Verifiable Privacy:

Proving Without Revealing for Financial Market Infrastructure

Declan Fox – VP, Consensys

LFDT Privacy for Financial Services, 1 July 2026

We are Architects of the Ethereum Ecosystem

Creators of Foundational Ethereum Technology

Across each layer of the stack

Infura
RPC Infrastructure

Besu
Enterprise Client

Linea/Lineth
zkEVM Prover

MetaMask
Non-Custodial Wallet

Market Leaders

Technology powering 8/10 of the largest public blockchains and nearly all enterprise private blockchains

Interacting with over 50% of all digital asset transactions worldwide.

Enterprise DNA

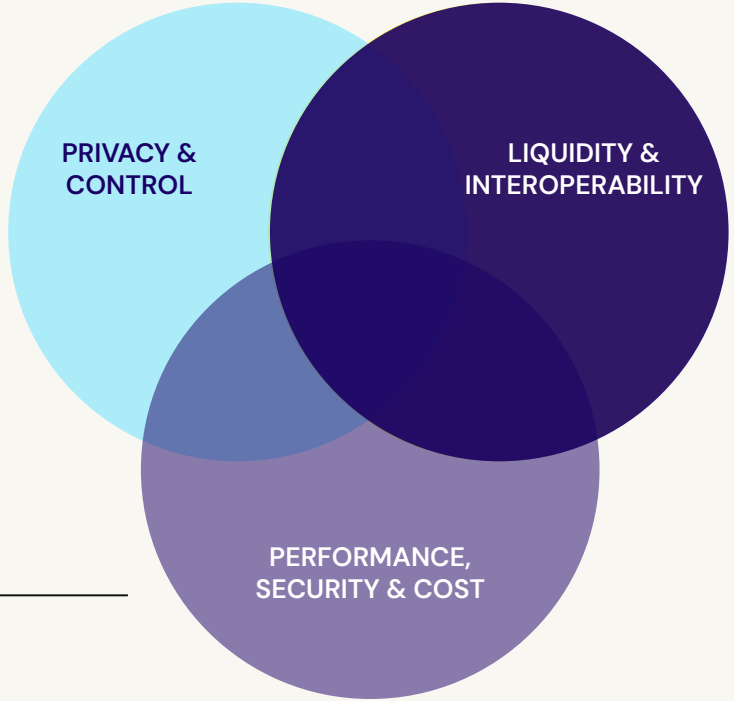
Vast institutional track record working with:

JPMorgan, Societe Generale, Enterprise Ethereum Alliance, SWIFT, VISA, mastercard, DTCC, UBS, Federal Reserve Bank of New York, Santander, Bank of England, citi, JPX, BNP Paribas, BNY, Hong Kong Monetary Authority 香港金融管理局, Banco Central do Brasil

consensys

Solving the Institutional Blockchain Trilemma

Dedicated chains without native interoperability become new siloes, failing to build network effects and tap into blockchain composability strength



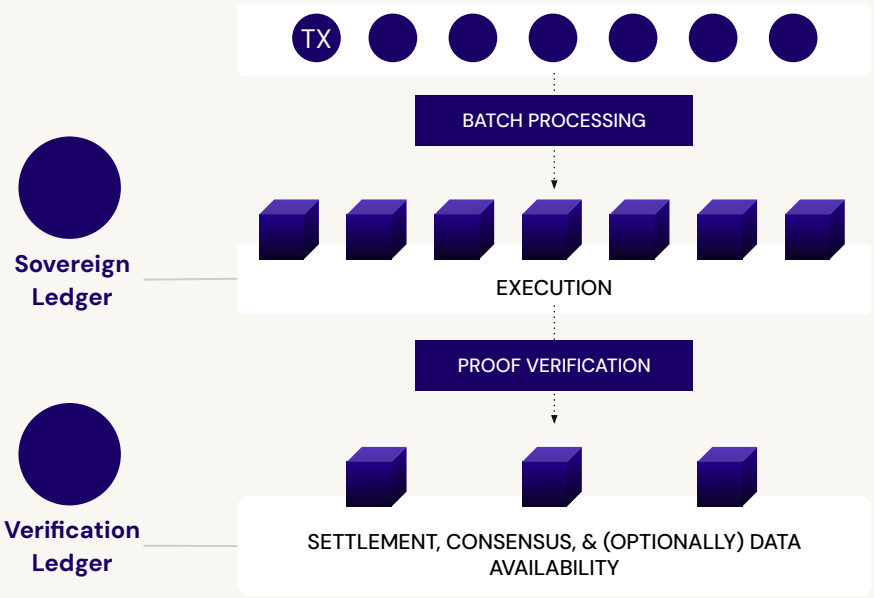
Public chains lack customizability, compliance and privacy features required to meet Institutions needs

Custom L1s lead to technical fragmentation, lower security guarantees and higher maintenance costs

