

A Conceptual Architecture for Cross-Chain Interoperability and Dynamic Compliance in RWA Tokenization

Md Abul Mansur

Nuspay International Inc., United States

[Doi:10.19044/esj.2026.v22n25p1](https://doi.org/10.19044/esj.2026.v22n25p1)

Submitted: 08 March 2026

Accepted: 28 September 2026

Published: 30 September 2026

Copyright 2026 Author(s)

Under Creative Commons CC-BY 4.0

OPEN ACCESS

Cite As:

Mansur, M.A. (2026). *A Conceptual Architecture for Cross-Chain Interoperability and Dynamic Compliance in RWA Tokenization*. European Scientific Journal, ESJ, 22 (25), 1.

<https://doi.org/10.19044/esj.2026.v22n25p1>

Abstract

The tokenization of Real-World Assets (RWAs) offers opportunities to connect traditional financial instruments with decentralized infrastructure. However, institutional adoption faces a structural bottleneck: “walled garden” liquidity fragmentation. Regulatory differences, isolated blockchain networks, and static compliance logic can restrict cross-chain asset mobility and require repeated identity verification across platforms and jurisdictions. This study proposes a conceptual architectural framework for cross-chain interoperability and dynamic compliance in regulated digital assets. Using qualitative architectural analysis, the framework combines the ERC-3643 token standard, Decentralized Identifiers (DIDs), off-chain Verifiable Credentials, Zero-Knowledge Proofs (ZKPs), and cross-chain messaging. It separates asset execution from identity and compliance functions and conceptually supports supply-preserving cross-chain transfers with destination-side eligibility checks, while reducing the need to disclose personal identity data on-chain. The proposed design could reduce technical and compliance-related barriers to asset mobility, subject to implementation security, credential governance, and applicable legal requirements. No integrated prototype, measured benchmark results, or empirical validation are presented; its effects on liquidity, performance, and regulatory compliance therefore remain to be evaluated. The contribution is an architectural basis for further implementation and testing, with implications for policymakers and protocol developers examining interoperable, privacy-preserving RWA infrastructure.

Keywords: Real-World Asset Tokenization, Cross-Chain Interoperability, Dynamic Compliance, Zero-Knowledge Proofs, Decentralized Identity, Liquidity Fragmentation, ERC-3643 Standard, Algorithmic Regulation

1. Introduction

1.1 Background and context

The evolution of Real-World Asset (RWA) tokenization. The tokenization of RWAs represents a structural shift in financial-market infrastructure, using distributed ledgers to represent claims on financial, physical, or intangible assets as programmable digital tokens. Recent institutional activity has expanded beyond pilot projects into tokenized government securities, funds, private credit, and other financial claims, although adoption remains at an early stage (OECD, 2025). The literature identifies potential benefits including automation, faster settlement, fractional access, and reduced reconciliation costs, while also emphasizing legal, governance, and interoperability constraints (Aldasoro et al., 2023; OECD, 2025).

1.2 Problem statement

The "walled garden" liquidity crisis and regulatory friction. In this study, a "walled garden" refers to a closed technical or regulatory environment in which an asset can circulate only within a particular network or among pre-approved participants. Tokenization can fractionalize assets, but it does not by itself create secondary-market turnover. Strict anti-money laundering (AML) and know-your-customer (KYC) requirements often lead issuers to use permissioned networks or transfer-restricted smart contracts, which can fragment liquidity across separate venues. Public blockchains create an additional privacy concern because transaction activity is visible to network participants. This can expose institutional trading patterns to maximal extractable value (MEV), meaning value that block producers or automated actors may obtain by reordering, inserting, or censoring transactions (Daian et al., 2020). Regulatory requirements also differ across jurisdictions; for example, the European Union's Markets in Crypto-Assets (MiCA) regime establishes a harmonized framework for covered crypto-assets and service providers, but it does not eliminate cross-border differences in the treatment of tokenized financial instruments (European Parliament & Council of the European Union, 2023; OECD, 2025).

1.3 Research objectives and questions

To explore how cross-chain asset mobility could be supported alongside regulatory compliance, this study proposes a conceptual framework

for RWA interoperability. The research is guided by the following core objectives:

- To examine the economic implications and technical challenges of liquidity fragmentation across different blockchain networks.
- To architect a dynamic compliance model utilizing permissioned token standards (specifically ERC-3643) combined with Decentralized Identifiers (DIDs), enabling tokens to navigate diverse regulatory jurisdictions programmatically.
- To determine how cryptographic primitives, such as Zero-Knowledge Proofs (ZKPs), can be integrated into cross-chain messaging protocols to facilitate institutional privacy while ensuring verifiable on-chain regulatory adherence.

1.4 Significance of the study and value proposition

This research addresses a gap between technical work on blockchain interoperability and legal work on regulated digital assets. It examines how ERC-3643, an Ethereum token standard designed for permissioned and compliant transfers of regulated tokens (Lebrun et al., 2021), can be combined with privacy-preserving identity proofs and cross-chain messaging. The policy discussion considers MiCA and the EU's Sixth Anti-Money Laundering Directive (AMLD6), which establishes mechanisms for preventing the use of the financial system for money laundering or terrorist financing (European Parliament & Council of the European Union, 2024). The objective is to identify an architecture that can reduce post-issuance fragmentation without treating regulatory compliance as an afterthought.

1.5 Structure of the paper

The remainder of this article is organized as follows. Section 2 presents a comprehensive literature review, examining the current state of institutional tokenization, network fragmentation, and regulatory asymmetry. Section 3 details the research methodology, outlining the qualitative architectural analysis and evaluation metrics employed. In Section 4, the study conducts an in-depth diagnostic of the structural bottlenecks within RWA markets, quantifying the economic impact of the walled garden phenomenon. Section 5 introduces the core contribution of this paper: the proposed architectural framework for cross-chain interoperability and zero-knowledge dynamic compliance. Section 6 contextualizes these technical solutions within current market implications and European regulatory standards. Section 7 acknowledges the technical and legal limitations of algorithmic enforcement. Finally, Section 8 concludes the paper with a synthesis of key findings and actionable recommendations for future institutional infrastructure.

2. Literature review and theoretical framework

2.1 Current state of institutional RWA tokenization

Institutional RWA tokenization has moved from experimental sandboxes toward live products in government securities, funds, and digital bonds. BlackRock's BlackRock USD Institutional Digital Liquidity Fund (BUIDL), a tokenized investment fund issued on Ethereum, is one prominent example (BlackRock, 2024). ABN AMRO, a Dutch banking group, has also issued a digital bond on a public blockchain (ABN AMRO, 2023). These deployments demonstrate growing institutional interest, but they do not by themselves establish deep secondary markets. Policy research continues to identify interoperability, legal certainty, settlement design, and market fragmentation as material constraints on broader adoption (OECD, 2025).

2.2 Blockchain fragmentation and interoperability challenges

A primary technical barrier to RWA liquidity is network fragmentation. Blockchains operate with different consensus mechanisms, state models, cryptographic assumptions, and governance arrangements. When economically related assets are issued on separate networks, liquidity and transaction activity can become divided across those environments, reducing direct composability between them (Belchior et al., 2022). Blockchain fragmentation raises interoperability challenges related to trust assumptions, connectivity across networks, and support for cross-chain data and asset transfers (Kotey et al., 2023). Earlier bridge designs frequently relied on wrapped assets, external validators, or custody arrangements that introduced additional security assumptions. Academic surveys and security studies therefore treat cross-chain communication as both an interoperability problem and a distinct security boundary (Belchior et al., 2022; Notland et al., 2026; Zamyatin et al., 2021). Protocols such as the Cross-Chain Interoperability Protocol (CCIP) illustrate the more recent shift toward generalized cross-chain messaging, although regulated assets still require the destination network to evaluate legal and identity-related conditions (Chainlink Labs, n.d.).

