Journal of Digital Assets and Monetary Research

Volume 1, Issue 1

Conceptual Article

Date of Submission: 06 May 2026
Date of Acceptance: 27 May 2026
Date of Publication: 29 May 2026

Interoperability-as-Infrastructure: Design-Space Tensions in Cross-Chain Tokenized Credit

Ian Staley*
Independent Researcher, USA
ORCID: 0009-0000-8592-3186

***Corresponding Author:** Ian Staley, Independent Researcher, USA.

Citation: Staley, I. (2026). Interoperability-as-Infrastructure: Design-Space Tensions in Cross-Chain Tokenized Credit. *J Digi Assets Monetary Res*. 1(1), 01-25.

Abstract

Cross-chain tokenization of real-world assets (RWAs) exhibits a class of design problems that differs structurally from both single-chain tokenization and from general-purpose cross-chain interoperability. Existing literature on bridge security treats cross-chain failures primarily as protocol-security problems amenable to cryptographic or auditing remedies, while literature on tokenized real-world assets treats them primarily as legal-authority problems amenable to regulatory or contractual remedies. This paper argues that a third category of problem—infrastructure-layer design-responsibility allocation—cuts across both framings and is inadequately theorized in either. Using the April 2026 KelpDAO bridge exploit as an animating case, the paper develops a three-layer taxonomy of cross-chain tokenization architecture (messaging, settlement, and asset-representation), identifies five design tensions that recur across these layers, presents a reference-architecture comparison of ten leading interoperability solutions evaluated against the design-tensions framework, and extends the analysis to tokenized credit—where the distinction between digital-twin and digital-native tokenization, the compliance architecture demanded by FATF Travel Rule obligations, and the non-transferability of perfected security interests across chains produce a design space that existing interoperability and tokenization literatures address only in parts. The paper's contribution is cartographic: it maps a design space that current vocabulary obscures, and concludes with a research agenda for cross-chain RWA infrastructure and a discussion of how design responsibility should be allocated and disclosed.

Keywords: Cross-Chain Interoperability, Tokenized Credit, Bridge Security, Design Responsibility, Travel Rule

Introduction

On April 18, 2026, an attacker drained approximately $292 million (116,500 rsETH, roughly 18 percent of rsETH's circulating supply) from KelpDAO's cross-chain bridge, exploiting not a flaw in KelpDAO's smart contracts but a weakness in the cross-chain messaging layer those contracts relied upon [1]. The attackers compromised remote

procedure call (RPC) nodes that the messaging layer's verifier used to confirm cross-chain transactions, replacing the node software with malicious variants that reported fraudulent state to the verifier while continuing to report accurate state to every other system querying the same infrastructure [2]. A concurrent distributed denial-of-service attack on unaffected RPC endpoints forced the verifier to fail over to the compromised nodes. A single-verifier configuration transformed a targeted infrastructure compromise into a catastrophic protocol failure. The messaging provider has preliminarily attributed the attack to DPRK-linked Lazarus Group (TraderTraitor subunit), pending formal government attribution [2,3].

The dispute that followed is, for this paper's purposes, more interesting than the forensics. The messaging infrastructure provider's post-mortem attributed the failure to the application developer's configuration choice: the single-verifier setup was explicitly discouraged, with multi-verifier redundancy recommended [3]. The application developer disputed this framing, pointing out that the single-verifier configuration was the default in the messaging provider's own quickstart documentation, was present in the provider's GitHub templates, and—per Dune Analytics's analysis of 2,665 active applications over the 90-day window preceding the exploit—was the configuration used by approximately 47 percent of those applications [4,5]. Independent researchers added a third observation: multi-verifier configurations inherit a different class of correlated-dependency risk, because nominally-independent verifiers typically read chain state from overlapping sets of infrastructure providers [5]. Redundancy at the verifier layer does not automatically produce independence at the infrastructure layer beneath it.

This paper argues that this dispute is not incidental to a security story. It is the security story, and existing interoperability and tokenization literatures lack vocabulary to tell it well. The conventional framing treats interoperability failures as problems of protocol choice—developers should select more secure bridges and configure multi-verifier setups [6,7]. Each prescription is correct as far as it goes, but each treats the design-responsibility allocation as if it were obvious: as if developers know which choices are consequential, as if infrastructure defaults are neutral starting points rather than prescriptive commitments, and as if security properties of a cross-chain system can be evaluated layer by layer without attending to how the layers interact. The KelpDAO case suggests none of these assumptions hold.

The Digital-Twin vs Digital-Native Distinction

The problem sharpens when the assets crossing chains are representations of real-world credit—tokenized receivables, tokenized asset-backed loans, tokenized fractional interests in secured commercial instruments. Tokenization of real-world assets admits two fundamentally different architectures. Digital-twin tokenization treats the on-chain token as a representation of an off-chain asset whose legal authority remains grounded in off-chain legal frameworks; the token is a claim against an off-chain legal vehicle (SPV, fund, custodian) that holds the underlying asset [8]. Digital-native tokenization treats the on-chain token as the asset itself, with legal frameworks constructed to recognize the token as the authoritative record of ownership rather than as a representation of off-chain ownership. The Swiss DLT Act (adopted 2020, in force 2021) provides the most developed legal framework for digital-native tokenization, with Wyoming's Digital Asset

Act, Liechtenstein's TVTG, and Singapore's Payment Services Act providing parallel approaches in other jurisdictions [9].

The distinction matters for cross-chain design because the two architectures have different relationships to the chains they live on. A digital-twin token can be represented on any chain that supports the appropriate smart-contract patterns, because the chain does not carry the token's legal authority—the chain is a ledger, and the legal authority sits in the off-chain vehicle. A digital-native token's legal authority is bound to a specific chain whose register has statutory recognition; moving such a token to another chain requires either accepting that the wrapped representation loses its digital-native status or extending the jurisdictional framework to recognize the wrapped representation.

Contributions

This paper makes four contributions. First, a three-layer taxonomy of cross-chain tokenization architecture separating messaging, settlement, and asset-representation concerns, arguing that existing work conflates these layers in ways that obscure consequential distinctions. Second, five design tensions that recur across these layers and admit no clean resolution, providing an analytical framework that goes beyond the security-vs-decentralization framing dominant in existing literature. Third, a reference-architecture comparison of ten leading interoperability protocols across four architectural categories.

Fourth, extension of the analysis to tokenized credit, arguing that the interaction of cross-chain architectural commitments with the digital-twin / digital-native distinction, FATF Travel Rule obligations, and UCC Article 9 perfected-security-interest frameworks produces a design space that neither literature adequately addresses.

The paper's contribution is cartographic rather than prescriptive. It does not propose a new protocol or offer a solution to the legal-authority problem in tokenized credit. It maps the design space, identifies tensions that any serious design effort must navigate, and frames a research agenda.

Methodology

This paper follows the tradition of conceptual design-space analysis in information systems and infrastructure research [10-12]. Design-space analysis aims to make explicit the consequential decisions embedded in existing artifacts and the tradeoffs that constrain future designs, rather than to evaluate specific designs empirically or derive formal properties from models. The paper draws on published post-mortems of cross-chain exploits (with particular attention to KelpDAO), protocol documentation and audits from the ten interoperability solutions analyzed in Section 5, regulatory and standards-body documentation, and academic literature on bridge security, tokenization, and interoperability. The paper's analytical moves are interpretive rather than deductive, and its claims should be evaluated on the coherence of the framework it proposes rather than on empirical grounds it does not claim.

Structure

Section 2 positions the paper relative to bridge security, interoperability, tokenization, and compliance literatures. Section 3 develops the three-layer taxonomy. Section 4

identifies five design tensions. Section 5 compares ten interoperability protocols against the framework. Section 6 extends the analysis to tokenized credit. Sections 7 and 8 frame a research agenda and discuss design-responsibility implications. Sections 9 and 10 address limitations and conclude.

Related Work

The paper draws on and synthesizes four literatures.

Bridge security and cross-chain protocol analysis has developed rapidly since 2021 in response to high-profile exploits. Zhang et al. provide a systematic survey of cross-chain bridge attacks, categorizing failure modes across cryptographic, economic, and operational dimensions [6]. Lee et al. analyze the Ronin and Wormhole exploits with attention to verifier-set compromise, while Belchior et al. survey the broader interoperability landscape [13,7]. This literature addresses protocol-level security properties but treats interoperability as a technical problem in isolation from the asset-type characteristics (particularly legal authority) that RWA tokenization introduces.