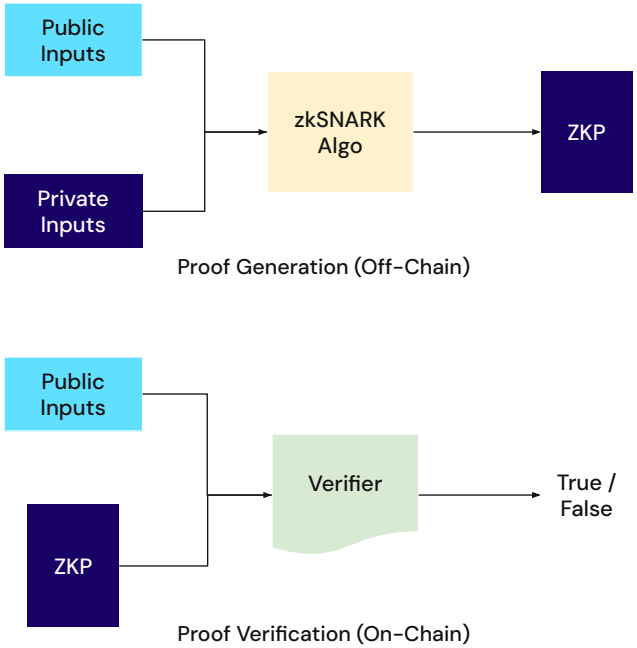
Solution: Zero-Knowledge Proofs

Zero-Knowledge enabled Sovereign Ledger executes transactions and generates cryptographic proofs of correctness. These proofs are verified on a common Verification Ledger, for a single canonical truth.

The proof crosses the boundary; the data never does.



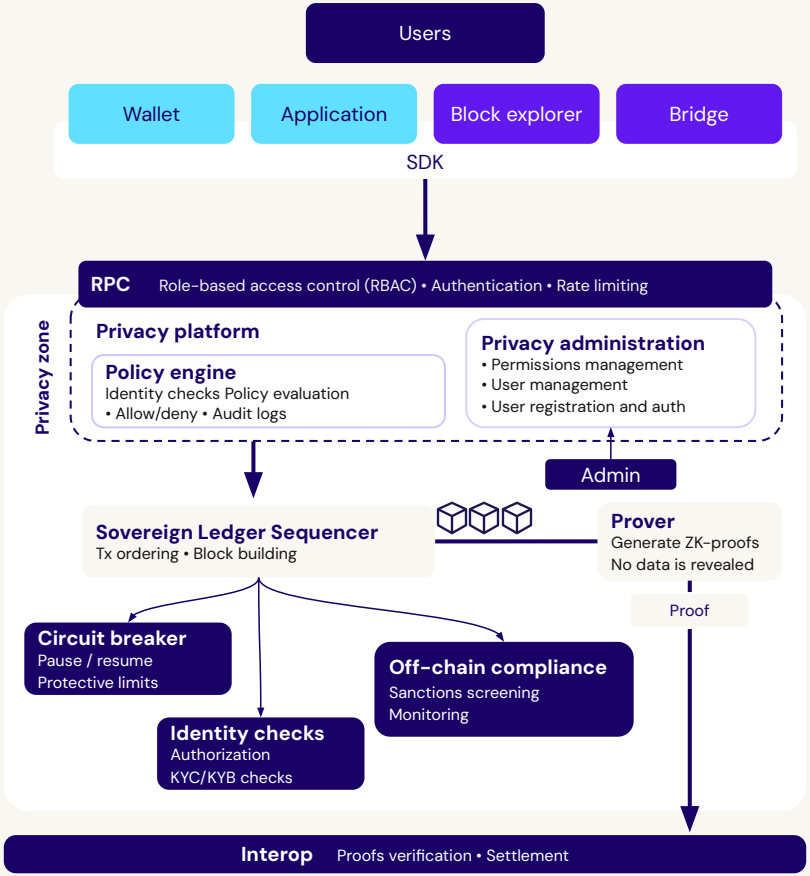
ZK proofs have properties of succinctness and privacy



RBAC with a operator-privacy model

A configuration of Lineth that ensures the state remains private. Lineth's proof mechanism guarantees proper execution while no data is revealed publicly.