2.3 Regulatory asymmetry across jurisdictions

Technical fragmentation is compounded by differences in legal classification and jurisdictional requirements. "RWA tokenization" describes a technical representation of assets or claims rather than a single regulatory category. In the European Union, Article 2(4)(a) of MiCA excludes crypto-assets that qualify as financial instruments. Tokenized securities and tokens representing units in collective investment undertakings must therefore be assessed under the relevant financial-instrument and fund frameworks, rather than treated automatically as MiCA-covered assets. Classification depends on

the rights and economic characteristics of the instrument, not its token label or blockchain standard (European Parliament & Council of the European Union, 2023; ESMA, 2025).

Other MiCA-covered crypto-assets: Crypto-assets that are neither asset-referenced tokens nor e-money tokens may fall under MiCA Title II, subject to its scope and exemptions.

Tokenized securities: Tokens qualifying as transferable securities are financial instruments. They are excluded from MiCA and remain subject to applicable securities-market requirements.

Fund tokens: Tokens qualifying as units in collective investment undertakings are financial instruments. Applicable fund rules, including UCITS or AIFMD where relevant, require separate assessment.

Stablecoins: “Stablecoin” is not a single legal category. Tokens referencing one official currency may qualify as e-money tokens, while tokens referencing other values, rights, or combinations may qualify as asset-referenced tokens, subject to the statutory definitions and exclusions.

Tokenized deposits and other instruments: Deposits, including structured deposits, are excluded from MiCA. Other tokenized instruments require assessment against the relevant financial-services categories and exclusions.

2.4 Existing compliance mechanisms: KYC/AML in permissioned and public ledgers

To manage these requirements, issuers have generally relied on either permissioned infrastructure or public networks with transfer restrictions. Each approach improves control but can limit market fluidity.

- Permissioned ledgers restrict network participation to identified or authorized entities. Hyperledger Fabric, for example, uses a membership-based architecture that can integrate enterprise identity controls (Androulaki et al., 2018). This design supports governance and access control, but assets issued inside a private network do not automatically interoperate with liquidity or applications on other chains.
- Public ledgers with static smart contracts can enforce transfer restrictions while retaining access to public blockchain infrastructure. ERC-3643, for example, conditions token transfers on identity and compliance checks (Lebrun et al., 2021). This can still create a walled garden at the token level when only pre-approved addresses are eligible to transact. Data protection also requires care: placing personally identifiable information on an immutable ledger can

conflict with principles such as storage limitation, erasure, and data minimization under the General Data Protection Regulation (GDPR) (European Parliament & Council of the European Union, 2016; Finck, 2019).

2.5 Gap analysis: limitations of current dynamic solutions

The literature identifies mature lines of work on blockchain interoperability, cross-chain security, privacy-preserving cryptography, and regulatory treatment, but these areas are often examined separately (Belchior et al., 2022; Kotey et al., 2023; OECD, 2025). Interoperability studies primarily analyze communication and trust assumptions, whereas privacy research focuses on proving statements without revealing underlying data (Goldwasser et al., 1989; Groth, 2016). The gap addressed here is therefore architectural: how to combine cross-chain messaging, regulated token controls, decentralized identity, and privacy-preserving eligibility proofs in a single conceptual design for RWAs.

3. Methodology

This study uses a conceptual architectural research approach informed by Design Science Research (DSR), supported by qualitative analysis of published technical standards, academic literature, regulatory texts, and institutional examples. The research develops a proposed architecture for cross-chain RWA transfers by examining how existing interoperability, identity, privacy, and compliance mechanisms could be combined. Its output is a conceptual design rather than an implemented or validated system. The study does not include a prototype, simulation, testnet deployment, performance measurements, or systematic numerical scoring of protocols. Section 7.1.1 provides a qualitative architectural threat model, but no formal security verification or empirical security testing has been conducted.

3.1 Research design

The research design uses comparative architectural analysis and case-study synthesis. Because standardized secondary-market data for tokenized RWAs remain limited, the study focuses on protocol architectures, trust assumptions, identity and compliance mechanisms, and representative institutional deployments.

The study follows a three-phase design:

- Examination of existing approaches. Published sources are used to identify limitations of permissioned networks, transfer-restricted tokens, and existing cross-chain mechanisms, with particular attention to liquidity fragmentation, identity verification, and privacy.

- Qualitative comparison of architectural options. Cross-chain transfer mechanisms are compared descriptively in terms of their execution models, trust assumptions, security dependencies, and potential suitability for regulated RWAs. The comparison draws on published interoperability and security research rather than experimental testing or numerical scoring (Belchior et al., 2022; Zamyatin et al., 2021).
- Conceptual architectural synthesis. The analysis informs a proposed integration of ERC-3643 token controls, decentralized identity, off-chain Verifiable Credentials, zero-knowledge proofs, and cross-chain messaging. The resulting design specifies component responsibilities and an illustrative transaction lifecycle. Its feasibility and effectiveness remain subject to implementation and evaluation.

3.2 Data collection and sources

Data for this research are derived from primary technical standards, regulatory texts, peer-reviewed computer-science literature, policy research, and selected institutional case studies.

- Technical specifications are drawn from Ethereum Improvement Proposals for ERC-20 and ERC-3643, together with W3C standards for Decentralized Identifiers (DIDs) and Verifiable Credentials (Lebrun et al., 2021; Vogelsteller & Buterin, 2015; World Wide Web Consortium [W3C], 2022, 2025). ONCHAINID, referenced in the proposed architecture, is an identity framework used in ERC-3643 implementations to associate blockchain addresses with verified identity claims; it is treated here as an implementation component rather than as a substitute for the W3C DID standard.
- Regulatory sources include the EU's MiCA regulation, GDPR, and AMLD6, supplemented by comparative policy analysis of tokenized financial markets (European Parliament & Council of the European Union, 2016, 2023, 2024; OECD, 2025).
- Institutional case studies include BlackRock's BUIDL fund and ABN AMRO's public-blockchain digital bond, used as examples of live institutional tokenization rather than as performance benchmarks (ABN AMRO, 2023; BlackRock, 2024).

Sources are used according to their evidential role. Academic research supports the analysis of interoperability, cryptographic mechanisms, and security limitations. Regulatory texts and official supervisory guidance establish the relevant legal scope, while technical standards define token and identity interfaces. Corporate documentation describes specific implementations and reported institutional activities. It is not treated as independent evidence of the proposed architecture's security, performance, regulatory acceptance, or market-wide benefits.

3.3 Assessment criteria and proposed evaluation metrics

To ensure the proposed architecture is both technically scalable and legally robust, the study establishes a dual-faceted evaluation matrix. Table 1 identifies criteria relevant to assessing the proposed architecture. Security and trust assumptions, identity and compliance controls, privacy, and jurisdictional adaptability are considered qualitatively through the architectural discussion. Latency and gas consumption are identified as metrics for future implementation-based testing; they are not measured in this study. The matrix therefore organizes assessment criteria rather than presenting validated performance results.

Table 1: Evaluation metrics for RWA interoperability and compliance

Category	Metric	Definition and operational goal
Cross-chain performance	Latency (mint and full-cycle)	Time required to finalize the source-chain state and authorize the corresponding destination-chain state change. The benchmark protocol records end-to-end finality under stated test conditions (Zamyatin et al., 2021).
Cross-chain performance	Gas efficiency and cost	Computational cost of cross-chain messaging, token-state changes, and verification, measured in native gas units and network fees.
Cross-chain performance	Security and trust assumptions	Degree to which the transfer depends on external validators, custody, or additional trust assumptions beyond the underlying chains (Belchior et al., 2022; Zamyatin et al., 2021).
Smart-contract compliance	Dynamic KYC/AML enforcement	Ability of the compliance layer to evaluate identity and transfer eligibility before a regulated token transfer (Lebrun et al., 2021).
Smart-contract compliance	Data privacy (GDPR alignment)	Ability to verify eligibility without publishing personally identifiable information on-chain; zk-SNARK verification is evaluated as a privacy-preserving mechanism (Groth, 2016).
Smart-contract compliance	Jurisdictional adaptability	Ability to update compliance parameters without migrating the core token contract.

