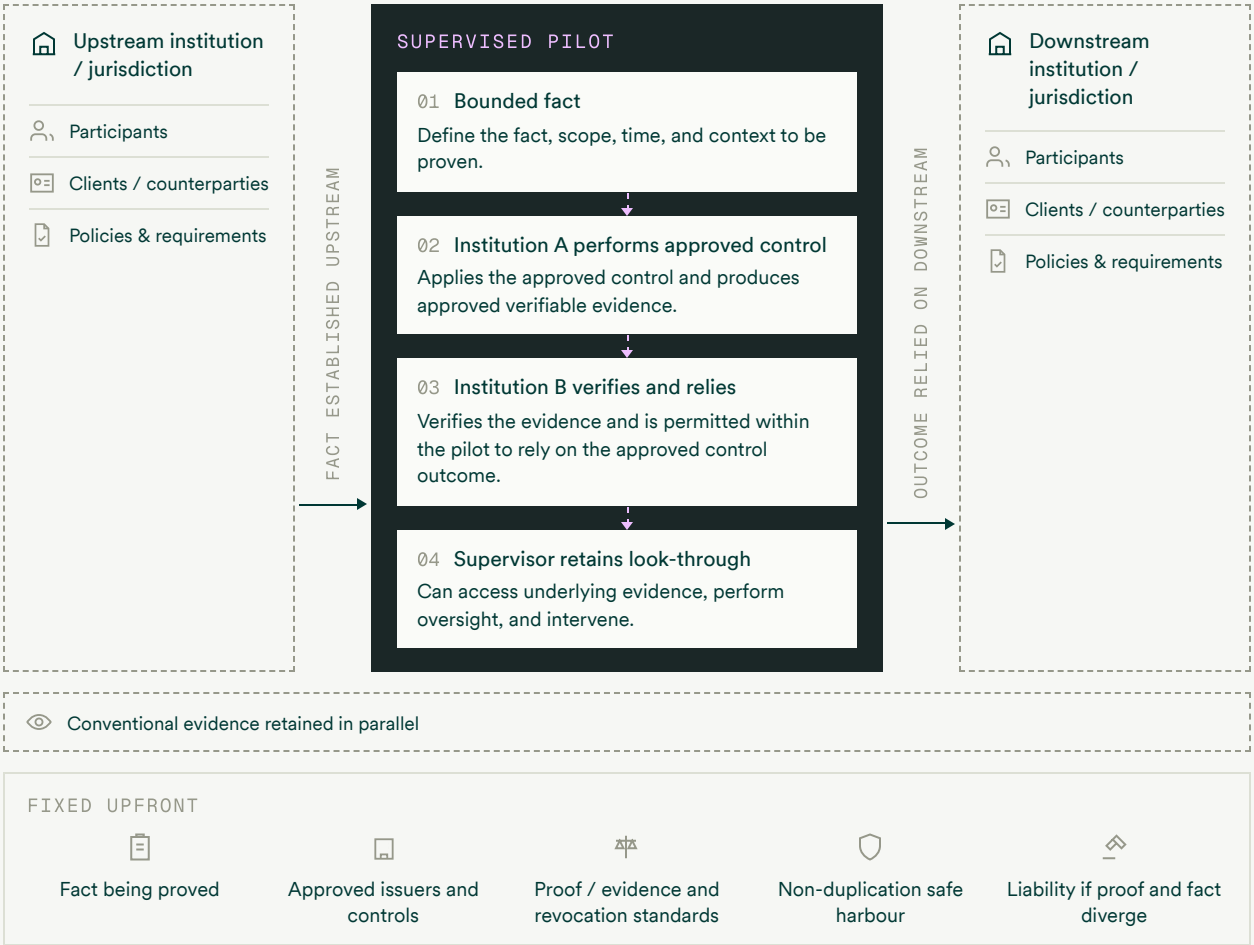
Start with one bounded fact: customer eligibility at a defined point in time. Institution A performs the approved control and generates the proof. Institution B verifies it and, within the pilot, is allowed to rely on that proof rather than repeat the same check. The supervisor retains the underlying evidence and full look-through rights.