The interoperability literature addresses cross-chain systems at higher abstraction, focusing on protocol-level mechanisms for communication and value transfer [7,14-16]. This literature classifies interoperability approaches into hash-lock mechanisms, relay-based protocols, notary schemes, sidechains, and zero-knowledge proof systems. Its strength is systematic treatment of mechanism space; its limitation is focus on cryptocurrency-native assets and general-purpose message passing, without engaging substantively with constraints imposed by tokenized real-world assets or how legal-authority requirements interact with cross-chain architectural choices.

Real-world asset tokenization literature has grown alongside institutional adoption [17-19]. Allen etal. survey legal and regulatory considerations for digital assets [8]. A specialized legal literature addresses interaction of tokenization with existing collateral and securities frameworks: work on UCC Article 9 and Article 12 analyzes challenges of perfecting security interests in on-chain collateral; Fox and Green examine property-law treatment of cryptoassets; the UNIDROIT Principles on Digital Assets and Private Law attempt cross-jurisdictional harmonization [17,20-22]. This literature engages seriously with legal-authority questions but generally treats them in jurisdiction-specific or single-chain terms.

A recent literature addresses technical implementation of FATF Recommendation 16 (the "Travel Rule") for virtual asset transfers [23-25]. The IVMS 101 data standard provides a common format for originator and beneficiary information, and protocols including TRP, TRISA, and Sygna Bridge implement alternative transport layers [26,27]. This literature addresses Travel Rule compliance primarily in centralized VASP contexts and has only begun to address cross-chain compliance challenges.

The present paper's contribution is to bring these literatures into sustained contact. Design-responsibility allocation in cross-chain infrastructure is an infrastructure-security question the bridge-security literature does not frame as such. The extension of legal-authority frameworks and Travel Rule obligations across chains is a legal-technical composition question neither tokenization nor interoperability literature addresses

directly. The reference-architecture comparison (Section 5) evaluates solutions against the specific constraints of tokenized RWA credit infrastructure. The three-layer taxonomy (Section 3) offers vocabulary for problems existing literatures describe only in parts.

A Three-Layer Taxonomy of Cross-Chain Tokenization Architecture

Cross-chain tokenization architectures make consequential design commitments at three distinct layers, each operating under different trust assumptions and failure modes. These layers are often conflated in industry discourse, with "cross-chain security" or "bridge security" deployed as if they named a single property rather than a composition of properties that interact in non-obvious ways. This section develops a taxonomy that separates the layers for analytical purposes, as a precondition for Section 4's analysis of tensions that arise when the layers interact. Figure 1 provides an overview.

FIGURE I Three-Layer Taxonomy of Cross-Chain Tokenization Architecture

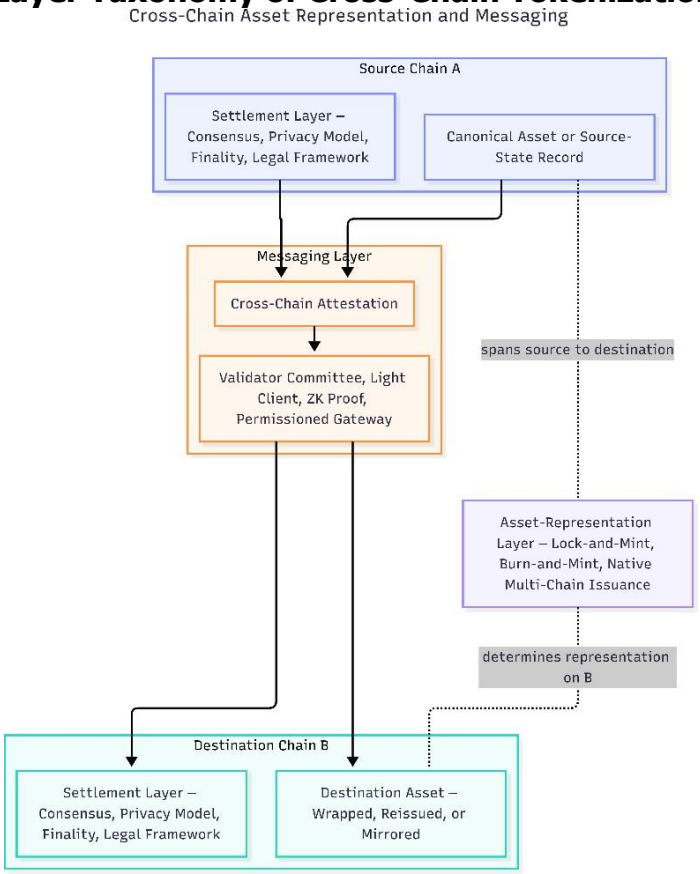

Figure I. Three-layer taxonomy of cross-chain tokenization architecture, separating messaging, settlement, and asset-representation concerns across source and destination chains.

The Messaging Layer

The messaging layer carries attestations that events on one chain have occurred and that corresponding actions on another chain are authorized. Messaging protocols differ primarily in their trust model for verifying cross-chain messages: external validator committees (LayerZero, Wormhole, Axelar), light-client verification (Cosmos IBC), zero-knowledge proofs (Succinct, Polyhedra), or permissioned consortium verification (enterprise DLT API gateways like Overledger). The layer's security property is

authenticity: can the destination chain verify that the message originated from a legitimate state transition on the source chain. The layer's failure modes are signature forgery, verifier compromise (as in KelpDAO), message replay, and liveness loss.

The Settlement Layer

The settlement layer is the specific chain on which the tokenized asset is held, transferred, and enforced. Each chain embeds its own privacy, finality, expressiveness, and legal-framework commitments. Canton Network's Daml-based need-to-know privacy model supports institutional confidentiality requirements but precludes general-purpose DeFi composability. Ethereum and EVM-compatible chains offer transparent state and broad composability at the cost of native privacy. Solana optimizes for throughput. XRPL and Stellar are payment-optimized with constrained smart-contract expressiveness. Move-based chains (Sui, Aptos) enforce ownership semantics at the language level. These are not just technical differences; they are different implicit theories of what a tokenized asset is, and the theories do not compose cleanly across chains.

The Asset-Representation Layer

The asset-representation layer spans the source-destination traversal and determines how an asset exists across chains. Lock-and-mint architectures keep the canonical asset on the source chain with wrapped representations on destination chains, introducing vault-wrapper distinctions that complicate perfected security interests. Burn-and-mint architectures destroy the asset on the source chain and mint it on the destination chain, preserving single-point control cleanly but requiring coordinated state transitions.

Natively multi-chain issuance has the issuer mint in parallel on each chain, preserving jurisdictional clarity per chain but fragmenting canonical supply. Each representation choice has distinct failure modes and legal-authority implications, developed in Section 4.3.

Summary of the Three-Layer Taxonomy

Table I summarizes the three layers, their functions, trust models, and characteristic failure modes.

TABLE I Three-Layer Taxonomy of Cross-Chain Tokenization Architecture

Layer	Function	Trust Model	Failure Modes
Messaging	Cross-chain attestation of state transitions	External committee, light-client, ZK, or permissioned	Signature forgery, verifier compromise, replay, liveness loss
Settlement (each chain)	Asset custody, transfer, enforcement	Chain-specific consensus and legal framework	State-visibility mismatches, finality differences, expressiveness gaps
Asset Representation (cross-cutting)	How asset exists across source-destination	Depends on lock/burn/mint-in-parallel choice	Canonical-supply fragmentation, control-attachment ambiguity

The layers are not independent. Security, privacy, and legal-authority properties of the overall system emerge from the interaction of choices at each layer, in ways not reducible to layer-level analysis. Section 4 analyzes the five design tensions that arise at these interactions.

Five Design Tensions

This section identifies five tensions that recur across the three layers of cross-chain tokenization architecture and that admit no clean resolution. Each tension is a recurring pattern in which two architecturally desirable properties constrain each other, such that improvement in one comes at the cost of the other. The tensions organize the design space the paper maps; they are not ranked and are not exhaustive.