These criteria structure the discussion of the design and identify requirements for subsequent evaluation. The qualitative analysis describes intended capabilities and dependencies; it does not establish measured scalability, legal compliance, or operational effectiveness.

3.4 Proposed benchmarking plan for future validation

Future evaluation should implement the proposed components and measure three dimensions: gas consumption for representative ERC-3643 operations and proof verification; zero-knowledge proof-generation and verification latency; and end-to-end cross-chain execution time. Testing should document hardware, software versions, contract configurations, proof-

system parameters, network conditions, finality assumptions, and the number of repeated trials. Results should distinguish successful transfers from failed or delayed transactions and report variation across trials. A separate security assessment should define the threat model and examine message replay, compromised credentials, unauthorized minting, and destination-side compliance failures. This study does not perform these tests or report benchmark results; the plan identifies work required to evaluate the conceptual architecture..

4. Structural bottlenecks of RWA markets

As RWA tokenization moves toward institutional use, three interconnected constraints remain central to the proposed design: technical fragmentation, regulatory rigidity, and the privacy tension created by transparent ledgers.

4.1 Technical silos and fragmented liquidity

Blockchain ecosystems contain many networks that are not natively interoperable. When tokenized RWAs are issued across separate public and permissioned ledgers, trading interest and market depth can be divided among those venues. This can complicate price discovery, collateral mobility, and secondary-market access.

Fragmented liquidity can reduce market depth and produce uneven pricing across otherwise comparable venues. Cross-chain movement also introduces additional fees, latency, and security assumptions, particularly when bridge designs rely on external validators, wrapped assets, or custody mechanisms (Belchior et al., 2022; Zamyatin et al., 2021). These frictions can suppress secondary-market turnover and complicate institutional allocation.

4.2 Static smart contracts and fluid global regulations

The second bottleneck is the mismatch between relatively static smart-contract logic and changing legal requirements. Tokenized securities can be subject to different transfer restrictions, investor-eligibility rules, sanctions controls, and data-protection obligations across jurisdictions. A contract configured for one regulatory perimeter cannot safely assume that the same rules apply elsewhere. The proposed architecture therefore separates the token ledger from an updateable compliance layer, while recognizing that legal interpretation and governing-law questions cannot be reduced entirely to code (European Parliament & Council of the European Union, 2023; OECD, 2025).

4.3 Privacy paradox: institutional confidentiality and on-chain transparency

The third barrier is the privacy tension inherent in public ledgers. Although blockchain addresses are pseudonymous, transaction histories and smart-contract interactions are visible on-chain. For institutional participants, such visibility may reveal trading patterns, counterparties, or portfolio activity.

Privacy-preserving eligibility verification

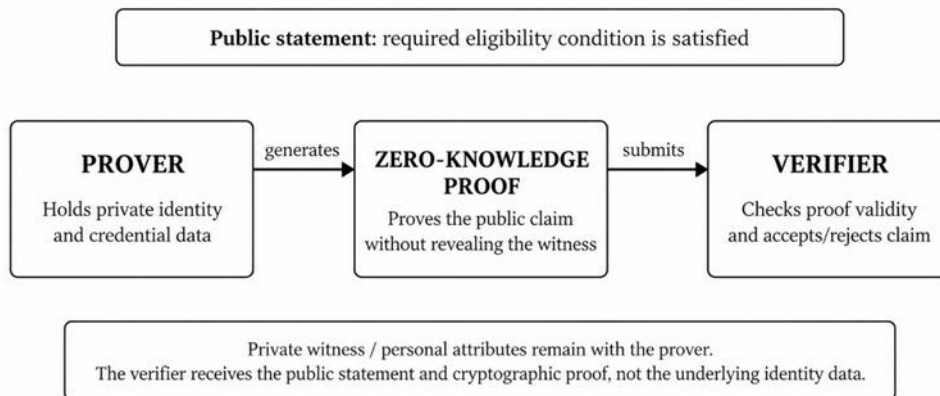


Figure 1: Conceptual representation of a zero-knowledge proof

Transparent transaction ordering can expose trading activity to MEV strategies (Daian et al., 2020). A separate concern arises when identity information is placed on immutable infrastructure: direct on-chain storage of personally identifiable information can conflict with GDPR requirements and data-protection principles (European Parliament & Council of the European Union, 2016; Finck, 2019). The proposed design therefore treats identity evidence as off-chain data and uses cryptographic proofs to verify eligibility without publishing the underlying personal information.

Table 2: Institutional privacy paradox in RWA tokenization

Operational requirement	Public-blockchain condition	Privacy-preserving response
Trade confidentiality	Transaction values, asset interactions, and execution timing can be visible on-chain.	Zero-knowledge proofs can demonstrate the validity of a statement without disclosing the underlying witness or unnecessary transaction data (Goldwasser et al., 1989; Groth, 2016).
Regulatory compliance (KYC/AML)	Transfer eligibility must be linked to verified identity evidence.	DIDs and off-chain Verifiable Credentials can separate identity data from the public ledger while supporting cryptographic verification (W3C, 2022, 2025).

Data privacy (GDPR alignment)	Publishing PII to an immutable ledger can conflict with data-protection requirements.	Keep PII off-chain and verify only the minimum required eligibility claim through cryptographic proofs (European Parliament & Council of the European Union, 2016; Finck, 2019).
-------------------------------	---	--

The design objective is privacy-preserving verification: the ledger should be able to verify a compliance statement without receiving the underlying identity data. Zero-knowledge proofs provide the cryptographic basis for this approach (Goldwasser et al., 1989; Groth, 2016).

5. Proposed architectural framework

The principal output of this study is a conceptual architecture addressing the liquidity fragmentation and privacy constraints identified in Section 4. The design combines ERC-3643 token controls, decentralized identity, off-chain Verifiable Credentials, zero-knowledge proofs, oracle-based regulatory inputs, and cross-chain messaging. It specifies component responsibilities and a proposed transaction sequence, rather than demonstrating an operational solution. Figures 1–2 and Tables 1–5 illustrate the underlying concepts, assessment criteria, and design relationships; they do not provide empirical evidence of the architecture’s effectiveness.

Throughout this paper, dynamic compliance refers to the evaluation of transfer eligibility using governed, updateable rules and credential-status information. The compliance payload comprises the proof and associated public inputs or references required for cross-chain eligibility verification; it excludes complete credentials and underlying personal records. Oracle updates refer to authenticated updates from approved off-chain sources. CCIP-style messaging denotes the proposed messaging design informed by CCIP documentation, while burn-and-mint denotes source-chain token destruction followed by equivalent destination-chain issuance after the required checks.

5.1 Cross-chain interoperability design for RWAs

The proposed architecture considers how cross-chain messaging could connect otherwise separate, network-specific RWA deployments. Historically, attempts to connect disparate ledgers have been hindered by the Interoperability Trilemma, which posits that cross-chain protocols can optimize for only two of three properties: trustlessness (security), extensibility (scalability across many chains), and generalizability (the ability to handle complex arbitrary data). Institutional RWAs therefore require a shift from legacy token bridges to cross-chain messaging protocols that prioritize security and support complex data exchange.

5.2 Messaging standards and asset bridging mechanisms

Traditional token bridges commonly lock assets on a source chain and represent them on another chain, introducing additional custody, validator, or smart-contract assumptions. Security research shows that bridge architecture creates a distinct attack surface and that wrapped representations can fragment liquidity when multiple versions of an asset coexist (Notland et al., 2026; Zhang et al., 2024; Zamyatin et al., 2021). The proposed framework uses generalized cross-chain messaging to coordinate asset-state changes and associated compliance information. Its analysis of communication models and trust dependencies draws on academic interoperability research (Belchior et al., 2022; Zamyatin et al., 2021). Chainlink CCIP documentation supplies an implementation reference for the proposed messaging layer, rather than independent validation of the integrated design (Chainlink Labs, n.d.). Table 3 compares the principal transfer models considered in this study.