The pilot splits cleanly by authority, and each prong has a route that already exists. Investor eligibility on a restricted instrument belongs to the SEC, which holds general exemptive authority under Exchange Act Section 36,[36] has an active crypto task force whose members posed this question in public, and has just shown in the Paxos registration that it will grant time-limited, condition-laden approvals.[37] Sanctions screening belongs to FinCEN, which holds exemptive authority under 31 U.S.C. 5318(a)(7). Reserves belong in the GENIUS Act rulemaking now in progress.[38] Each prong is narrow, and narrow is what moves within a year.

Before the pilot begins, the rules are fixed: what fact is being proved, which issuers and controls qualify, how proofs can be revoked, when duplicate checks can be avoided, and who is liable if the proof and the underlying fact diverge.

FIG. 04 **Supervised pilot**

Test whether one approved control outcome can be relied on downstream without repeating the control.



The main test is simple: Can B rely on A's verified control without repeating the check or increasing supervisory exceptions?

Measure the duplicate-control rate against the conventional arm, then track time to reliance, exception rates, and look-through findings.

The pilot must be able to fail. If reliance rises and examination findings rise with it, or look-through shows proof-to-fact divergence above a pre-set threshold, recognition should not scale. Success means more than verifying a proof: the control must remain auditable, revocation effective, liability allocated and examination credit granted.

Five objections deserve answers before a supervisor commits to any of this.

01 **A proof can attest faithfully to a false input.** In the piloted designs the circuit checks two things: a signature over the inputs from a designated provider — a screening vendor, a credential issuer, a custodian — and that those inputs satisfy the rule, bound to a named list or credential version. The remaining trust therefore shifts to that provider's controls, key governance and the integrity of the input. A proof replaces the transmission and storage of evidence; it does not replace the diligence that produced it, and the pilot is where liability for the gap between proof and fact gets written down.

02 **The proof system may itself fall within model-risk governance purview.** Under SR 11-7 and its OCC equivalent,[39] an institution must validate the circuits, govern the keys, and confirm that the statement being proved matches the obligation the law imposes. This is the strongest objection, and the answer is narrowness: three defined facts require three validated statements, and an examined intermediary could reduce duplicative validation across relying institutions — the economics that already justify service-provider examination under 12 U.S.C. 1867(c).[40] Validation scope should name the failure the market has already seen: a single compromised verifier. It should also favor proof systems that need no per-circuit setup ceremony and stay verifiable for the years an examination file lives.

03 **Examiners must retain access.** Statutory access to books and records (12 U.S.C. 481;[41] 12 U.S.C. 1820[42]) cannot be impaired by architecture, and proof-based evidence does not impair it. Proofs are the routine tier; examiners escalate to the underlying records when a proof raises suspicion. The form of routine evidence changes and statutory reach does not.

04 **The auditor's letter already exists.** Supervisors accept third-party attestations today, and the CFTC's reserve-attestation regime shows the demand.[43] The difference is one of kind: an attestation is periodic, sample-based and rests on trusting the attester, while a proof is per-transaction, machine-verifiable and tied to a named list version at the moment of proving. The two work together, and the reserves case shows how — cryptographic solvency proofs are point-in-time and cannot by themselves establish that the liability list is complete, so the near-term form of recognition may well be attestation frameworks whose underlying evidence is cryptographic.

05 **Enforcement must be able to unpack the record.** A proof that cannot be expanded into admissible facts would weaken a case, and the Commission holds access to all records of registered entities under Exchange Act Section 17(b).[44] The same two-tier answer applies: proofs serve examination, records remain available for enforcement. This is why recognition at the SEC runs through rulemaking or exemptive relief rather than guidance.

What a supervisor gains is a more consistent and machine-verifiable evidentiary view across systems, verified rather than assembled by hand, at a cost that falls as adoption grows. The heaviest relief lands on the smallest institutions, which today carry the duplication least well.

If the pilot succeeds, the policy agenda should shift from demonstrating technical feasibility to institutionalizing reliance: measuring where trust breaks at system boundaries and aligning adjacent identity frameworks before they crystallize into fragmented recognition regimes.

05

Two supervisory changes should accompany it

First, supervisors should examine whether controls survive movement rather than which platform activity sits on by collecting two figures nobody collects today: the share of tokenized volume crossing a trust perimeter, and the duplicate-control rate there. Repo is the precedent: a $700bn blind spot persisted until measured.