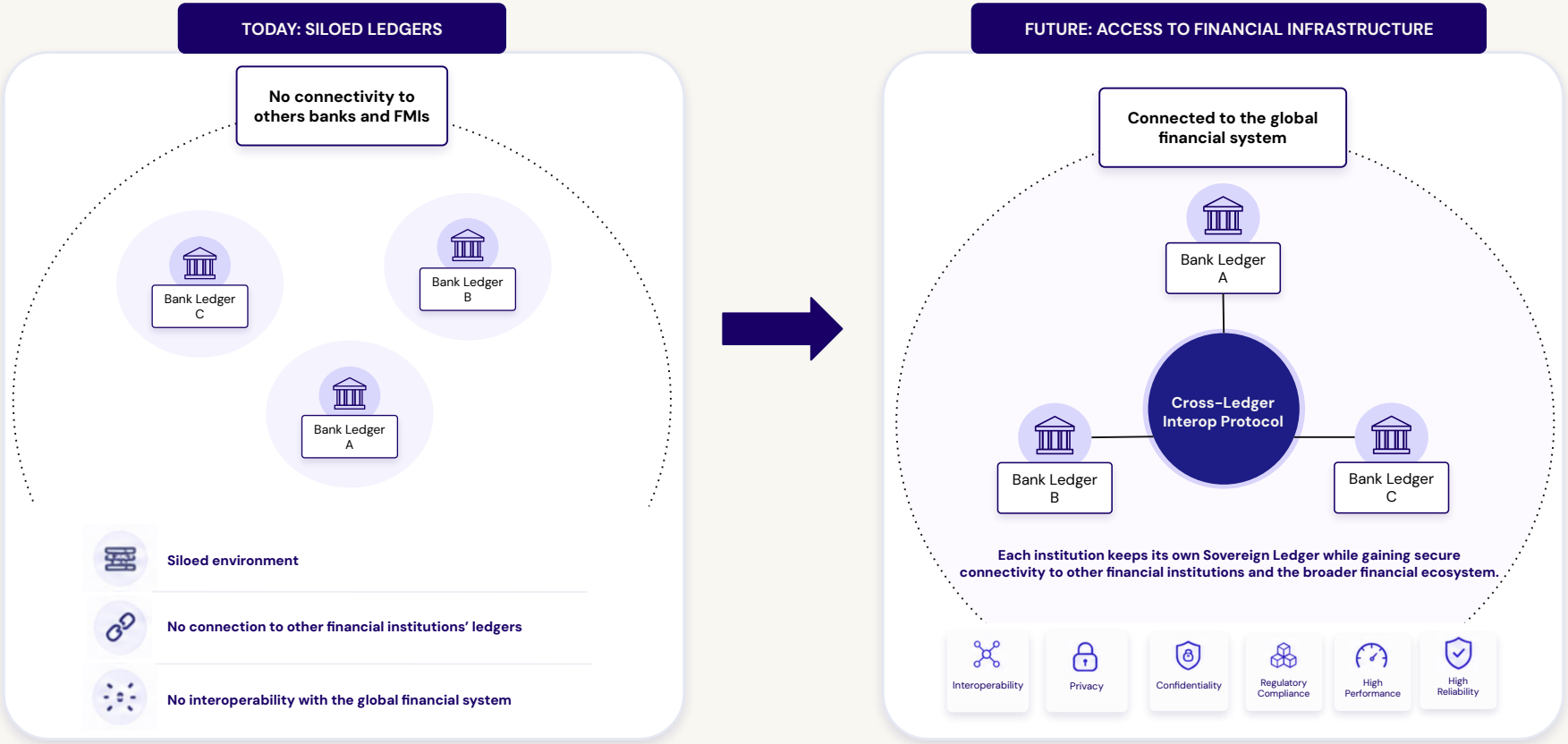
- **Global access policy**, applied across every access path with systematic logging, ensuring consistent enforcement and auditability
- **EVM-native authorization model**: define highly expressive permissions around contracts, functions and events that adapt to any smart contract and EVM tooling
- **Enterprise-ready identity support:** integrate with SSO, link wallets to identities, and support both users and machine access
- **Fine-grained, least-privilege rules** to match real workflows while preventing common misuse



consensys

From Siloed Ledgers to Connected

Consensys has built technology to enable interoperability, privacy, and enterprise-grade reliability across institutions.



consensys

Verifiable Privacy in ZK Systems

What stays private

State

- Account balances
- Transaction details
- Contract storage
- Counterparty identities

What becomes shared

Root hash
Merkle root of the state

Proofs
ZK-proofs of correct execution

Data commitments
Hashes binding to private block data

What can be verified

Inclusion
X is part of the state
Eg: Bob has escrowed 100€ for Alice.

Non-inclusion
Y is not part of the state
Eg: Alice is not sanctioned.

Public commitments make private state verifiable, without revealing it

RISC-V zkVM: Verifiable Computation

Execution becomes a mathematical statement any counterparty can verify, without re-running it.

FROM RISC-V EXECUTION TO A VERIFIABLE PROOF

Execution client
Standard Ethereum client, compiled to a RISC-V binary

Traces
Execution recorded as matrices of machine state

The traces
The evidence. Matrices recording every value the machine touched during execution, checked against the constraints.

Arithmetization
zkC constraints bind the traces

The statement behind every proof:
a system of mathematical equations that captures the correct execution of a virtual machine

The constraints
The rules. Every operation the VM can performa, translated into equations that any valid execution must satisfy.

If the equations hold, executions was correct
Verification replaces re-execution between counterparties.