Table 3: Comparative analysis of cross-chain bridging mechanisms for RWAs

Bridging mechanism	Technical execution	Security assumptions and vulnerabilities	Suitability for institutional RWAs
Lock-and-mint	Tokens are locked on the source chain and a wrapped representation is minted on the destination chain (Zamyatin et al., 2021).	Depends on the security of the bridge custody or verification mechanism; locked assets can create concentrated risk.	Low to moderate. It can create multiple wrapped representations and additional custody assumptions.
Lock-and-unlock (liquidity pools)	Tokens are locked on the source chain while pre-funded liquidity is released on the destination chain.	Requires sufficient destination liquidity and introduces liquidity-provider and rebalancing dependencies.	Moderate for fungible, liquid assets; less suitable for unique or tightly controlled regulated tokens.
Burn-and-mint (proposed model)	Tokens are burned on the source chain and an equivalent amount is minted on the destination chain after verified cross-chain attestation (Chainlink Labs, n.d.).	Requires tightly governed mint/burn permissions and secure message verification; it avoids a pooled locked-asset honeypot.	High within the proposed design because it preserves aggregate token supply without creating a wrapped version.

For this conceptual architecture, burn-and-mint is used as a supply-preserving cross-chain transfer method: a specified token amount is destroyed on the source chain and an equivalent amount is issued on the destination chain after verification. This avoids maintaining multiple wrapped representations of the same regulated token, although the mechanism still depends on secure cross-chain attestation and correctly governed mint-and-burn permissions (Chainlink Labs, n.d.; Zamyatin et al., 2021).

5.3 Decentralized validation architecture

Executing a burn-and-mint transfer requires high confidence that the source-chain state is final before the destination chain authorizes minting. In the proposed design, this validation is handled by Decentralized Oracle Networks (DONs), meaning groups of independent oracle nodes that collectively observe, attest to, and relay cross-chain state. The separation of message commitment, execution, and risk monitoring follows the CCIP implementation described in its documentation (Chainlink Labs, n.d.). Assessment of the resulting trust assumptions and attack surfaces draws separately on cross-chain security research; the presence of these components does not establish the security of the proposed integration (Zamyatin et al., 2021; Zhang et al., 2024).

- The committing network observes the finalized burn event and its compliance payload on the source blockchain. It signs a Merkle root, a single cryptographic hash that commits to the contents of a Merkle tree, and commits the resulting message to the destination network.
- The executing network independently verifies the committed message and triggers the destination smart contract only after the required cross-chain checks succeed.
- The Risk Management Network (RMN) operates as an independent monitoring layer. It checks cross-chain messages for anomalous conditions and can halt execution when configured safety conditions are breached (Chainlink Labs, n.d.).

This messaging architecture is intended to support cross-chain transfers of tokenized RWAs while transmitting the compliance payload needed for destination-side verification.

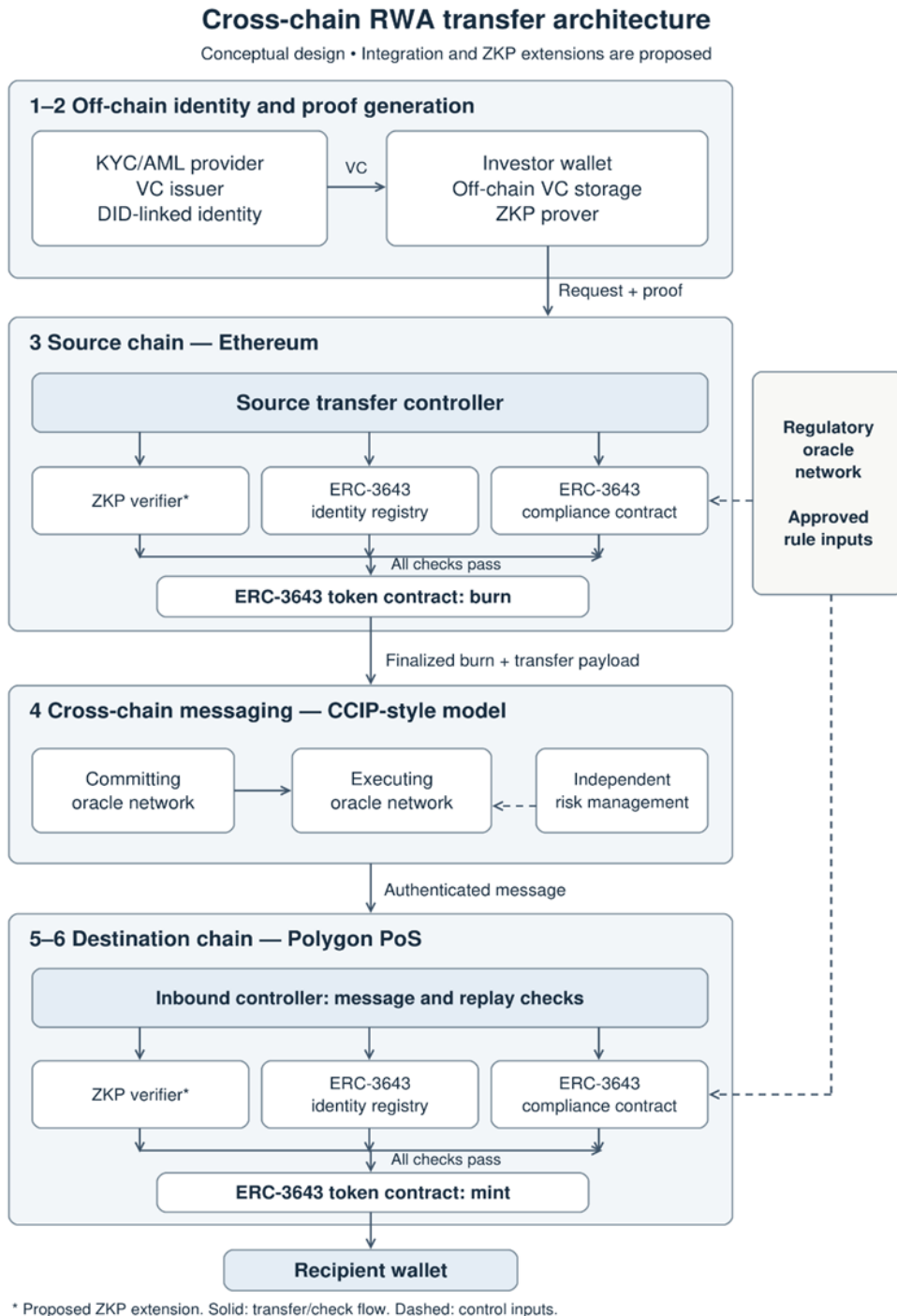


Figure 2: High-level cross-chain RWA compliance and interoperability architecture

Figure 2 presents the proposed component interactions for a cross-chain RWA transfer. Solid arrows represent credential delivery, transaction requests, verification results, and cross-chain messages. Dashed arrows represent regulatory updates and risk-management controls. The transfer controllers and zero-knowledge verification modules represent proposed integration components whose implementation and effectiveness remain unvalidated.

- **Credential issuance:** An authorized KYC/AML provider verifies the investor and issues an off-chain Verifiable Credential linked to the investor's digital identity. The credential and underlying personal information remain off-chain.
- **Proof generation and submission:** The investor wallet acts as the prover and generates an eligibility proof for the requested transfer. The proposed proof must be bound to the relevant transfer details, including the asset, amount, recipient, destination network, and a unique transfer identifier.
- **Source-chain checks and burning:** The source controller coordinates proof verification, identity-registry checks, and compliance-contract evaluation. These modules return verification results; they do not themselves burn tokens. If the required checks pass, an authorized operation burns the specified amount through the source ERC-3643 token contract.
- **Cross-chain attestation:** After source-chain finality, the messaging layer commits and relays the burn event and associated transfer payload. An independent risk-management layer monitors the messaging process and can prevent execution when configured safety conditions are breached.
- **Destination-side validation:** The destination controller checks message authenticity and replay protection, then coordinates proof verification, recipient-identity checks, and evaluation of current destination-side compliance rules. Approved oracle inputs inform the compliance rules on each chain; they do not replace identity or proof verification.
- **Destination minting:** An authorized operation mints the equivalent amount to the recipient only after all destination checks succeed. A failed check prevents minting. If a failure occurs after the source burn, the transfer remains unresolved pending a defined recovery procedure; secure recovery and retry behavior require further specification and testing.