FIGURE II Five Design Tensions in Cross-Chain Tokenization Infrastructure

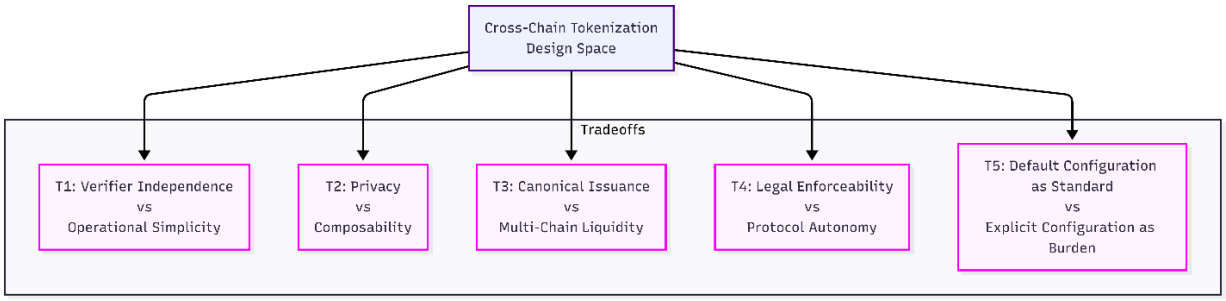

Figure II. Five recurring design tensions in cross-chain tokenization infrastructure identified in the paper's framework.

Tension 1: Verifier Independence vs Operational Simplicity

The KelpDAO exploit crystallized the operational form this tension takes in practice [2-5]. The vulnerable configuration was a single-verifier setup, in which one attestor's sign-off sufficed to release funds across chains. Multi-verifier configurations with independent attestors appear to resolve the tension: if no single verifier can authorize a release alone, no single compromise produces catastrophic failure. But the independence of "independent" verifiers is itself a technical claim that deserves scrutiny. Nominally-distinct verifiers typically consume chain state from overlapping RPC providers, share monitoring infrastructure, and run on overlapping cloud-service backbones. Correlated-dependency risk at the infrastructure layer beneath the verifier layer is not automatically reduced by redundancy at the verifier layer [5]. The tension is operational rather than cryptographic: achieving genuine verifier independence requires operational work (diversifying infrastructure, coordinating incident response across unrelated operators, auditing for shared upstream dependencies) that application developers are poorly positioned to undertake and that infrastructure providers have weak incentives to require.

Tension 2: Privacy vs Composability

Cross-chain tokenization of regulated financial instruments requires both privacy (counterparty-specific obligations are confidential; identity information is transmitted under legal compulsion) and composability (the asset must be useable as collateral, in multi-chain portfolios, and for automated settlement). These objectives pull in opposing

architectural directions. Canton Network's need-to-know data distribution makes Canton suitable for institutional confidentiality but precludes cross-chain composability in the general-purpose DeFi sense—a protocol on another chain cannot programmatically consume Canton's private state [28]. Transparent-state chains (Ethereum, Solana) enable composability but expose transaction graphs and address-to-entity mapping to on-chain analysis, which for regulated counterparties is a compliance risk that native-privacy chains do not face. Hybrid approaches—zero-knowledge attestations, selective-disclosure credentials, confidential transactions overlays—mitigate the tension but introduce their own costs (proof-generation overhead, reduced composability with protocols that don't speak the disclosure format, legal uncertainty about the enforceability of ZK-attested claims).

Tension 3: Canonical Issuance vs Multi-Chain Liquidity

Tokenized assets on multiple chains face a fundamental choice about where the canonical version of the asset lives. Lock-and-mint architectures (the asset is locked on Chain A, wrapped representations are minted on Chain B) preserve canonical issuance on a single chain at the cost of vault security and wrapper-versus-original legal ambiguity. Burn-and-mint architectures (the asset is burned on A and newly issued on B) preserve single-point control cleanly—canonical supply exists on exactly one chain at any instant—but require coordinated state transitions that are difficult across heterogeneous consensus mechanisms. Natively multi-chain issuance (the issuer mints separately on each chain) offers the cleanest per-chain legal treatment but fragments liquidity and creates cross-chain reconciliation obligations. For tokenized credit, the legal implications are consequential: a tokenized receivable whose canonical form lives on Chain A under a specific legal framework faces different questions about what the wrapped representation on Chain B legally is depending on the architectural choice. The extension of legal authority across chains (Section 6) interacts with this choice in ways neither the interoperability nor tokenization literature has adequately mapped.

Tension 4: Legal Enforceability vs Protocol Autonomy

Permissionless cross-chain protocols optimize for protocol autonomy: no external party can prevent a valid cross-chain transfer from executing. Legal enforceability, by contrast, requires identifiable parties, jurisdictional clarity, and mechanisms by which legal remedies (seizure, injunction, reversal) can apply to on-chain assets. Traditional legal frameworks for secured transactions presume courts can order transfer reversal, asset seizure, and counterparty identification. Permissionless cross-chain protocols resist these orders by design: transfers are atomically final, assets cannot be seized without chain-level authority, and counterparties are identified only by addresses. This is not an implementation flaw; it is the property distinguishing permissionless protocols from traditional infrastructure. The tension is most acute for tokenized credit, where the economic function depends on legal enforceability and where the default architectural commitments of general-purpose cross-chain interoperability optimize for the opposite property.

Tension 5: Default Configuration as De Facto Standard vs Explicit Configuration as Burden

The fifth tension is the one the KelpDAO dispute crystallized. Infrastructure providers offer configurable security parameters; application developers must choose configurations. The tension is that providers cannot enforce secure configurations without eliminating the flexibility that makes the infrastructure broadly usable, while developers—especially those without security expertise—default to whatever the provider's quickstart documentation and templates show. Per Dune Analytics, 47 percent of 2,665 active LayerZero applications used the 1-of-1 DVN default configuration pre-KelpDAO [5]. When defaults are adopted at rates that high, defaults function as prescriptive commitments: the provider is effectively specifying a deployed security posture for most applications, even if the provider's formal position is that applications choose their own. The allocation of design responsibility between provider and developer—who is responsible when a default configuration produces catastrophic failure across many deployments—is the analytical locus of this tension, and of the KelpDAO dispute that animates the paper.

Summary of the Design Tensions

Table II summarizes the five tensions, their competing properties, and the locus at which each is most decisive.

TABLE II Five Design Tensions in Cross-Chain Tokenization Infrastructure

Tension	Competing Properties	Key Locus
T1: Verifier Independence	Genuine verifier independence vs operational simplicity	Messaging layer; correlated infrastructure dependencies
T2: Privacy vs Composability	Institutional confidentiality vs cross-chain programmability	Settlement layer; privacy-model mismatches
T3: Canonical Issuance	Single-point control vs multi-chain liquidity	Asset-representation layer; lock-mint vs burn-mint vs native
T4: Legal Enforceability	Jurisdictional remedies vs protocol autonomy	Cross-layer; permissionless-by-design vs legal-framework-compatible
T5: Default Configuration	Infrastructure flexibility vs adoption-at-default security	Design-responsibility allocation between provider and developer

Reference Architecture Comparison

This section presents a systematic comparison of ten cross-chain interoperability solutions against five dimensions derived from the design-tensions framework and the specific requirements of tokenized RWA credit infrastructure. The comparison is organized into four architectural categories corresponding to fundamentally different approaches to the interoperability problem.

FIGURE III Interoperability Solutions Categories

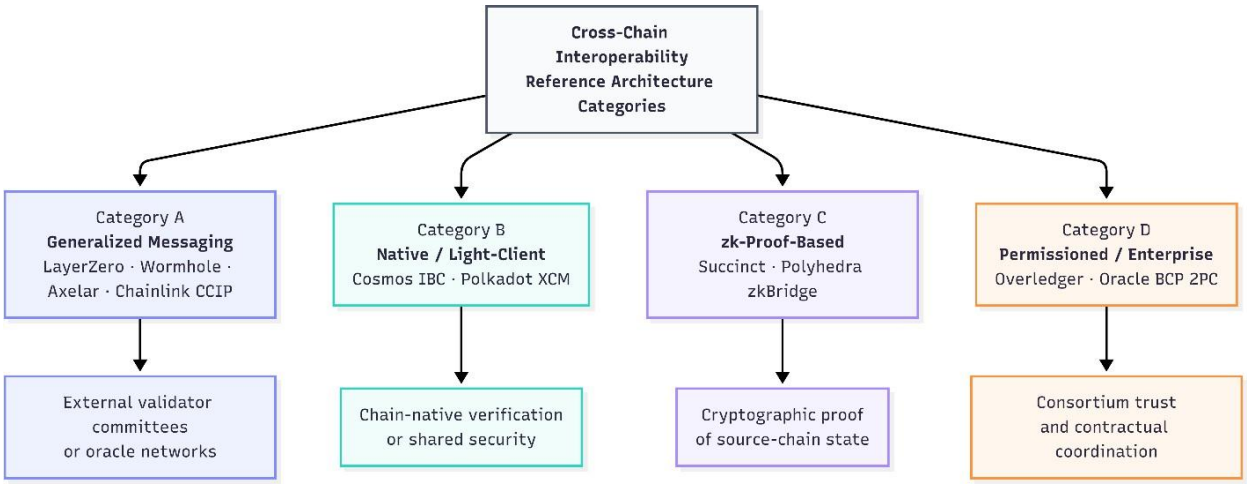

Figure III. Four architectural categories of cross-chain interoperability solutions evaluated in the paper.