And second, the identity frameworks being built in parallel, from EU wallets to vLEI to GENIUS certification, should be treated as one recognition problem before they harden separately; GENIUS section 13 already directs coordination, yet tokenized-deposit clearing still has no assigned regulator. Narrowness also makes the timing realistic: evidence standards move slowly when they move broadly. Electronic records took twenty-five years, while constrained cases moved fast, as when the CFTC went from prohibition to conditional stablecoin-margin relief in under a year.[45]

06

Conclusion

We can move the money, generate the proof, and increasingly verify it elsewhere. What no institution can yet do is rely on it. Until a supervisor says when a proof is enough, every boundary restarts the trust process: duplicate checks, duplicate evidence, and disclosure that re-establishes what was already settled. Without a clear basis for regulatory reliance, institutions rebuild controls at each boundary, and the operational, liquidity and balance-sheet costs of fragmentation persist. A framework for reliance would not eliminate fragmentation, but it would remove one of the structural reasons it holds. The pilot proposed here is cheap and binds no one beyond its scope. The next advance may not be another bridge but a rule that lets the proof count. What remains open is whether the cross-system version of this market gets built inside the regulatory perimeter, or outside it.

1 Broadridge DLR, Jul 2026.

2 Broadridge Financial Solutions, “Broadridge's Distributed Ledger Repo Processes $7.5 Trillion in June,” July 7, 2026; J.P. Morgan, “Latest Milestones at Kinexys by J.P. Morgan,” April 28, 2026; Canton Network, “Canton Unlocks the Wallet Stack for Developers,” June 16, 2026.

3 Canton Network. “Canton Unlocks the Wallet Stack for Developers.” June 16, 2026.

4 Broadridge Financial Solutions. Quarterly volume disclosure, three consecutive quarters at $350–384bn/day.

5 Circle CCTP share of bridged volume, early 2026.

6 National Securities Clearing Corporation. SEC rule filing evidencing $519tn gross netted to $9tn settled.

7 Broadridge Financial Solutions, “SEC Central Clearing Rule Changes”; Zenith Network, “Zenith Advances Roadmap toward Full EVM-Composability on Canton MainNet,” August 6, 2026; SIFMA, Regulated Settlement Network Proof of Concept: Legal Viability Report, December 5, 2024; The Clearing House, “CHIPS Delivers Record Value and Resilience for Participants in 2025,” April 7, 2026.

8 SIFMA, Regulated Settlement Network Proof of Concept: Legal Viability Report, December 5, 2024.

9 Wormhole Foundation, “Securitize Announces Wormhole as Official Interoperability Provider for VanEck's First Tokenized Fund, VBILL,” May 13, 2025.

10 Commodity Futures Trading Commission, Timothy Massad, “Keynote Remarks before the Risk USA Conference,” October 22, 2015 (reporting approximately 75% of swap transactions centrally cleared a little over five years after Dodd-Frank).

11 International Swaps and Derivatives Association and Global Digital Finance. Survey. July 7, 2026.

12 HQLAx. Collateral-mobility business.

13 Wormhole Foundation, “Securitize Announces Wormhole as Official Interoperability Provider for VanEck's First Tokenized Fund, VBILL,” May 13, 2025.

14 Bank for International Settlements, Project Agorá: A Shared Programmable Platform for Wholesale Cross-Border Payments, May 2026; U.S. Securities and Exchange Commission, Paul S. Atkins, “Remarks at the Crypto Task Force Roundtable on Financial Surveillance and Privacy,” December 15, 2025.

15 Loan Syndications and Trading Association. Delayed compensation at daily SOFR plus 11.448bps spread adjustment.

16 Average par settlement ~22 days, early 2025.

17 Secondary loan trading past $1tn trailing-year, early 2026.

18 Figure Certificate Company, Registration Statement on Form S-1/A (describing AML/KYC attributes and failed-transfer handling); Office of Financial Research, “Sizing the U.S. Repo Market,” December 4, 2025.

19 Bank for International Settlements, Project Mandala: Streamlining Cross-Border Transaction Compliance, October 28, 2024; Bank for International Settlements, “Project Tamga,” November 11, 2025.