5.4 Dynamic compliance and decentralized identity (DID)

Technical interoperability alone is insufficient for regulated RWAs because transfer eligibility must also be evaluated. ERC-3643, formally titled T-REX (Token for Regulated EXchanges), extends the ERC-20 token interface with identity, compliance, freeze, recovery, mint, and burn functions for regulated tokens (Lebrun et al., 2021; Vogelsteller & Buterin, 2015). In this manuscript, the compliance contract refers to the smart-contract module that evaluates transaction-level regulatory rules before a transfer is executed. The architecture also uses ONCHAINID as the identity-registry implementation associated with ERC-3643, while DIDs and Verifiable Credentials provide the broader standards-based identity model (W3C, 2022, 2025).

Table 4: Core modular components of the ERC-3643 identity and compliance framework

Smart-contract module	Functional responsibility	Role in the transfer lifecycle
Token contract	Handles regulated token operations, including transfer, mint, burn, pause, and recovery functions.	Executes the state change only after the relevant identity and compliance conditions are satisfied (Lebrun et al., 2021).
Identity registry	Maps wallet addresses to identity records and evaluates whether the required claims are valid.	Confirms that the relevant participant satisfies configured identity requirements through <code>isVerified()</code> (Lebrun et al., 2021).
Compliance contract	Contains transaction-level rules such as investor limits, transfer restrictions, or lock-up conditions.	Evaluates whether the proposed transfer satisfies the configured compliance rules before execution (Lebrun et al., 2021).

5.4.1 Privacy-preserving KYC with zero-knowledge proofs (ZKPs)

Placing identity attributes directly on a public or consortium ledger creates data-protection risks. GDPR requires data controllers to consider principles including data minimization, storage limitation, and erasure, which are difficult to reconcile with immutable publication of personal data (European Parliament & Council of the European Union, 2016; Finck, 2019). The proposed architecture therefore uses zero-knowledge proofs, specifically zk-SNARK-style proofs, in the compliance workflow. A zero-knowledge proof allows a prover to demonstrate that a statement is true without disclosing the witness or underlying information beyond what the proof itself reveals (Goldwasser et al., 1989). zk-SNARK constructions provide succinct, non-interactive verification suitable for compact cryptographic claims (Groth, 2016).

The proposed integration comprises three steps:

- Credential issuance begins with an off-chain regulated KYC/AML provider verifying the investor and issuing a Verifiable Credential to the investor's wallet. The credential remains off-chain and follows the issuer-holder-verifier model formalized by the W3C Verifiable Credentials standard (W3C, 2025).
- Selective disclosure via ZKP allows the wallet to prove a required compliance condition, such as accreditation or non-sanctioned jurisdiction status, without revealing unnecessary attributes such as the user's name, precise net worth, or residential address.
- On-chain verification uses the ERC-3643 Identity Registry's `isVerified()` function. In ERC-3643, `isVerified()` is a Boolean eligibility check that returns true only when the wallet is registered and the required identity claims are valid under the configured trusted issuers and claim topics (Lebrun et al., 2021). In the proposed extension, the registry would additionally verify the relevant zero-knowledge proof before authorizing the transfer.

This arrangement keeps sensitive identity data off-chain while allowing the smart-contract layer to enforce defined eligibility rules. It does not remove the need for legal oversight, trusted credential issuers, or appropriate governance of the compliance rules.

In the proposed design, personal identification documents, underlying KYC/AML records, and complete Verifiable Credentials remain off-chain. The credential issuer retains verification records under its applicable retention and access policies, while the investor stores the issued credential in a wallet or protected credential repository. The wallet uses the credential as a private input to proof generation; neither the complete credential nor its underlying personal attributes is submitted to the public ledger.

On-chain data comprise token balances and supply changes, wallet-to-identity associations required by the identity registry, configured issuer and claim references, compliance parameters, and transfer execution records. The proposed verification extension would submit a zero-knowledge proof and its required public inputs as transaction data. These inputs would bind the proof to the asset, amount, recipient, source and destination networks, unique transfer identifier, applicable policy version, and validity period. Where credential-status verification uses a cryptographic commitment, the relevant status root would also be available on-chain. Raw credentials and direct hashes of personal identification documents would not be published. Public transaction metadata would remain visible; the design does not claim full transaction confidentiality.

Update authority would be divided among explicitly authorized roles. Credential issuers would control issuance and revocation of their credentials.

Designated governance roles would approve changes to trusted issuers, accepted claim requirements, compliance policies, and verification parameters. Regulatory oracle networks would relay authenticated updates from approved sources rather than independently interpret law or authorize policy changes. On-chain updates would require access-controlled authorization and produce auditable records. Credential expiry and revocation would require checks at both source-side authorization and destination-side execution. Expiry verification would establish that the credential remains valid at the time of each check. Revocation verification would use an issuer-maintained status mechanism, with a current authenticated status commitment made available to the verification layer. The proof would establish eligibility against that status commitment without disclosing the underlying credential. Outdated status information, an expired credential, or a revoked credential would prevent authorization. A credential that expires or is revoked after the source burn could therefore prevent destination minting and require the defined recovery process. The status mechanism, acceptable update delay, proof-refresh procedure, and recovery controls remain implementation requirements for future validation.

5.4.2 Programmatic regulatory adaptation via decentralized oracles

A further limitation of static smart contracts is that regulatory inputs can change after deployment. Sanctions lists, eligibility requirements, and other external conditions may therefore need to be updated without redeploying the token contract. In the proposed design, an oracle layer would relay approved regulatory inputs to the compliance contracts. This is a proposed architectural function; it does not imply that CCIP independently interprets legal requirements or provides a validated regulatory-update service.

- Continuous data ingestion monitors approved regulatory or institutional data sources for relevant updates.
- State updates occur when the oracle network signs and publishes an approved change, such as an update to a sanctions or eligibility list.
- Automated rule execution allows the ERC-3643 compliance module to apply the verified update to subsequent transaction checks.

The proposed arrangement is intended to support updates to selected compliance parameters without changing the core token ledger. Its effectiveness would depend on reliable data sources, authorized update procedures, timely propagation, and consistent application of revised rules. These dependencies have not been tested in this study, and policy interpretation and source governance remain external responsibilities.

5.5 System architecture and process flow

The preceding components—cross-chain messaging, modular compliance contracts, decentralized identity, Verifiable Credentials, and zero-knowledge proofs—are combined into a single conceptual process for a compliant cross-chain RWA transfer.

5.5.1 Cross-chain compliance topology

The proposed architecture uses a layered structure that separates asset execution, identity and compliance, and interoperability. This separation is intended to reduce coupling between functions and to prevent an interoperability failure from automatically bypassing the asset's compliance checks.

The topology consists of three primary layers:

- The asset and execution layer contains the ERC-3643 token contract and maintains the token supply and asset state. Transfers remain subject to the compliance module.
- The identity and compliance layer combines the identity registry, standards-based credentials, zero-knowledge verification, and the compliance contract used to authorize state changes (Lebrun et al., 2021; W3C, 2022, 2025).
- The interoperability layer carries verified messages between networks and coordinates the proposed burn-and-mint sequence. In the conceptual model, this role is represented by CCIP-style messaging (Chainlink Labs, n.d.).

