LIQUID BRIDGE

Compliant Cross-Chain Securities Transfer
with MPC Threshold Custody

Zach Kelling

Satschel, Inc.

Version 1.0 — April 2026

Contents

1 Abstract **3**

2 Introduction **3**

3 Architecture **3**
3.1 Protocol Layers 3
3.2 Compliance Gate 3

4 MPC Custody for Bridge Keys **4**

5 Warp Messaging **4**

6 Supported Chains **4**

7 ERC-3643 Compliance Preservation **4**

8 Security Model **5**

9 Conclusion **5**

Abstract

We present Liquid Bridge, a compliant cross-chain securities transfer protocol for the Liquidity Network. Unlike token bridges that move fungible assets between chains, Liquid Bridge transfers **regulated securities** subject to transfer restrictions, KYC/AML requirements, and jurisdictional compliance. The bridge uses CGGMP21 threshold ECDSA [7] for custody — no single key holder can authorize a transfer. Warp messaging with Ringtail post-quantum signatures [3] ensures message authenticity survives quantum adversaries. All cross-chain transfers enforce ERC-3643 compliance on both source and destination chains, with on-chain proof that the recipient passes accreditation, jurisdiction, and lockup requirements before settlement.

Introduction

Traditional token bridges (Wormhole, LayerZero, Axelar) were designed for fungible assets with no transfer restrictions. Moving a regulated security cross-chain requires:

1. Verifying the sender is authorized to transfer (not locked, not restricted)
2. Verifying the recipient passes KYC/AML on the destination chain
3. Verifying jurisdictional compatibility (Reg D, Reg S, Rule 144)
4. Atomically burning on source and minting on destination
5. Preserving the full compliance history across chains
6. Ensuring custody keys are threshold-managed (MPC, not single-key)

Liquid Bridge solves all six requirements using the Lux cross-chain research stack [1, 2].

Architecture

Protocol Layers

```
User (sends transfer request)
  -> Compliance Gate (KYC/AML/accreditation check on BOTH chains)
  -> Bridge Contract (source chain: lock or burn)
  -> Warp Messenger (PQ-signed cross-chain message)
  -> MPC Custody (CGGMP21 2-of-3 threshold authorization)
  -> Bridge Contract (dest chain: mint or unlock)
  -> Compliance Gate (verify recipient eligibility)
  -> Settlement (T+0 on destination)
```

Compliance Gate

Every cross-chain transfer passes through a compliance gate on both chains:

Check	Source Chain	Destination Chain
KYC verified	Sender must be KYC'd	Recipient must be KYC'd
AML screening	Sender not on sanctions list	Recipient not on sanctions list
Accreditation	Sender holds valid accreditation	Recipient holds valid accreditation
Jurisdiction	Sender jurisdiction allows transfer	Recipient jurisdiction allows receipt
Lockup	Security not in lockup period	N/A

Transfer limit	Daily/monthly limits respected	N/A

If any check fails, the transfer reverts atomically — no partial state.

MPC Custody for Bridge Keys

Bridge custody uses CGGMP21 [7] threshold ECDSA with 2-of-3 shards:

1. **Bridge Operator**: Automated shard, rate-limited, policy-enforced
2. **Compliance Validator**: Signs only after compliance checks pass
3. **HSM Escrow**: Emergency recovery shard held by third-party custodian

No single party can authorize a bridge transfer. The compliance validator independently verifies KYC/AML status before co-signing.

Warp Messaging

Cross-chain messages are signed using Ringtail lattice-based threshold signatures [4], providing post-quantum security. Each message contains:

- Source chain ID, destination chain ID
- Security token address (ERC-3643 compliant)
- Sender address, recipient address
- Amount, compliance proof hash
- BLS aggregate signature (classical) + Ringtail signature (post-quantum)

The dual-signature (classical + PQ) ensures security against both current and future quantum adversaries [5].

Supported Chains

Chain	**Chain ID**	**Bridge Type**	**Status**
Liquidity Network	8675309	Native (home chain)	Production
Ethereum	1	Lock/Unlock (ERC-3643)	Production
Polygon	137	Lock/Unlock (ERC-3643)	Production
Arbitrum	42161	Lock/Unlock (ERC-3643)	Production
Zoo Network	200200	Burn/Mint (native Warp)	Planned

ERC-3643 Compliance Preservation

The bridge preserves full ERC-3643 (T-REX) compliance metadata across chains:

- Identity Registry: recipient must be registered on destination chain
- Compliance Module: transfer restrictions enforced on both sides
- Claim Topics: KYC, accreditation, jurisdiction claims transferred
- Lockup Schedules: Rule 144 lockups preserved across chains

Security Model

Threat	Mitigation
Bridge key compromise	2-of-3 MPC threshold (no single key)
Quantum attack on signatures	Ringtail PQ signatures on all messages
Compliance bypass	Independent compliance validator co-signs
Double-spend	Atomic burn/mint with finality confirmation
Censorship	Multiple bridge operators, decentralized relayers
Front-running	Encrypted order flow via FHE [6]

Conclusion

Liquid Bridge is the first cross-chain protocol designed for regulated securities. By combining MPC threshold custody, post-quantum Warp messaging, and ERC-3643 compliance preservation, it enables institutional securities to move between chains while maintaining full regulatory compliance. The bridge inherits its security model from the Lux Network's cross-chain research stack and adapts it for the specific requirements of SEC/FINRA-regulated digital securities.

References

[1] Z. Kelling, "Lux Bridge: Threshold-Secured Cross-Chain Communication," Lux Industries, 2023.

[2] Z. Kelling, "Teleport Protocol: Trustless Cross-Chain Asset Transfer," Lux Industries, 2022.

[3] Z. Kelling, "Lux Warp Messaging: Cross-Appchain Communication with BLS," Lux Industries, 2023.

[4] Z. Kelling, "Ringtail: Lattice-Based Post-Quantum Threshold Signatures," Lux Industries, 2024.

[5] Z. Kelling, "Post-Quantum Cryptographic Suite for EVM," Lux Industries, 2024.

[6] Z. Kelling, "Torus Threshold Fully Homomorphic Encryption," Lux Industries, 2025.

[7] R. Canetti et al., "UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts," ACM CCS, 2020.

[8] Tokeny, "ERC-3643: T-REX Token for Regulated Exchanges," Ethereum, 2021.