Prover
Lattice-based, chunked and parallelized



Proof
Compact, post-quantum, verifiable by any party

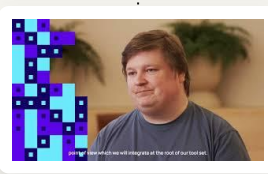


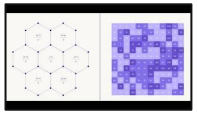
Post-quantum by construction

Lattice-based cryptography, 128-bit security. Security lives in the proving system independent of the statement being proven. It carries over unchanged from the zkEVM to RISC-V, and forward to whatever comes next.

Formally verifiable

Precompiles, hash functions and the VM are all written in zkC, with formal verification as a first-class citizen from day one, auditable as a whole system.



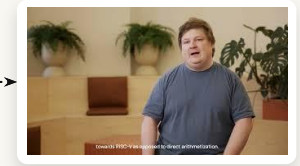


Olivier Begassat
→ Team Lead Arithmetization at Consensys
→ PhD in algebraic Topology
→ Owns the mathematical statement behind the proof: constraints, traces, and RISC-V semantics.

FROM zkEVM TO RISC-V zkVM

2021 - 2025 - zkEVM
Proving the EVM directly
Four years, a 1,000+ page spec.
Unique in the ecosystem.

2026 - RISC-V zkVM
Proving a compiled client
Semantics come from battle-tested client

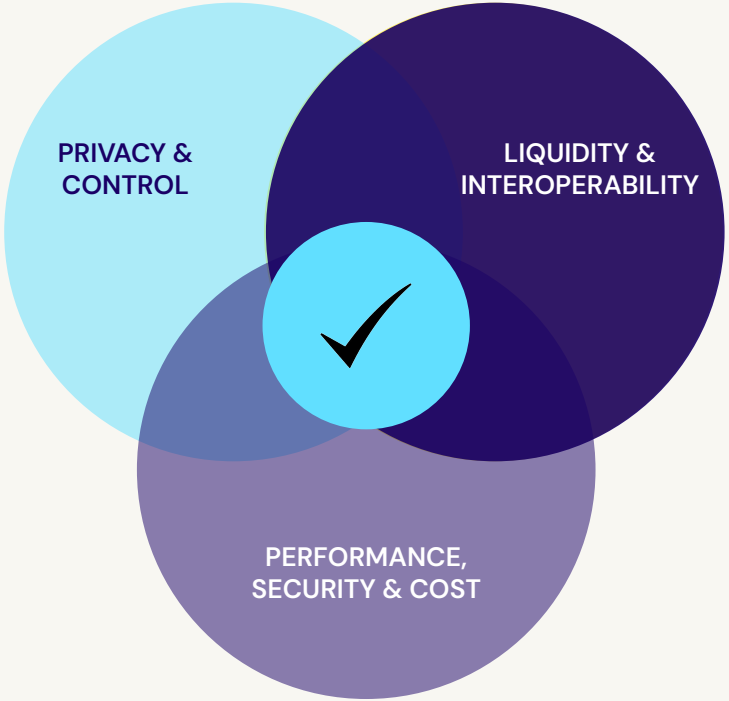


Simpler
Registers, RAM, bytecode

A simpler machine
a faster upgrade path

Faster
Upgrade the client, recompile

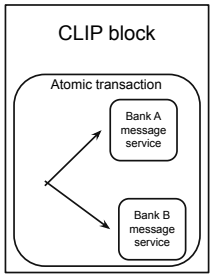
Solving the Institutional Blockchain Trilemma



Key properties of native interoperability

Guaranteed Atomicity

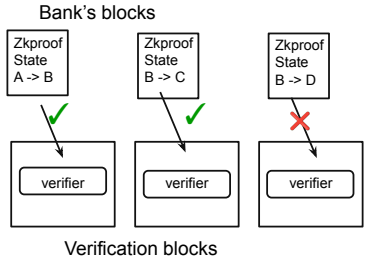
Ensures all-or-nothing execution, eliminating partial or failed state risks.



A single transaction on the CLIP atomically triggers execution on participant DLTs.

Strong Non-Repudiation

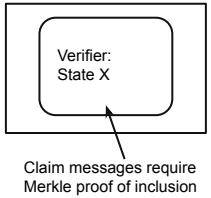
Commitments are enforced by the protocol directly at the node level.



A DLT that has committed a state "C" must built over this state, otherwise the network will reject further operations.

No bridge risk

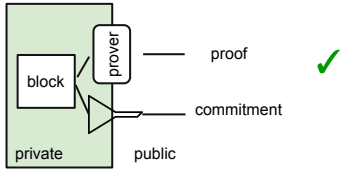
Relies on mathematical proofs rather than centralized verifier committees.



One must provide mathematical evidence that a transactions are part of the shared state to execute it

Privacy

All data remains private to the parties involved. No data is available publicly.