5.5.2 Closed-loop transaction lifecycle

To illustrate the process, the study considers an institutional investor transferring a tokenized U.S. Treasury claim from Ethereum, a public programmable blockchain supporting smart contracts (Wood, 2014), to Polygon PoS, an EVM-compatible sidechain for Ethereum (Polygon Labs, n.d.). The example is illustrative and does not report a completed production transfer.

The process flow operates in five distinct phases:

Phase 1: Off-chain credentialing and identity anchoring

Before on-chain interaction, the investor completes KYC/AML screening with an authorized provider. The provider issues a Verifiable Credential to the investor's wallet, which can be associated with the identity used by the ERC-3643 registry without publishing the underlying personal data on-chain (Lebrun et al., 2021; W3C, 2025).

Phase 2: Transfer initiation and ZKP generation

The investor initiates the cross-chain transfer through a decentralized application. Because the destination network may apply different eligibility conditions, the wallet generates a zero-knowledge proof asserting the required compliance attributes without disclosing the underlying personal data (Groth, 2016).

Phase 3: Source-chain validation and asset burning

The transaction is submitted to Ethereum. The ERC-3643 compliance and identity modules evaluate the transfer request, including the `isVerified()` eligibility check. If the required conditions are satisfied, the token contract burns the specified token amount on the source chain (Lebrun et al., 2021; Wood, 2014).

Phase 4: Decentralized cross-chain attestation

After the source-chain burn is finalized, the interoperability layer attests to the state change and carries the associated compliance payload to Polygon. In the proposed CCIP-style messaging model, separate oracle functions commit and execute the message while an independent risk layer monitors the transfer (Chainlink Labs, n.d.).

Phase 5: Destination settlement and dynamic rule execution

On Polygon PoS, the destination compliance module verifies the inbound message and any current eligibility conditions before authorizing the equivalent mint. Polygon PoS is EVM-compatible, so Ethereum-style smart contracts can be deployed there with network-specific configuration (Polygon Labs, n.d.).

The technical execution and cryptographic dependencies of this lifecycle are summarized in Table 5.

Table 5: Cryptographic and operational matrix of a cross-chain RWA transfer

Process phase	Primary actor or network	Operational action	Cryptographic or regulatory dependency
1. Credentialing	Off-chain KYC/AML provider	Issues a Verifiable Credential to the investor wallet.	Links verified off-chain identity evidence to a reusable digital credential (W3C, 2025).
2. Initiation	Investor wallet	Generates the compliance proof for the proposed cross-chain transfer.	Uses a zero-knowledge proof to disclose only the eligibility statement required for verification (Groth, 2016).
3. Source validation	ERC-3643 on Ethereum	Checks identity/compliance conditions and burns the specified token amount.	Depends on ERC-3643 identity and compliance functions and source-chain finality (Lebrun et al., 2021).

4. Attestation	Cross-chain messaging layer	Carries the verified token-state change and compliance payload.	Depends on cross-chain message verification, oracle/validator security, and risk controls (Chainlink Labs, n.d.).
5. Destination minting	ERC-3643 on Polygon PoS	Verifies the inbound message and authorizes the equivalent mint.	Depends on destination-side compliance checks and correctly governed mint permissions.

This conceptual process is designed to reduce fragmentation and unnecessary disclosure by combining destination-side compliance checks with cross-chain state transfer. Its effectiveness remains dependent on implementation security, governance, and the reliability of identity and oracle inputs.

6. Discussion and market implications

The proposed framework combines ERC-3643, zero-knowledge proofs, standards-based digital identity, and cross-chain messaging to address the technical and regulatory constraints identified in the preceding sections.

6.1 Secondary-market liquidity and arbitrage efficiency

A potential economic benefit of the proposed architecture is a reduction in the frictions created by fragmented token venues. Interoperability research shows that cross-chain transfers introduce additional trust assumptions, latency, and transaction costs, while financial-policy research identifies fragmented infrastructures as a constraint on the development of tokenized markets (Belchior et al., 2022; OECD, 2025; Zamyatin et al., 2021). A supply-preserving cross-chain mechanism could make it easier for market participants to move a regulated token between supported networks without creating multiple wrapped representations. The study does not establish whether this mechanism would improve spreads, market depth, or trading volume. Any liquidity benefit would also depend on investor participation, trading-venue access, transaction costs, and applicable transfer restrictions; technical connectivity alone does not establish market liquidity.

6.2 Alignment with European and global regulatory frameworks

Institutional adoption depends on compliance with applicable law regardless of the underlying technical architecture. MiCA establishes EU requirements for covered crypto-assets and service providers, while GDPR governs the processing of personal data (European Parliament & Council of the European Union, 2016, 2023). The proposed use of ERC-3643 provides programmable transfer restrictions, while off-chain credentials and zero-knowledge proofs reduce the need to publish identity data on a public ledger.

(Finck, 2019; Groth, 2016; Lebrun et al., 2021; W3C, 2025). This architecture should therefore be understood as a technical compliance mechanism, not as a substitute for legal classification, supervisory judgment, or regulated intermediaries.

For the proposed architecture, legal classification must precede configuration of the compliance rules. The applicable checks would depend on the instrument, issuer, investor, activity, and jurisdiction. A tokenized Treasury claim or fund interest should not be assumed to fall within MiCA merely because it is issued on a blockchain. MiCA is considered here only where its scope applies; ERC-3643 and privacy-preserving verification are proposed technical components, not evidence of compliance with any particular legal regime.

6.3 Considerations for institutional adoption

Existing institutional deployments provide context for considering individual elements of the proposed design. BlackRock's BUIDL fund illustrates tokenized fund issuance on a public blockchain (BlackRock, 2024), while Swift's interoperability experiments examine connections between established financial messaging infrastructure and blockchain networks (Swift, 2023). These examples do not demonstrate the feasibility of the integrated architecture proposed here. Institutional adoption would require further assessment of integration costs, operational governance, security, and applicable regulatory requirements.

- i. BlackRock and ABN AMRO: Examples of their reported tokenization activities.
- ii. Swift: Description of its reported interoperability experiments.
- iii. Polygon documentation: Network-specific characteristics and configuration.
- iv. Chainlink documentation: Descriptions of CCIP-specific components.

The proposed design therefore favors compatibility with existing operational systems rather than requiring a complete replacement of institutional back ends.

7. Challenges, risks, and limitations

The proposed architectural framework seeks to address liquidity fragmentation and privacy constraints, but its effectiveness remains unvalidated and its implementation presents technical and legal challenges. The deployment of decentralized infrastructure for institutional capital introduces novel technical vulnerabilities and profound legal complexities that must be critically addressed.

7.1 Technical vulnerabilities in cross-chain bridges

Cross-chain interoperability adds a distinct technical attack surface because security depends not only on each underlying blockchain but also on message verification, validator or oracle assumptions, smart-contract logic, and key management. Systematic studies document recurring vulnerabilities in bridge architectures and past exploits across several design classes (Notland et al., 2026; Zhang et al., 2024). The proposed burn-and-mint model reduces the custody concentration of some lock-and-mint designs, but it does not remove cross-chain security risk.

The primary technical risks include:

- Compromised keys and validator collusion can allow attackers to forge messages or approve unauthorized state transitions when a bridge depends on a limited validator set. Cross-chain security studies identify validator and key-management failures as recurring attack vectors (Zhang et al., 2024).
- Smart-contract logic flaws can arise in message verification, signature validation, replay protection, or destination-side execution. Because cross-chain protocols coordinate state across separate systems, a defect in one verification path can have effects beyond a single contract (Notland et al., 2026; Zhang et al., 2024).
- Insufficient rate limits and circuit breakers can magnify losses when an invalid cross-chain message is accepted. Defense-in-depth designs therefore use monitoring, bounded transfer capacity, and emergency controls to reduce the impact of a compromised component (Notland et al., 2026).

7.1.1 Threat model for the proposed architecture

The proposed architecture requires protection of token-supply integrity, transfer authorization, credential validity, compliance-policy integrity, personal-data confidentiality, and service availability. Its principal trust boundaries lie between the investor wallet and credential issuer, off-chain information sources and on-chain registries, source and destination blockchains, and governance authorities and operational contracts.