Methodology and Comparison Dimensions

Each solution is evaluated along five dimensions identified in Sections 3 and 4 as most differentiating for tokenized cross-chain credit: D1 Trust model (verifier structure, economic security); D4 Privacy model (transparent vs selective-disclosure-capable vs private); D8 Legal-authority compatibility (fit with tokenized-RWA legal frameworks including Swiss DLT Act, eWpG, UCC Article 12); D9 Travel Rule compliance architecture (IVMS 101 support, VASP attribution, identity binding); and D10 Governance and default configuration (decentralization, configurability burden, default security posture).

Supplementary dimensions (finality/latency, chain coverage, composability, asset-representation flexibility, operational track record) are discussed in the per-protocol paragraphs.

Architectural Categories

The ten solutions cluster into four categories: Category A (Generalized Messaging Protocols) — LayerZero, Wormhole, Axelar, Chainlink CCIP — use external validator networks or oracle committees to verify cross-chain messages. Category B (Native / Light-Client-Based Interoperability) — Cosmos IBC, Polkadot XCM — embed verification at the chain level via light-client proofs or shared-security validator sets. Category C (zk-Proof-Based Interoperability) — Succinct, Polyhedra zkBridge — use zero-knowledge proofs to verify cross-chain state transitions cryptographically. Category D (Permissioned / Enterprise Interoperability) — Overledger (Quant) integrated with Oracle Blockchain Platform 2PC — provides DLT API gateway and atomic cross-chain orchestration for consortium deployments. Table III summarizes.

TABLE III Four Architectural Categories of Cross-Chain Interoperability

Category	Examples	Verification Approach	Trust Basis
A. Generalized Messaging	LayerZero, Wormhole, Axelar, CCIP	External validator committee or oracle network	Permissioned committee or PoS validator set
B. Native / Light-Client	Cosmos IBC, Polkadot XCM	Chain-native light-client verification or pooled-security validators	Counterparty chain's consensus; no external verifier
C. zk-Proof-Based	Succinct (SP1), Polyhedra (zkBridge)	Cryptographic proof of source-chain state	Proof-system soundness
D. Permissioned / Enterprise	Overledger + Oracle BCP 2PC	DLT API gateway + atomic transaction coordinator	Consortium membership; contractual trust

Category A — Generalized Messaging Protocols

LayerZero V2 commits to application-owned security: OApps configure a per-pathway Security Stack of Decentralized Verifier Networks (DVNs) and Executors. Trust is polymorphic—1-of-1 DVN reduces to single-entity trust, while multi-DVN stacks approximate defense-in-depth. Privacy is transparent; no native IVMS 101 support. Legal fit is favorable for OFT burn-and-mint (UCC Art. 12 "control" is clean) but ambiguous for OFT Adapter lock-and-mint. The KelpDAO episode exposed D10: 47 percent of 2,665 active OApps ran 1-of-1 DVN pre-exploit [5]. Post-incident, LayerZero announced it will no longer sign for 1-of-1 configurations; migration is ongoing. Best fit: cross-chain stablecoin distribution and native omnichain credit tokens under a single registrar.

Wormhole uses a 19-Guardian PoA committee with 13-of-19 VAA threshold [29]. Native Token Transfers (NTT) support both burn-and-mint and hub-and-spoke locking. The 2022 Solana-bridge signature-verification exploit (~$325M, ETH replaced by Jump Crypto; ~$140M recovered via 2023 counter-exploit) remains the anchor D7 event. No native Travel Rule; VAAs carry no IVMS 101 schema or VASP attribution. Static committee default is uniform but equivalent to a prescriptive commitment.

Best fit: tokenized-fund share-class distribution across EVM, Solana, Sui, Aptos where broad non-EVM coverage matters more than slashable economic security.

Axelar operates a permissionless PoS Layer 1 (~75 validators, Cosmos SDK) with quadratic (√stake) voting for cross-chain validation since the 2022 "Maeve" upgrade [30]. Interchain Token Service (ITS) extends canonical issuance to EVM plus Sui, Stellar, XRPL via ITS Hub. Trust is slashable PoS—a qualitative step beyond Wormhole's PoA. Privacy transparent; Travel Rule non-native. GMP primitives can carry attestation payloads, relevant when a DLT-Act register operator transmits ledger-based-security state transitions. Best fit: multi-chain RWA issuance reaching heterogeneous VMs where a slashable validator set is preferred.

Chainlink CCIP uses defense-in-depth through N-version programming: a Decentralized Oracle Network (DON) plus an independent Risk Management Network (RMN, formerly ARM) running a Rust-language reimplementation [31]. Cross-Chain Token (CCT) standard, mainnet January 2025, provides self-serve burn-and-mint or lock-and-mint issuance. Privacy uniquely rich among Category A via Blockchain Privacy Manager and CCIP Private Transactions. D8 strongest in category: SWIFT pilot, ANZ Bank, HKMA e-HKD+, MAS Project Guardian, DTCC Smart NAV [32] (distinct from R3 Corda's Project Ion). D9 is the clearest native-capable architecture among public-chain messaging protocols via the Automated Compliance Engine (ACE) and Digital Transfer Agent standard, though IVMS 101 schema is not on-chain. Default posture is conservative—RMN and DON both active, not reducible by applications. Best fit: institutional interbank settlement, tokenized MMF distribution, regulated stablecoin corridors.

Category B — Native / Light-Client-Based Interoperability

Cosmos IBC provides trust-minimized, consensus-agnostic light-client verification (ICS-002) [33]. IBC v2 "Eureka" (March 2025) extends to Ethereum via Succinct SP1 zkVM, with Solana on the roadmap. Trust reduces to participating chains' security—the cryptographically purest Category B model. Privacy transparent; Travel Rule absent natively. D8 strong architecturally: channel/port semantics allow authoritative-register projection without relinquishing canonical issuance, aligned with Swiss DLT Act single-ledger exclusivity (Art. 973d para. 1 CO) and eWpG register-centric models. D10 unusually favorable—no "dangerous default" analog to 1-of-1 DVN because security is not application-configurable. Best fit: sovereign-chain RWA where issuers control both endpoints (Noble USDC, MANTRA Chain); Eureka opens cryptographically rigorous Ethereum ↔ Cosmos pathways for tokenized treasuries.

Polkadot XCM is a message format defining an XCVM instruction set; transport is HRMP (current production, full XCMP still under development), secured by Relay Chain paravalidators [34]. Parachains inherit pooled security with no independent finality. XCM v5 origin and MultiLocation semantics provide clean authority-delegation well-suited to representing issuer-controlled RWAs across parachains. Privacy transparent (DID-adjacent parachains like KILT offer off-platform primitives). Travel Rule absent natively. HRMP channels are opt-in with DOT deposits and "deny all by default" configuration guidance. Ecosystem anchors: Centrifuge, Polkadot Capital Group (2025). Best fit: parachain-native structured credit; limited for cross-ecosystem institutional credit.

Category C — zk-Proof-Based Interoperability

Succinct provides the SP1 RISC-V zkVM (now SP1 Hypercube) and the Succinct Prover Network (mainnet August 2025) [35]. SP1 Hypercube proves 99.7 percent of Ethereum L1 blocks in under twelve seconds on sixteen GPUs, achieving real-time parity with Ethereum slot times. ~$4B TVL secured across Polygon, Celestia, Avail, Optimism, Taiko, Lido, and IBC Eureka's Ethereum endpoint. Succinct is infrastructure for other bridges rather than a branded bridge. Trust reduces to proof-system soundness plus on-chain SNARK wrapper verification key. SP1 core has no trusted setup; Groth16 wrapper does. Travel Rule not applicable at this layer. Best fit: cryptographic rather than committee-based verification substrate for credit infrastructure (tokenized-fund NAV attestation, ZK-authenticated Cosmos ↔ Ethereum bridges, privacy-preserving compliance proofs).