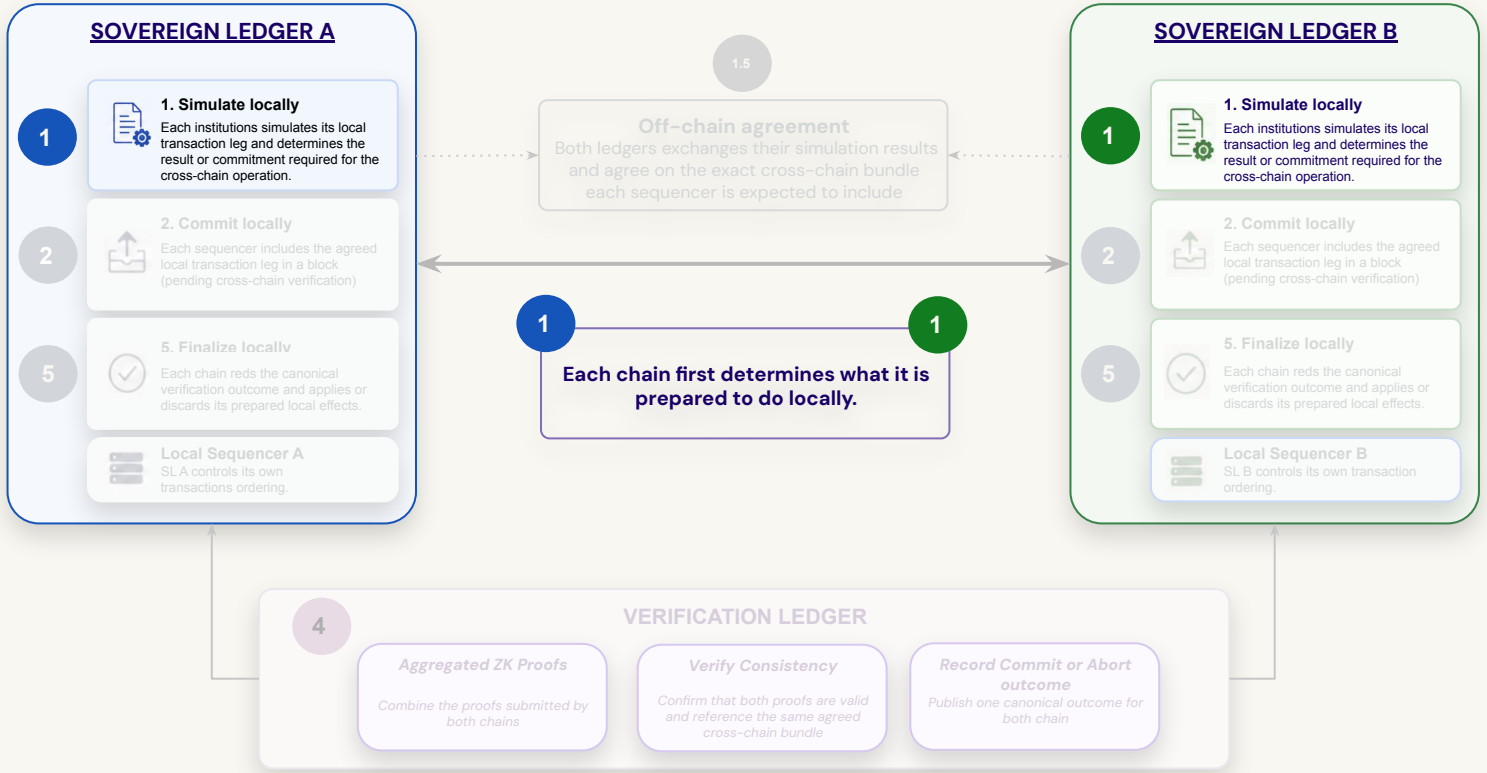


Zero-knowledge proofs don't leak any data while ensuring validity of interoperability operations

If interoperability does not reduce reconciliation and counterparty trust, it is not solving the problem.