Potential adversaries include external attackers, malicious investors, compromised credential issuers, colluding oracle operators, and insiders controlling privileged accounts. An attacker may submit fabricated or expired credentials, compromise a wallet, replay messages, delay cross-chain delivery, manipulate regulatory inputs, or exploit weaknesses in contracts and proof-verification logic. Privileged attackers may also attempt unauthorized changes to trusted issuers, compliance rules, verification keys, or minting permissions.

The design assumes that the underlying chains satisfy their stated finality and consensus-security assumptions, cryptographic primitives remain

secure, and the required proportion of oracle operators follows the messaging protocol. Credential eligibility additionally depends on trustworthy issuance and timely status updates. A cryptographically valid proof cannot establish that an issuer's underlying assessment was truthful. The following table identifies threats, proposed controls, and residual risks; these controls have not been implemented or validated in this study.

Table 6: Threat model and proposed controls for the conceptual architecture

Threat and attack vector	Potential impact	Proposed controls	Residual risk
Forged credentials: fabricated signatures, altered attributes, or use of expired or revoked credentials	Unauthorized transfer eligibility	Verify issuer signatures, holder binding, required claims, expiry, and current credential status	Stale status information or faulty validation may permit acceptance
Compromised issuer: a trusted issuer deliberately or accidentally issues false claims	Ineligible investors receive apparently valid credentials	Govern issuer admission; monitor issuance; support issuer removal, key rotation, and credential revocation	Valid signatures do not establish the truth of issued claims
Oracle collusion or manipulation: operators relay false, incomplete, or outdated information	Incorrect compliance updates or cross-chain authorization	Authenticated sources, threshold-based verification, independent monitoring, and freshness checks	Correlated compromise or manipulation of an authoritative source can defeat these controls
Replay attacks: reuse of a proof, message, or transfer identifier	Duplicate minting or execution in an unintended context	Bind proofs and messages to the asset, amount, recipient, chain identifiers, policy version, and unique transfer identifier; record consumed identifiers	Incorrect binding or inconsistent replay records may leave exploitable paths
Bridge or messaging failure: forged attestations, delivery interruption, or premature acceptance of source finality	Unauthorized minting or assets remaining unavailable after burning	Finality checks, authenticated messaging, rate limits, risk-management gates, and controlled retry procedures	A prolonged outage may prevent settlement; recovery must prevent both source restoration and destination minting
Governance-key compromise: misuse of administrative, upgrade, or minting privileges	Unauthorized policy changes, freezes, transfers, or token creation	Separate roles, multiple approvals, protected key storage, privilege limits, and auditable changes	Compromise or collusion among sufficient authorized parties remains possible

Wallet compromise: stolen signing keys or malicious proof-generation software	Unauthorized requests, credential exposure, or diversion of assets	Secure credential storage, transaction-detail confirmation, protected signing, and controlled recovery	User-device compromise can defeat local protections
Privacy leakage: correlation of addresses, public inputs, status queries, or transaction metadata	Disclosure of investor relationships or sensitive activity	Minimize public inputs, retain personal records off-chain, and assess metadata and credential-status linkability	Zero-knowledge eligibility proofs do not conceal all public transaction activity
ZKP implementation flaws: under-constrained circuits, incorrect verification keys, or defective verifier integration	Acceptance of invalid eligibility claims or unintended disclosure	Circuit and verifier review, adversarial test cases, version-controlled verification keys, and secure setup procedures where required	Undetected implementation errors or compromised setup assumptions can invalidate security guarantees
Contract or registry compromise: unauthorized registry changes, access-control defects, or inconsistent policy state	Bypassed eligibility checks or unauthorized token operations	Restrict registry writes, review contract permissions, test state transitions, and check policy versions before execution	Contract defects and inconsistent updates across chains remain risks

7.2 Legal enforceability of algorithmic compliance

A second challenge lies at the intersection of deterministic smart-contract execution and legal systems that allow remedies, interpretation, and institutional discretion.

Algorithmic compliance can enforce predefined technical rules, but it cannot resolve every legal question or factual dispute. Smart-contract execution therefore remains dependent on governance, legally authorized intervention, and external sources of truth (Savelyev, 2017; Werbach & Cornell, 2017).

- The reversibility problem arises when law requires a result that differs from the immutable transaction history, for example after fraud, loss of a private key, or a court-ordered seizure. ERC-3643 includes controlled recovery, freeze, and forced-transfer functions, which can support such interventions but also introduce governance and key-management responsibilities (Lebrun et al., 2021; Werbach & Cornell, 2017).

- Doctrinal clashes arise because traditional contract law considers context, remedies, mistake, good faith, and other factors that deterministic code does not evaluate on its own. Incorrect oracle data or ambiguous external events can therefore create disputes that require legal interpretation beyond the smart contract (Savelyev, 2017; Werbach & Cornell, 2017).
- Jurisdictional ambiguity remains when a cross-chain transaction involves participants, infrastructure, and assets connected to several legal systems. Determining governing law, supervisory responsibility, and the appropriate forum for disputes remains a legal and policy issue beyond the scope of protocol-level compliance checks (OECD, 2025).

The proposed architecture would require a documented intervention policy linking legally authorized decisions to specific technical controls. A designated operator or governance body would authenticate instructions, determine their applicability to the asset and relevant participants, and authorize action through access-controlled procedures. Sensitive supporting documents would remain off-chain, while intervention identifiers, approvals, and resulting state changes would be recorded for audit. High-impact actions would require approval by more than one authorized person.

Court orders would undergo review of authenticity, scope, jurisdiction, and the authority of the issuing body before execution. Where legally applicable, authorized token agents could use freeze, recovery, or forced-transfer functions supported by ERC-3643 (Lebrun et al., 2021). Such actions would create subsequent state changes rather than erase the original transaction history. Cross-chain coordination would also be necessary to prevent a pending transfer from bypassing the intervention.

Sanctions updates would originate from approved authoritative sources and enter the compliance layer through controlled update procedures. The responsible compliance function would determine the applicable restriction and its effective time; the oracle network would transmit the approved update. Checks would apply before source burning and destination minting. Where an update requires restrictions on existing holdings, an authorized operator would initiate the relevant freeze procedure rather than assume that an oracle update automatically freezes assets.

Mistaken transfers would require a documented claim and review of transaction records, ownership evidence, and the applicable legal or contractual basis for correction. A reported mistake would not automatically authorize reversal. Where correction is permitted, an authorized recovery or forced transfer could be considered. For a transfer already burned on the source chain but not minted on the destination chain, recovery would require a coordinated process that prevents both destination minting and source restoration from occurring for the same transfer.

Frozen assets would remain recorded in the token ledger but would be subject to the configured restrictions. The intervention policy would specify whether a restriction applies to particular balances, an address, or broader token operations. Release would require authorized review confirming that the restriction has expired, been withdrawn, or otherwise ceased to apply. Restrictions affecting a cross-chain transfer would need to be recognized by both participating deployments.

Lost-key recovery would require renewed identity verification and evidence linking the claimant to the affected holdings. Where recovery is authorized, the operator could invoke the token's recovery mechanism to associate the holdings with a replacement wallet, while updating the relevant identity records and preventing further use of the compromised or superseded address. This process would remain subject to applicable law and the issuer's documented recovery policy.

Conflicting jurisdictional requirements would be escalated for legal assessment rather than resolved automatically by an oracle or smart contract. The assessment would consider the asset's legal structure, governing documents, relevant parties, and applicable mandatory rules. Where no lawful execution path can be established, the proposed system would withhold the affected transfer pending resolution. A conflict arising after source burning would enter the controlled recovery process. These procedures define governance requirements for the conceptual architecture; they do not establish that an intervention would be legally recognized in every jurisdiction.