Polyhedra zkBridge uses bespoke GKR/sumcheck proof systems (Virgo, deVirgo, Orion, Pianist, Expander) purpose-built for data-parallel BLS-signature verification [36]. deVirgo proves Ethereum full-PoS consensus (~32,000 BLS signatures) in ~8–10 seconds with ~220K gas on-chain. Productionized as LayerZero V2 DVN on 30+ L1/L2 networks; lifetime >21M cross-chain txs, >40M proofs. Trust is cryptographic under honest-prover soundness assumption; liveness depends on single-operator Polyhedra DVN unless composed. Integrations: Ondo USDY (multi-DVN model), BitGo WBTC, Google Cloud Proof Cloud, EigenLayer. Best fit: tokenized-treasury and stablecoin corridors using multi-verifier Security Stacks; poor fit for single-DVN deployments.

Category D — Permissioned / Enterprise Interoperability

Overledger (Quant) + Oracle Blockchain Platform 2PC. Category D is presented as a single complementary architecture following the February 2025 Oracle-Quant partnership, under which Overledger was certified on Oracle Blockchain Platform (OBP) Digital Assets Edition [37,38]. Per Quant's taxonomy aligned with the WEF three-way classification (API gateway / notary-relayer / HTLC), Overledger is a DLT API gateway and does not perform cross-chain state verification; atomic workflows depend on OBP's atomicTransactions REST API implementing XA-standard 2PC across OBP channels, extending atomicity to EVM via last-resource-commit (USPTO patent 12,373,424). OBP is maintained through release 25.4.1 (December 2025). Trust is permissioned membership with PKI identity. Privacy strongest in the set: Fabric channels provide native confidentiality. Legal fit strongest: OBP can serve as BaFin-registrable eWpG register, satisfies Swiss DLT Act integrity requirements, and burn-and-mint plus 2PC-LRC pattern preserves control cleanly under UCC Art. 12 §12-105. Travel Rule not native to either component but architecturally closest to "native-compatible" via closed-membership VASP vetting.

Active deployments: UK Regulated Liability Network tokenised sterling deposits (September 2025: Barclays, HSBC, Lloyds, NatWest, Nationwide, Santander UK); Bank of England–BIS Project Rosalind (June 2023) [39,40]. Best fit: interbank tokenized-deposit settlement, wholesale CBDC corridors, regulated syndicated-credit workflows.

Cross-Cutting Analysis

The ten protocols cluster sharply along the three-layer taxonomy. Category A protocols converge on transparent-default privacy and permissioned or configurable verifier sets; only CCIP's N-version RMN architecture and ACE/Privacy Manager product surface move the protocol appreciably along D4, D8, D9—which is why CCIP dominates the institutional pilot record. Category B offers the cleanest D1 profiles and D10 postures (no dangerous defaults, because security is not application-configurable) but is weakest on D9. Category C is not comparable on D8 or D9 at the same layer—these are verification substrates contributing to tokenized credit when composed into Category A or B stacks. Category D dominates D4 and D8 by construction at the cost of open-ecosystem composability and public-chain reach.

The default-configuration problem (T5) manifests differently across categories. Category A faces it most acutely: LayerZero's 47 / 45 / 5 distribution across 1-of-1, 2-of-2, 3-of-3+

configurations shows a configurable architecture with a permissive quickstart resolves empirically toward the weakest safe choice. CCIP's choice to make RMN non-reducible by applications is a prescriptive default in the strong sense—it removes the degree of freedom that produced the KelpDAO pattern. Category B sidesteps the problem: IBC security is not a parameter; XCM HRMP channels are explicitly opt-in with "deny all by default" guidance. Category C shifts the default question to trusted-setup composition and prover-operator singularity (zkBridge's default deployment as single-entity DVN recreates Category A's problem at Polyhedra's layer). Category D externalizes defaults to consortium agreements.

On legal-authority and Travel Rule, no protocol meets institutional requirements fully "out of the box." CCIP is the only public-chain protocol with a native compliance architecture (ACE, DTA standard, Privacy Manager, external identity registry integration via vLEI/ERC-3643), and even CCIP does not embed IVMS 101 as an on-chain schema. Other Category A, B, and C protocols are D9-silent—Travel Rule compliance is handled as an off-chain overlay through Notabene, 21 Analytics, Sumsub, or VerifyVASP at each VASP endpoint. The canonical institutional pattern is two-rail: a settlement rail on the interoperability protocol and a compliance-messaging rail through correspondent-banking infrastructure (ISO 20022, SWIFT gpi) or dedicated Travel Rule gateways. Category D makes two-rail architecturally explicit. On D8, burn-and-mint canonical issuance (CCIP CCT, LayerZero OFT, Wormhole NTT burn-mode, Axelar ITS, OBP with 2PC-LRC) aligns cleanly with UCC Article 12 §12-105 "control" semantics, while lock-and-mint variants reintroduce vault-wrapper ambiguity. Swiss DLT Act single-ledger exclusivity and eWpG single-authoritative-register model remain regulatory gaps for cross-chain representations as of April 2026—neither FINMA nor BaFin has published cross-chain guidance—which makes the most defensible architectural pattern authoritative-register-plus-projection (an eWpG- or DLT-Act-registered ledger on one chain, with IBC light-client projections or CCT/ITS burn-and-mint representations on destination chains).

The design-tensions framework refracts into a clear ranking for tokenized credit. T1 (verifier independence) is most decisive across Category A—the KelpDAO episode, Wormhole's 2022 exploit, and CCIP's RMN architecture are expressions of the same question. T2 (privacy-composability) is most decisive for Category D and CCIP's institutional positioning. T3 (canonical issuance) systematically favors burn-and-mint. T4 (legal enforceability) is where categories cluster most sharply: Category D at the legal-enforceability pole by construction, Category B neutral, Category A ranging from CCIP (strong institutional fit) to LayerZero and Wormhole (weak absent issuer-side overlay). T5 (default configurations) is where LayerZero stands alone as illustrative case. The joint implication: no single protocol is categorically sufficient. The infrastructurally coherent pattern is an authoritative register in a cross-chain-tolerant asset-law jurisdiction (UCC Article 12, or—with caveats—Swiss DLT Act), issued as canonical burn-and-mint, projected via a defense-in-depth verifier stack (CCIP RMN+DON, IBC light clients with SP1 verification, or multi-DVN LayerZero), with Travel Rule compliance on a parallel off-chain rail bound to on-chain transactions by cryptographic reference.

Summary Comparison Table

TABLE IV Ten Protocols Evaluated Across Five Differentiating Dimensions for Tokenized Credit

Protocol	D1 Trust	D4 Privacy	D8 Legal fit	D9 Travel Rule	D10 Default posture
LayerZero V2	App-config DVN X-of-Y-of-N; polymorphic	Transparent	OFT burn-mint clean for UCC Art. 12; adapter ambiguous	No native; external overlay	1-of-1 default; 47% of OApps pre-KelpDAO
Wormhole	19 Guardians PoA; 13-of-19 threshold	Transparent	NTT burn-mint clean; locked mode weaker	No native; no VASP attribution	Static committee; Governor rate-limit
Axelar	~75-validator PoS; quadratic voting	Transparent	ITS supports canonical issuance; favorable	No native; application-layer overlay	Uniform; Amplifier governance
Chainlink CCIP	DON + independent RMN (N-version)	Selective-disclosure capable (Privacy Mgr, CCIP PT)	Strongest public-chain fit (ACE, DTA)	Native-capable via ACE + external identity	RMN+DON both active; not reducible
Cosmos IBC	Light-client (ICS-002); no external verifier	Transparent	Strong; single-register doctrine alignment	No native; application overlay	Permissionless relayers; no dangerous default
Polkadot XCM	Relay chain paravalidators ; pooled NPoS	Transparent (parachain-specific DID optional)	XCM v5 origin semantics clean	No native; no originator/beneficiar y fields	HRMP opt-in with DOT deposits; deny-all default
Succinct (SP1)	Proof soundness + SNARK wrapper key	App-determined; private inputs supported	Indirect; favorable substrate	N/A at this layer	No trusted setup (STARK core); Groth16 wrapper
Polyhedra zkBridge	ZK soundness; single-op DVN unless composed	App-level ZK attestations possible	Indirect; cryptographic substrate	No native	Partially transparent; single-DVN liveness risk
Overledge	Permissioned	Enterprise	Strong for	Two-rail (settlement	Contractual;

r (Quant)	API gateway; PKI/OAuth	confidentiality	eWpG/Swiss DLT Act registers	+ off-chain IVMS)	consortium governance
Oracle BCP (2PC)	Permissioned Fabric + XA 2PC; LRC to EVM	Channel-native confidentiality	Strongest UCC Art. 12 single-component fit	Off-chain overlay architecture	SOC/ISO/FedRAMP inherited; serializable isolation

Audit coverage is discussed in Sections 5.3–5.6 (auditors named per protocol: Trail of Bits, Zellic, OpenZeppelin, OtterSec, Informal Systems, Quarkslab, SRLabs, NCC Group, Ackee Blockchain, Veridise, Cantina, KALOS, Nethermind Security, Atredis Partners). A supplementary table with quantitative performance benchmarks (latency, throughput, gas, proof-generation times) is deferred to v1.1.