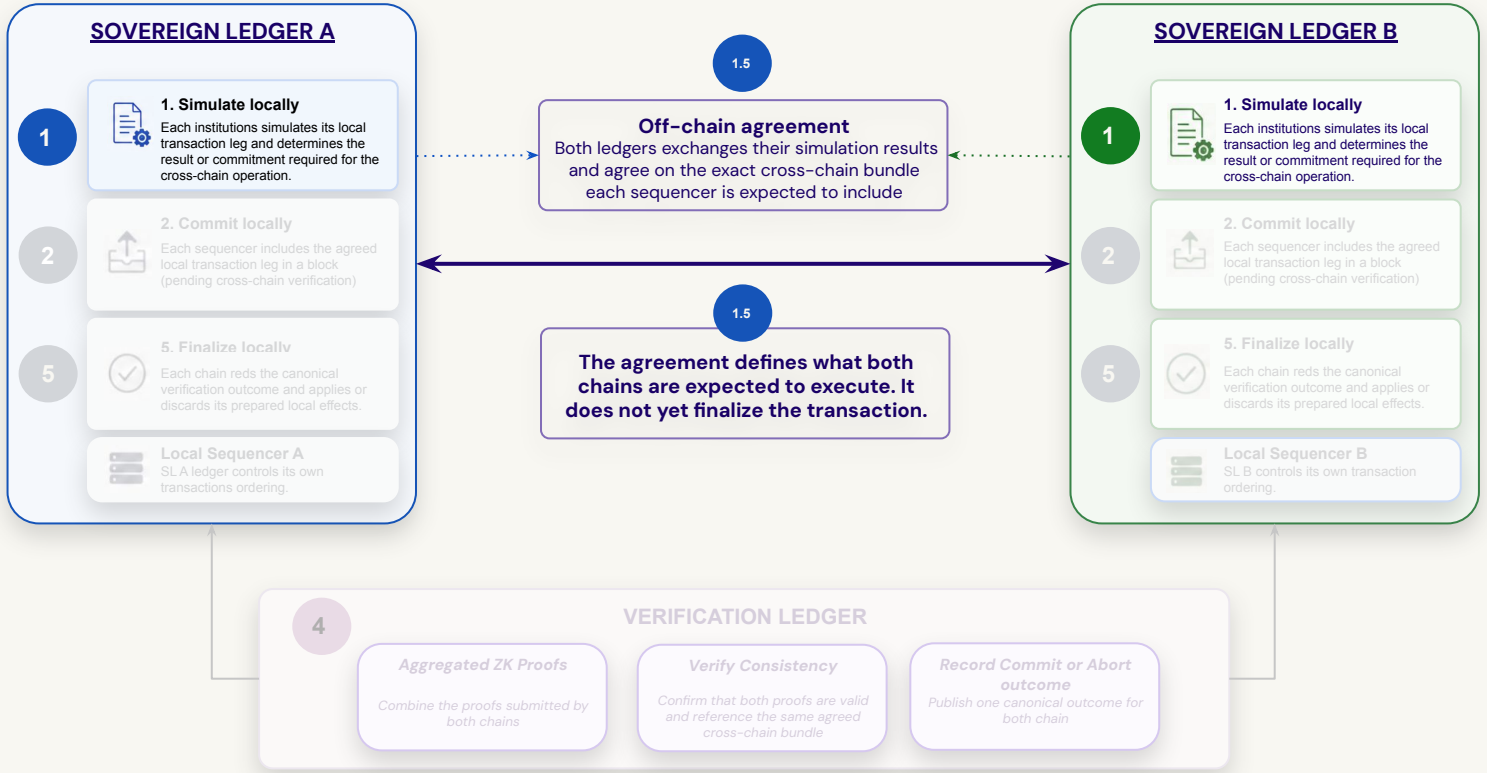
Interoperability across sovereign ledgers