7.3 Limitations of the current study

Several limitations should be acknowledged. First, the proposed synthesis of ERC-3643, zero-knowledge proofs, standards-based credentials, and CCIP-style messaging is a conceptual design that has not been empirically validated as an integrated production system. The evaluation is primarily qualitative and architectural; Section 3.4 provides a benchmarking protocol rather than measured performance results. Second, the framework assumes that trusted institutions can issue and govern interoperable digital credentials at scale, an assumption that is not yet uniformly realized across financial markets. Third, the analysis focuses mainly on European regulatory requirements and selected international examples; its applicability to other legal systems requires jurisdiction-specific evaluation.

8. Conclusion and future directions

8.1 Summary of key findings

This study identifies network fragmentation, transfer restrictions, and privacy requirements as interconnected challenges in RWA tokenization. It proposes a conceptual architecture combining ERC-3643 token controls,

decentralized identity, off-chain Verifiable Credentials, zero-knowledge proofs, and cross-chain messaging. The design separates asset execution from identity and compliance functions and outlines a cross-chain transfer process with destination-side eligibility checks. The contribution is an architectural synthesis rather than evidence of an effective operational system. The analysis provides a basis for investigating how these components could be integrated, but it does not demonstrate reduced liquidity fragmentation, improved performance, successful institutional adoption, or regulatory acceptance. These outcomes remain dependent on implementation, security testing, empirical evaluation, and jurisdiction-specific legal assessment.

8.2 Recommendations for policymakers and protocol developers

Scaling tokenized financial markets will require coordination between regulators, financial institutions, standards bodies, and protocol developers.

For policymakers

- Recognition of cryptographic privacy mechanisms should be considered where regulators can verify that privacy-preserving proofs satisfy the substantive requirements of KYC/AML and data-protection law. Such recognition would still require governance of credential issuers, proof systems, and auditability.
- Cross-border taxonomies and recognition mechanisms should be made more consistent where legally possible. Common definitions and reciprocal recognition of compliant digital-identity evidence could reduce duplicate verification while preserving jurisdiction-specific investor-protection rules.

For protocol developers

- Developers should evaluate transfer models against asset-specific custody, supply-control, security, and recovery requirements. Burn-and-mint is the approach examined in this conceptual design, but its suitability depends on governed mint-and-burn permissions, reliable cross-chain attestations, and procedures for failed or delayed transfers. The study does not establish its superiority over alternative models.
- Enterprise abstraction should allow institutions to access cross-chain functions through established APIs and financial messaging standards, reducing the need to replace existing operational systems.

8.3 Avenues for future research

The proposed architecture offers a conceptual approach to interoperability and compliance challenges, but its practical effectiveness and legal acceptability remain unverified.

Future research should prioritize the following domains:

- Algorithmic dispute resolution and reversibility require further research on how legally authorized recovery or override mechanisms can be implemented without creating unacceptable concentrations of technical control.
- AI-assisted decentralized oracles could be studied as tools for classifying or monitoring regulatory updates, but any automated change to compliance rules would require verifiable data provenance, human oversight, and clear accountability.
- Empirical latency and cost analysis should measure gas consumption, proof-generation overhead, cross-chain execution time, and failure behavior under reproducible test conditions before production claims are made.

Privacy-preserving identity, standards-based credentials, and cross-chain messaging provide a plausible direction for further architectural research. Establishing the value of their integration requires a working implementation, performance and security evaluation, and assessment under applicable legal requirements. The framework should therefore be understood as a proposal for investigation, not as a demonstrated solution to RWA market fragmentation or evidence of regulatory acceptance.

Conflict of Interest: The author reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The author did not obtain any funding for this research.

References:

1. ABN AMRO. (2023, January 10). ABN AMRO Registers First Digital Bond on Public Blockchain. ABN AMRO.
2. Aldasoro, I., Doerr, S., Gambacorta, L., Garratt, R., and Koo Wilkens, P. (2023). The Tokenisation Continuum. BIS Bulletin No. 72. Bank for International Settlements.
3. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., and Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. Proceedings of the 13th EuroSys Conference, Article 30, 1-15.

4. Belchior, R., Vasconcelos, A., Guerreiro, S., and Correia, M. (2022). A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Computing Surveys*, 54 (8), Article 168.
5. BlackRock. (2024, March 20). BlackRock Launches Its First Tokenized Fund, BUIDL, on the Ethereum Network. *Business Wire*.
6. Chainlink Labs. (n.d.). Chainlink Cross-Chain Interoperability Protocol (CCIP) Documentation.
7. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., and Juels, A. (2020). Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. *2020 IEEE Symposium on Security and Privacy*, 910-927.
8. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1-88.
9. European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/1114 of 31 May 2023 on Markets in Crypto-Assets. *Official Journal of the European Union*, L 150, 40-205.
10. European Parliament and Council of the European Union. (2024). Directive (EU) 2024/1640 of 31 May 2024 on Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing. *Official Journal of the European Union*.
11. Finck, M. (2019). Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law? *European Parliamentary Research Service*.
12. Goldwasser, S., Micali, S., and Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 18 (1), 186-208.
13. Groth, J. (2016). On the Size of Pairing-Based Non-Interactive Arguments. In Fischlin, M., and Coron, J.-S. (Eds.), *Advances in Cryptology – EUROCRYPT 2016, Lecture Notes in Computer Science*, 9666, 305-326. Springer.
14. Kotey, S.D., Tchao, E.T., Ahmed, A.-R., Agbemenu, A.S., Nunoo-Mensah, H., Sikora, A., Welte, D., and Keelson, E. (2023). Blockchain Interoperability: The State of Heterogeneous Blockchain-to-Blockchain Communication. *IET Communications*, 17, 891-914.
15. Lebrun, J., Malghem, T., Thizy, K., Falempin, L., and Boudjemaa, A. (2021). ERC-3643: T-REX—Token for Regulated Exchanges. *Ethereum Improvement Proposal No. 3643. Ethereum Improvement Proposals*.

16. Notland, J.S., Li, J., Nowostawski, M., and Haro, P.H. (2026). SoK: Cross-Chain Bridging Architectural Design Flaws and Mitigations. *Blockchain: Research and Applications*, 7 (1), 100315.
17. OECD. (2025). Tokenisation of Assets and Distributed Ledger Technologies in Financial Markets: Potential Impediments to Market Development and Policy Implications. OECD Business and Finance Policy Papers No. 75. OECD Publishing.
18. Polygon Labs. (n.d.). Polygon PoS Overview.
19. Savelyev, A. (2017). Contract Law 2.0: ‘Smart’ Contracts as the Beginning of the End of Classic Contract Law. *Information & Communications Technology Law*, 26 (2), 116-134.
20. Swift. (2023). Connecting Blockchains: Overcoming Fragmentation in Tokenised Assets—Swift's Interoperability Experiments Connecting to Public and Private Blockchain Networks. Swift.
21. Vogelsteller, F., and Buterin, V. (2015). ERC-20: Token Standard. Ethereum Improvement Proposal No. 20. Ethereum Improvement Proposals.
22. Werbach, K., and Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, 67 (2), 313-382.
23. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper. Ethereum.
24. World Wide Web Consortium. (2022, July 19). Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations. W3C Recommendation.
25. World Wide Web Consortium. (2025, May 15). Verifiable Credentials Data Model v2.0. W3C Recommendation.
26. Zamyatin, A., Al-Bassam, M., Zindros, D., Kokoris-Kogias, E., Moreno-Sanchez, P., Kiayias, A., and Knottenbelt, W.J. (2021). SoK: Communication Across Distributed Ledgers. In Borisov, N., and Diaz, C. (Eds.), *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, 12675, 3-36. Springer.
27. Zhang, M., Zhang, X., Barbee, J., Zhang, Y., and Lin, Z. (2024). Security of Cross-Chain Bridges: Attack Surfaces, Defenses, and Open Problems. *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2024)*, 298-316.
28. European Securities and Markets Authority (ESMA). (2025, March 19). Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments (ESMA75453128700-1323)