Extension to Tokenized Credit

Section 5's comparison evaluated ten interoperability solutions in general terms. This section extends the analysis to tokenized credit specifically, where three interactions produce a design space neither the interoperability literature nor the tokenization literature adequately addresses: the digital-twin vs digital-native distinction, the problem of perfecting security interests across chains, and the Travel Rule compliance architecture.

FIGURE IV Digital-Twin v. Digital-Native Tokenized Credit

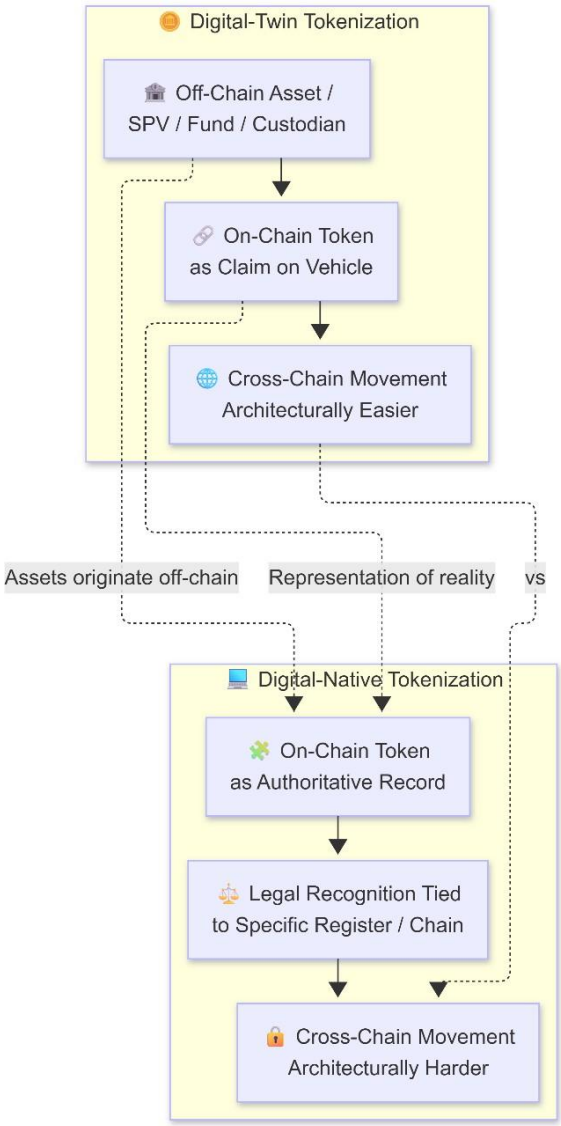

Figure IV. Digital-twin and digital-native tokenization differ in where legal authority resides and therefore in consequent cross-chain architectural implications.

Digital-Twin vs Digital-Native Tokenization in the Credit Context

The overwhelming majority of tokenized credit instruments deployed at scale through early 2026 follow the digital-twin pattern. BlackRock's BUIDL, Franklin Templeton's FOBXX (BENJI), Ondo's OUSG and USDY, and WisdomTree's tokenized funds are structured as digital-twin instruments where the on-chain token represents a claim against an off-chain Delaware-domiciled SPV or registered fund that holds the underlying Treasury securities. Tokenized private-credit products on Maple, Centrifuge, Goldfinch, and Credix similarly follow the digital-twin pattern. Table V summarizes the distinction across the dimensions most relevant to cross-chain credit design.

TABLE V Digital-Twin vs Digital-Native Tokenization in the Credit Context

Dimension	Digital-Twin	Digital-Native
Legal basis of ownership	Off-chain legal vehicle (SPV, fund, custodian) holds underlying asset; on-chain token is claim against vehicle	On-chain token is authoritative record of ownership under specific jurisdictional framework
Authority locus	Off-chain (governing-law of vehicle; usual contract/trust law)	On-chain (statutory register recognized under DLT Act, eWpG, etc.)
Cross-chain transfer	Architecturally trivial—token is a claim regardless of chain	Architecturally difficult—authoritative register lives on one chain
Example deployments	BUIDL, FOBXX, OUSG, WisdomTree; Maple, Centrifuge private credit	SIX Digital Exchange digital bonds, Sygnum, EIB digital bonds, Project Guardian pilots

Digital-twin tokenized credit inherits the legal frameworks of the off-chain vehicles that back it. A BUIDL token's holder has a claim against BlackRock Financial Management, Inc., as manager of the BlackRock USD Institutional Digital Liquidity Fund, under Delaware limited-partnership law supplemented by the fund's subscription agreement and investment-management agreement. The tokenization is an efficient distribution mechanism; the legal authority over the asset remains where off-chain legal infrastructure places it. Cross-chain movement of a BUIDL token is architecturally straightforward—the token remains a claim against the off-chain fund regardless of which chain holds it—but requires that the fund's transfer agent and recordkeeping systems recognize holders on destination chains.

Digital-native tokenized credit is comparatively rare in current deployments. The Swiss DLT Act's "ledger-based securities" framework (Art. 973d CO), Liechtenstein's TVTG, and Germany's eWpG have enabled a growing set of digital-native issuances (SIX Digital Exchange digital bonds, Sygnum Bank issuances, European Investment Bank digital bonds, certain MAS Project Guardian pilots), but these remain a small fraction of the tokenized-credit market [9,41]. The binding constraint is jurisdictional: the legal authority of a digital-native token depends on the register being recognized under a specific jurisdiction's framework, and extending that recognition across chains is not addressed by current law.

For cross-chain architectural implications: digital-twin tokenized credit can use permissionless burn-and-mint architectures (the off-chain vehicle's records treat wrapped tokens as claims identically to canonical tokens), provided the fund's transfer agent infrastructure can onboard holders on destination chains. Digital-native tokenized credit cannot use permissionless burn-and-mint without relinquishing its digital-native legal status, because the jurisdictional framework presumes a single authoritative register. The architecturally coherent pattern for digital-native cross-chain credit is authoritative-register-plus-projection: the canonical asset remains on its statutorily-recognized chain,

with non-authoritative representations on destination chains treated as derivative instruments (using IBC light-client verification, Category D permissioned-channel models, or CCIP CCT with burn-and-mint).

Perfected Security Interests and Cross-Chain Collateral

Article 9 of the UCC, as revised in 2022 to include new Article 12 on "controllable electronic records" (CERs), provides the primary US framework for perfecting security interests in digital assets [42]. A security interest in a CER may be perfected by "control" of the CER, with control defined in a manner adapted to distributed-ledger properties. Adoption across US states is incomplete as of early 2026; notably, New York enacted the 2022 amendments in December 2025 with provisions effective June 3, 2026 [43]. The amendments address primarily single-chain scenarios and presume the CER's governing law is identifiable.

The cross-chain perfection problem arises because "control" under Article 12 attaches to a specific chain-level representation. Lock-and-mint architectures fragment control: a lender perfecting a security interest in a canonical asset locked on Chain A does not automatically have control over wrapped representations on Chain B, yet the debtor may transfer the wrapped representation in ways that functionally transfer economic value. Burn-and-mint architectures preserve single-point control cleanly (canonical supply exists on exactly one chain at any instant, so "control" attaches unambiguously), but create attachment-continuity questions when the asset crosses chains. Natively multi-chain issuance creates parallel perfection obligations per chain, each under that chain's applicable law.

The digital-twin / digital-native distinction interacts with cross-chain perfection in consequential ways. For digital-twin collateral, perfection typically attaches to the off-chain claim—a security interest in a BUIDL token attaches under Delaware law to the limited-partnership interest the token represents—and cross-chain movement of the token does not fragment the security interest so long as the fund's records recognize the collateral arrangement. For digital-native collateral, perfection attaches to the on-chain register recognized under the relevant jurisdiction, and cross-chain projection to a non-authoritative representation on another chain does not automatically extend perfection. The regulatory gap is that Swiss DLT Act and eWpG single-authoritative-register models do not address cross-chain representations. The cross-chain perfection problem connects to T4 (legal enforceability) and T5 (default configurations): cross-chain credit infrastructure that defaults to permissionless cross-chain transfers does not automatically preserve the legal enforceability that the credit instrument's economic function depends on.