Step 1 – Simulate locally



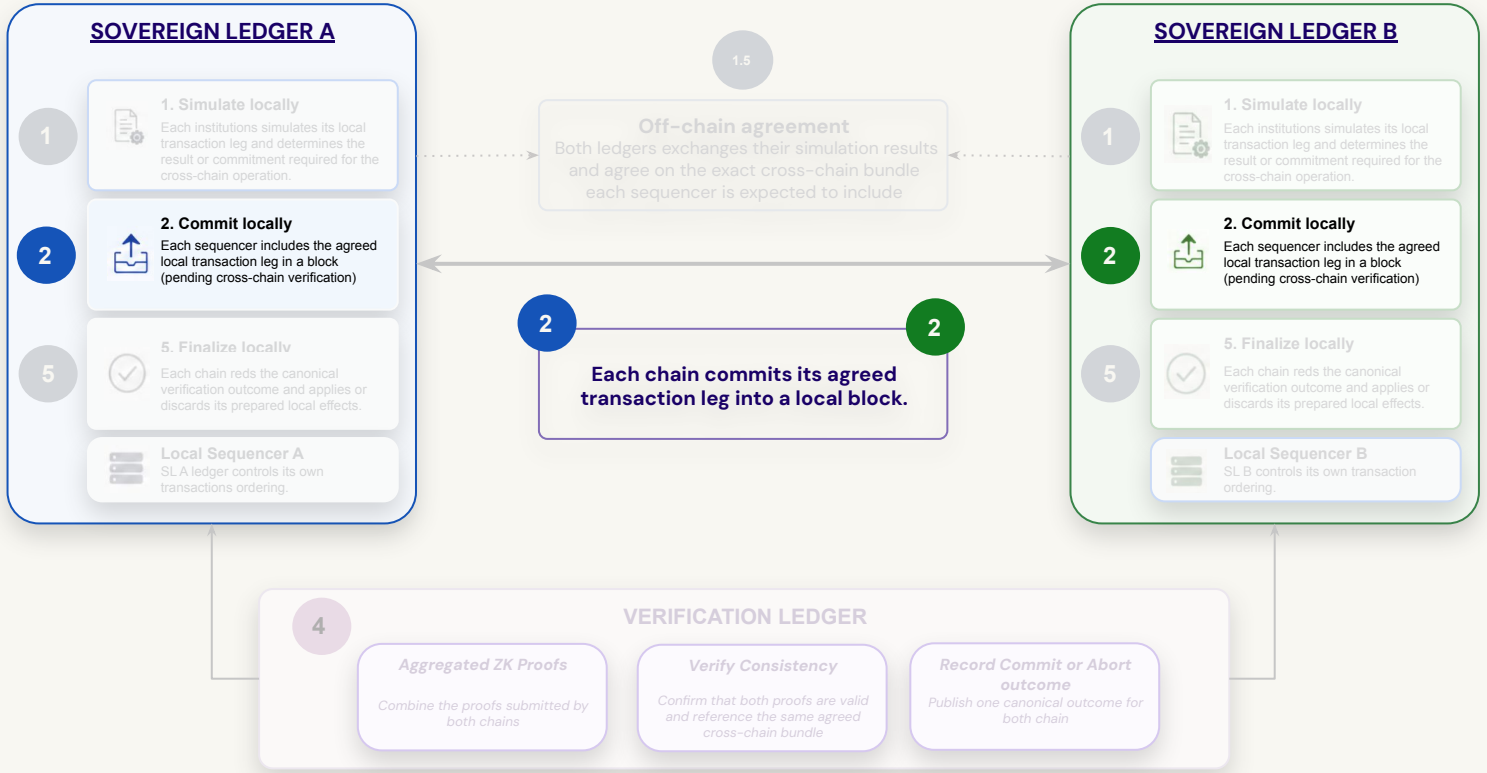
Interoperability across sovereign ledgers

Step 1.5 – Reach an off-chain agreement



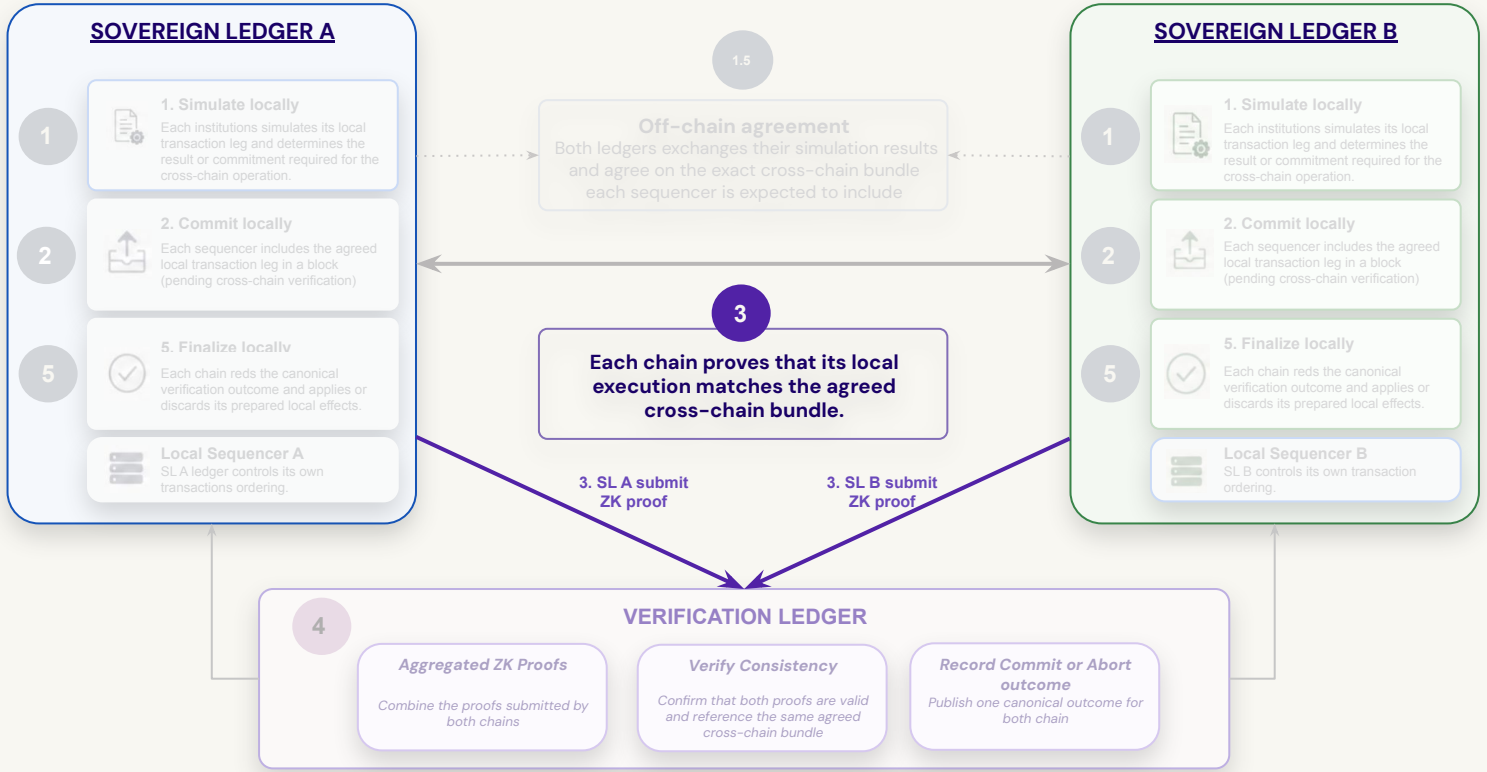
Interoperability across sovereign ledgers