20 Bank of England. Settlement finality designation, Fnality. December 2024.

21 U.S. Securities and Exchange Commission, Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants, Exchange Act Release No. 34-96034, October 12, 2022.

22 Cryptographic proofs are one promising way to do that while preserving the underlying data.

23 Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, October 2021, esp. Travel Rule table and paras. 159–162; FATF Recommendations, Recommendation 16 and Interpretive Note, revised June 2025.

24 The regulatory review included SEC rules/releases/no-action materials, federal banking guidance, FinCEN BSA/CDD materials, FATF Recommendations, Regulation (EU) 2024/1624 (AMLR), and Regulation (EU) 2023/1114 (MiCA).

25 New York State Department of Financial Services. Approval of shielded withdrawals with viewing-key access. 2020.

26 Financial Action Task Force. Opportunities and Challenges of New Technologies for AML/CFT. July 2021.

27 European Parliament and Council. Regulation (EU) 2024/1624 of 31 May 2024 (Anti-Money Laundering Regulation), arts. 75(4)(e) and 79.

28 Auer, Raphael. "Embedded Supervision: How to Build Regulation into Decentralised Finance." BIS Working Papers No. 811, September 2019.

29 U.S. Securities and Exchange Commission, Paul S. Atkins, "Remarks at the Crypto Task Force Roundtable on Financial Surveillance and Privacy," December 15, 2025.

30 U.S. Securities and Exchange Commission. Hester M. Peirce and Mark T. Uyeda, remarks at the Crypto Task Force Roundtable on Financial Surveillance and Privacy. December 15, 2025.

31 U.S. Securities and Exchange Commission, Paxos Securities Settlement Company, LLC; Order Granting an Application for Temporary Registration as a Clearing Agency, Exchange Act Release No. 34-105562, May 27, 2026.

32 Thomas F. Siems, "Do Banking Regulations Disproportionately Impact Smaller Community Banks?", CSBS Working Paper 25-01, July 2025 (2019 survey-year figures).

33 European Securities and Markets Authority. Final Report on the Call for Evidence on a Comprehensive Approach for the Simplification of Financial Transaction Reporting. July 2, 2026.

34 Board of Governors of the Federal Reserve System, FDIC, and OCC. Joint statement on enhanced procedures for highly sensitive examination information. July 16, 2026.

35 European Securities and Markets Authority, Final Report on the Call for Evidence on a Comprehensive Approach for the Simplification of Financial Transaction Reporting, July 2, 2026; Conference of State Bank Supervisors, Do Banking Regulations Disproportionately Impact Community Banks?, 2026.

36 Securities Exchange Act of 1934 §36, 15 U.S.C. §78mm (general exemptive authority).

37 U.S. Securities and Exchange Commission. Paxos Securities Settlement Company, LLC; Order Granting an Application for Temporary Registration as a Clearing Agency, Exchange Act Release No. 34-105562. May 27, 2026.

38 United States. Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), §13, 12 U.S.C. §5913.

39 Board of Governors of the Federal Reserve System. Supervisory Letter SR 11-7, "Guidance on Model Risk Management." April 4, 2011. The model risk framework formerly under SR 11-7 was superseded in April 2026 by the interagency guidance issued as SR 26-2.

40 Bank Service Company Act, 12 U.S.C. §1867(c).

41 12 U.S.C. §481 (examination of national banks).

42 12 U.S.C. §1820 (FDIC examination authority).

43 Commodity Futures Trading Commission. Staff Letter No. 26-05, Staff No-Action Position Regarding Digital Assets Accepted as Margin Collateral. February 6, 2026.

44 Securities Exchange Act of 1934 §17(b), 15 U.S.C. §78q(b).

45 GENIUS Act §13, 12 U.S.C. §5913(b) (coordination among federal and state payment stablecoin regulators); Commodity Futures Trading Commission, Staff Letter No. 26-05, February 6, 2026 (reissuing conditional no-action relief for specified digital assets accepted as margin collateral).

AFFILIATION NOTE

Twilight is a financial infrastructure company developing privacy-preserving interoperability and settlement infrastructure for institutional digital assets.