Compliance Architecture: Travel Rule Obligations

FATF Recommendation 16 requires originator and beneficiary information accompany virtual asset transfers above jurisdictional thresholds between VASPs [23]. In the single-chain case, Travel Rule compliance is addressed through TRP, TRISA, Sygna Bridge, and providers (Notabene, Sumsub, Veriscope) implementing IVMS 101 [26,27]. In the cross-chain case, three architectural problems arise.

Identity preservation. Most cross-chain messaging layers preserve transaction state (amount, asset, recipient address) but not identity information. Travel Rule information accompanying a Chain A transfer does not automatically accompany the wrapped representation on Chain B. Compliance requires either (a) out-of-band Travel Rule transmission parallel to the cross-chain transfer, (b) integration of Travel Rule data into the cross-chain messaging payload (few protocols support natively), or (c) restriction to closed networks where compliance is handled at the network-operator level.

Counterparty identification. Travel Rule presumes identifiable VASPs on both sides. In fully decentralized cross-chain transfers—where origination is from a non-custodial wallet and destination is a non-custodial wallet on a different chain—counterparty identification becomes acute. FATF guidance addresses this case but does not resolve the technical question [44].

Correlation of identity across chains. When a token exists in canonical form on Chain A and wrapped form on Chain B, Travel Rule information associated with the holder on A must correlate to the holder on B. Wallet addresses on different chains do not share identity namespaces; correlation requires either an identity layer (decentralized identity, verifiable credentials) or a trusted intermediary maintaining the mapping.

As developed in Section 5.7 and summarized in Table IV D9, Chainlink CCIP is the only public-chain protocol with a native compliance architecture; every other Category A, B, and C protocol handles Travel Rule as an off-chain overlay. Category D (Overledger + Oracle BCP) architecturally operationalizes the two-rail pattern—Travel Rule messaging on each bank's AML/KYC stack while settlement runs on permissioned ledgers [39]. None of this resolves the three architectural problems; it reveals that current practice manages them through institutional arrangements parallel to the cross-chain transfer rather than through on-chain primitives that bind identity to value movement natively—an arrangement that works within closed consortia but scales poorly to permissionless cross-chain credit markets.

Synthesis

The digital-twin / digital-native distinction and the perfected-security-interest problem are two refractions of the same question: where does legal authority reside, and how does it travel when the token crosses chains. Travel Rule compliance is the same problem under a different regulatory lens—both obligations presume identifiable, legally-liable parties on each side. The architectural patterns that best satisfy one tend to satisfy the other: closed-consortium permissioned infrastructure handles both cleanly; authoritative-register deployments with controlled projection handle both with overlay work; fully permissionless cross-chain tokenization handles neither natively and forces compliance into off-chain overlays that scale poorly to permissionless counterparties.

Tokenized cross-chain credit is a distinct design context—not a subset of DeFi interoperability, not a subset of RWA issuance, not a subset of institutional settlement, but a context in which all three sets of requirements must be satisfied simultaneously. No single protocol satisfies all five design tensions at once; the infrastructurally coherent pattern is a composition—an authoritative register in a cross-chain-tolerant asset-law

jurisdiction, issued as canonical burn-and-mint, projected via defense-in-depth verifier stack, with Travel Rule compliance on a parallel off-chain rail bound by cryptographic reference.

FIGURE V Tokenized Credit: Legal Authority, Settlement, and Compliance Rails

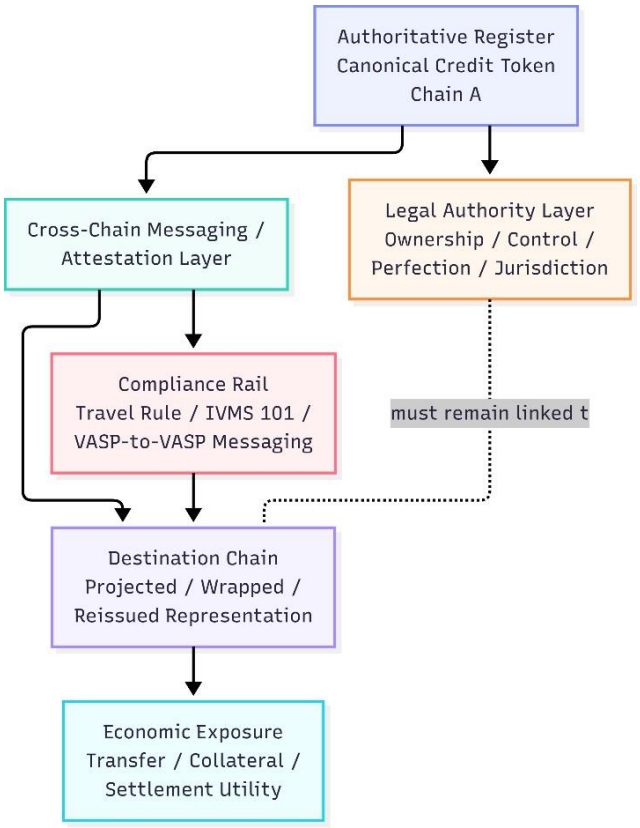

Figure V. Cross-chain tokenized credit requires coordinated handling of settlement, legal authority, and compliance rails rather than treating interoperability as a purely technical message-passing problem.

Research Agenda

The design space mapped in Sections 3 through 6 contains more open questions than resolved ones. Four research areas stand out. First, infrastructure-security composition: what formal frameworks can reason about security properties of compositions of cross-chain components (messaging layer, settlement layer, asset representation, application contracts), given that composition failures emerge from layer interactions rather than layer-level properties? Methodologies for identifying and disclosing correlated-dependency risk across shared upstream infrastructure (RPC providers, oracles, sequencers, prover services)—analogous to systemic-risk analysis in traditional finance—are an open problem [45]. Second, legal-authority portability across chains: how can the legal authority of a digital-native token be extended to wrapped representations on destination chains without relinquishing the single-register doctrines that jurisdictional frameworks (Swiss DLT Act, eWpG) depend on? Third, compliance architecture for decentralized cross-chain transfers: the three problems identified in Section 6.3 require both technical and regulatory innovation. Fourth, design-responsibility allocation and

disclosure: the KelpDAO dispute revealed that the field lacks vocabulary and accountability mechanisms for allocating responsibility between infrastructure providers and application developers when defaults function as prescriptive commitments. Developing such vocabulary—and the disclosure requirements, standards-of-care, and liability frameworks that follow from it—is foundational for the institutional maturation of cross-chain RWA infrastructure.

Discussion

The Design-Responsibility Argument

The paper's central analytical claim is that design-responsibility allocation between cross-chain infrastructure providers and application developers is under-theorized in ways that matter for the industry's institutional trajectory. The KelpDAO exploit provides the animating case: a single-verifier configuration adopted by 47 percent of active protocols produced a ~$292 million loss (116,500 rsETH), and the dispute between infrastructure provider and application developer turned on exactly the question the paper argues is under-theorized—who bears responsibility when infrastructure defaults shape high percentages of deployments. Infrastructure defaults in cross-chain contexts are prescriptive commitments rather than neutral starting points, the industry currently lacks vocabulary and accountability mechanisms for the shared-responsibility dynamics this produces, and developing such vocabulary is a central challenge for the field rather than a peripheral concern.

Implications for Practitioners

For application developers, default configurations require explicit review and documentation rather than implicit adoption. For infrastructure providers, defaults should reflect security properties appropriate for the most common deployment contexts rather than for the most flexible or permissive ones.

Implications for Regulators and Standards-Setting Bodies

For regulators, the composition and design-responsibility problems require frameworks addressing them as first-class concerns rather than treating them as settled by existing contract or tort law. For standards-setting bodies, coordinated work on cross-chain composition, default-configuration disclosure, and legal-authority portability is needed to support institutional maturation.

Limitations

The paper's analytical approach has explicit limitations. It is cartographic rather than empirical: it maps a design space rather than evaluating specific designs against metrics. Specific empirical claims about particular protocols' configurations, adoption patterns, and institutional deployments are snapshots that will age; the paper's analytical claims are intended to be robust to such changes but should be reevaluated as the industry evolves. The paper treats KelpDAO as an animating case rather than as a comprehensive empirical base; a full empirical treatment of cross-chain exploits would require work beyond the paper's scope. The paper addresses tokenized credit specifically because the analytical issues sharpen there, but the framework should extend to other tokenized RWA categories (real estate, intellectual property, commodities) with modifications the paper does not fully develop.

Conclusion

Cross-chain tokenization of real-world credit is at an inflection point. Institutional adoption accelerating through 2024–2026—BUIDL, BENJI, DTCC's commitment to tokenize $99 trillion in custodied securities, Canton Network's institutional expansion, regulated digital-native issuances under Swiss DLT Act and Project Guardian frameworks—has brought tokenization into contact with institutional requirements that purely on-chain assets did not face. The infrastructure supporting this scale is being designed now, and design choices being made will shape the industry for a decade. The paper's contribution is to argue those choices deserve more careful analysis than existing literatures provide, and to offer a framework that can support such analysis. The work framed—across composition, legal-authority portability, compliance architecture, and design-responsibility allocation—is substantial, interdisciplinary, and urgent. The industry's institutional aspirations depend on it being undertaken.

References

1. CoinDesk, "2026's biggest crypto exploit: KelpDAO hit for $292 million with wrapped ether (116,500 rsETH) stranded across 20 chains," Apr. 19, 2026.
2. CoinDesk, "LayerZero blames Kelp's setup for $290 million exploit, attributes it to North Korea's Lazarus," Apr. 20, 2026.
3. LayerZero Labs, "KelpDAO incident statement," Apr. 20, 2026.
4. CoinDesk, "KelpDAO claims LayerZero's default settings are what actually caused the $290 million disaster," Apr. 20, 2026.
5. The Defiant, "Dune Analytics reveals 47% of LayerZero OApps use minimal DVN security following KelpDAO hack," Apr. 20, 2026.
6. M. Zhang, X. Zhang, J. Barbee, Y. Zhang, and Z. Lin, "SoK: Security of cross-chain bridges: Attack surfaces, defenses, and open problems," arXiv preprint arXiv:2312.12573, Dec. 2023.
7. 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, pp. 1–41, 2022.
8. J. G. Allen, M. Rauchs, A. Blandin, and K. Bear, "Legal and regulatory considerations for digital assets," Cambridge Centre for Alternative Finance, University of Cambridge, Cambridge, UK, Oct. 2020.
9. Swiss Confederation, *Federal Act of 25 September 2020 on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act)*, AS 2021 33 (BBl 2020 233), adopted 25 September 2020, staggered entry into force 1 February 2021 and 1 August 2021.
    A. MacLean, R. M. Young, V. Bellotti, and T. P. Moran, "Questions, options, and criteria: Elements of design space analysis," *Human-Computer Interaction*, vol. 6, no. 3–4, pp. 201–250, 1991.
10. M. Shaw, "The coming-of-age of software architecture research," in *Proc. 23rd Int. Conf. Software Engineering (ICSE)*, 2001, pp. 656–664.
11. S. Easterbrook, J. Singer, M.-A. Storey, and D. Damian, "Selecting empirical methods for software engineering research," in *Guide to Advanced Empirical Software Engineering*, F. Shull, J. Singer, and D. Sjøberg, Eds. London, UK: Springer, 2008, pp. 285–311.

12. S.-S. Lee, A. Murashkin, M. Derka, and J. Gorzny, "SoK: Not quite water under the bridge — Review of cross-chain bridge hacks," in *Proc. 2023 IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, 2023, doi: 10.1109/ICBC56567.2023.10174993.
13. G. Wang, "SoK: Exploring blockchains interoperability," Cryptology ePrint Archive, Paper 2021/537, 2021.
14. V. Buterin, "Chain interoperability," R3 Research Paper, 2016.
15. J. Kwon and E. Buchman, "Cosmos: A network of distributed ledgers," Cosmos Whitepaper, 2016.
16. C. L. Reyes, "Creating cryptolaw for the uniform commercial code," *Washington and Lee Law Review*, vol. 78, no. 4, pp. 1521–1609, 2021.
17. Boston Consulting Group and ADDX, "Relevance of on-chain asset tokenization in 'crypto winter,'" BCG Report, 2022.
18. H. J. Allen, "DeFi: Shadow banking 2.0?," *William & Mary Law Review*, vol. 64, no. 4, pp. 919–968, 2023.
19. C. W. Mooney, Jr., "Beyond intermediation: A new (FinTech) model for securities holding infrastructures," *Univ. of Pennsylvania Journal of Business Law*, vol. 22, no. 2, pp. 386–442, 2020.
20. D. Fox and S. Green, Eds., *Cryptocurrencies in Public and Private Law*. Oxford, UK: Oxford Univ. Press, 2019.
21. UNIDROIT, *Principles on Digital Assets and Private Law*. Rome, Italy: International Institute for the Unification of Private Law, 2023.
22. Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris, France: FATF, 2021.
23. Elliptic, "The Travel Rule: Industry moves towards a full solution," Elliptic Research, 2023.
24. Financial Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*. Paris, France: FATF, Jun. 2023.
25. Joint Working Group on interVASP Messaging Standards (JWG), "IVMS 101 — interVASP Data Model Standard (Issue 1)," May 2020.
26. InterVASP Standards Working Group, "IVMS 101: Updated specification (v2024)," ratified Jun. 4, 2024.
27. Digital Asset, "Canton Network: A privacy-enabled network of networks for institutional assets," Digital Asset Whitepaper, 2023.
28. Wormhole Foundation, "Guardian network, VAA specification, and Native Token Transfers framework," Wormhole Documentation, 2025.
29. Axelar Foundation, "Maeve upgrade: Quadratic voting for cross-chain transaction validation," Axelar Network blog and Axelar Documentation, Aug. 2022, updated 2025.
30. Chainlink Labs, "CCIP architecture: Decentralized Oracle Network, Risk Management Network, and Cross-Chain Token standard (v1.5)," Chainlink CCIP Documentation, Jan. 2025.
31. Depository Trust & Clearing Corporation, "Smart NAV pilot report with BNY Mellon, Franklin Templeton, JP Morgan, State Street, and Invesco," DTCC, May 2024.
32. Interchain Foundation, "IBC v2 (Eureka) technical walkthrough: SP1-verified Tendermint light client on Ethereum," Cosmos Network Blog and ibcprotocol.dev,

Mar. 2025.
33. Web3 Foundation and Parity Technologies, "XCM v5 specification and HRMP channel semantics," Polkadot Wiki and Developer Documentation, May 2025.
34. Succinct Labs, "SP1 Hypercube: Real-time proving of Ethereum L1 blocks in under 12 seconds on 16 GPUs," Succinct Blog, 2025; "Succinct Prover Network mainnet launch," Aug. 5, 2025.
35. Polyhedra Network, "zkBridge proof systems: Virgo, deVirgo, Orion, Gemini, Pianist, and Expander," zkBridge Documentation, 2024–2025.
36. Quant Network, "Quant partners with Oracle to drive digital assets innovation," press release, Feb. 14, 2025.
37. Oracle Corporation, "Unveiling Oracle Blockchain Platform Digital Assets Edition," Oracle Blockchain Blog, Feb. 2025; "Atomic cross-channel updates and Ethereum interoperability via last-resource-commit," Oracle Blockchain Platform documentation (release 25.4.1), Dec. 2025.
38. UK Finance, "UK Finance announces live pilot phase to deliver tokenised sterling deposits," Sep. 26, 2025.
39. Bank for International Settlements Innovation Hub London Centre and Bank of England, "Project Rosalind: Building API prototypes for retail CBDC ecosystem innovation," BIS Paper No. 69, Jun. 2023.
40. German Bundestag, *Gesetz über elektronische Wertpapiere (eWpG) of 3 June 2021*, BGBl. I S. 1423, in force 10 June 2021.
41. American Law Institute and Uniform Law Commission, *Uniform Commercial Code Amendments (2022): New Article 12 — Controllable Electronic Records*, approved by ALI 18 May 2022 and by ULC at its July 2022 Annual Meeting.
42. Orrick, Herrington & Sutcliffe LLP, "New York enacts 2022 UCC amendments (effective June 3, 2026)," Orrick Legal Update, Dec. 2025.
43. Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation — The FATF Recommendations*. Paris, France: FATF, 2012 (last updated October 2025).
44. V. V. Acharya, L. H. Pedersen, T. Philippon, and M. Richardson, "Measuring systemic risk," *Review of Financial Studies*, vol. 30, no. 1, pp. 2–47, 2017.