Step 2 – Commit locally



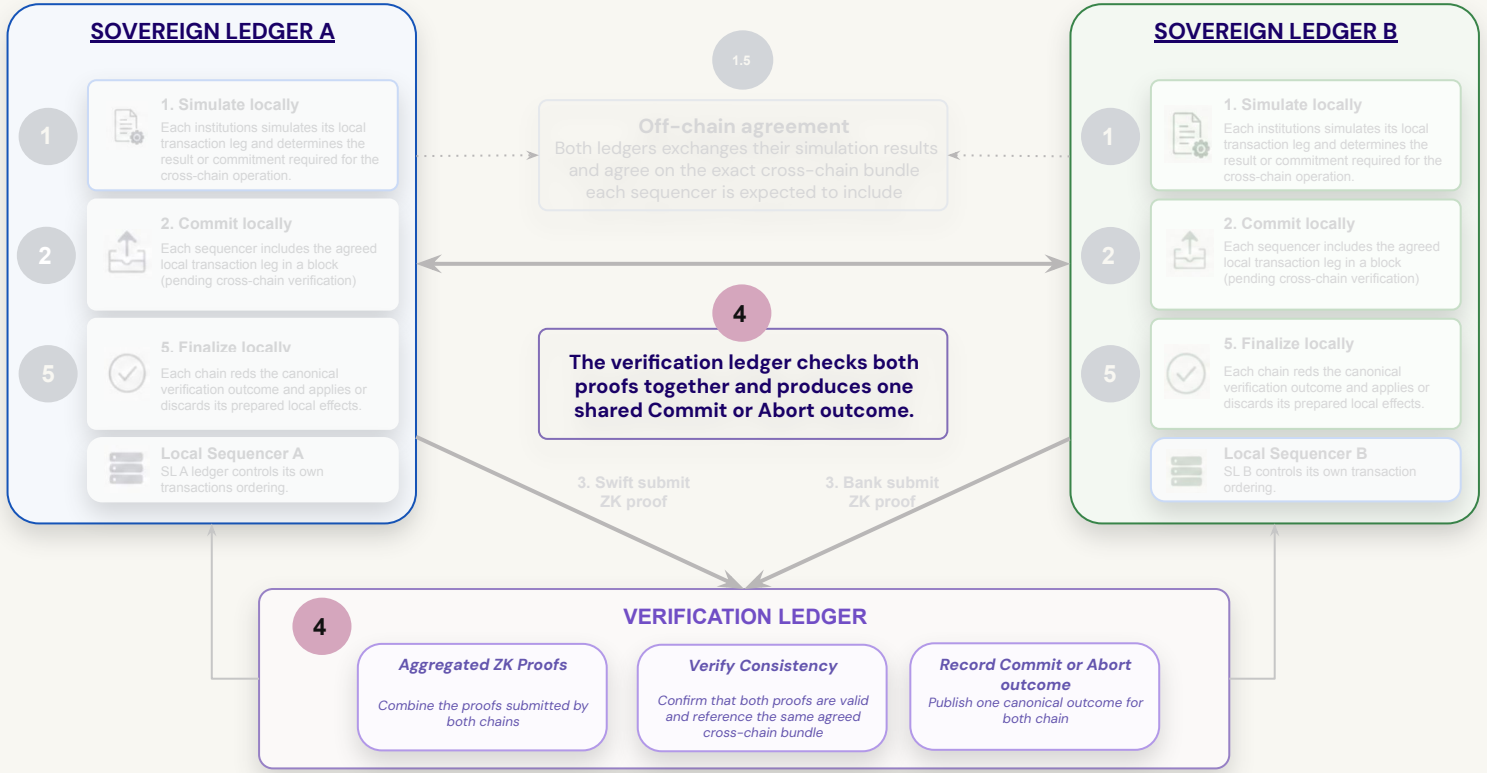
Interoperability across sovereign ledgers

Step 3 – Submit ZK Proofs



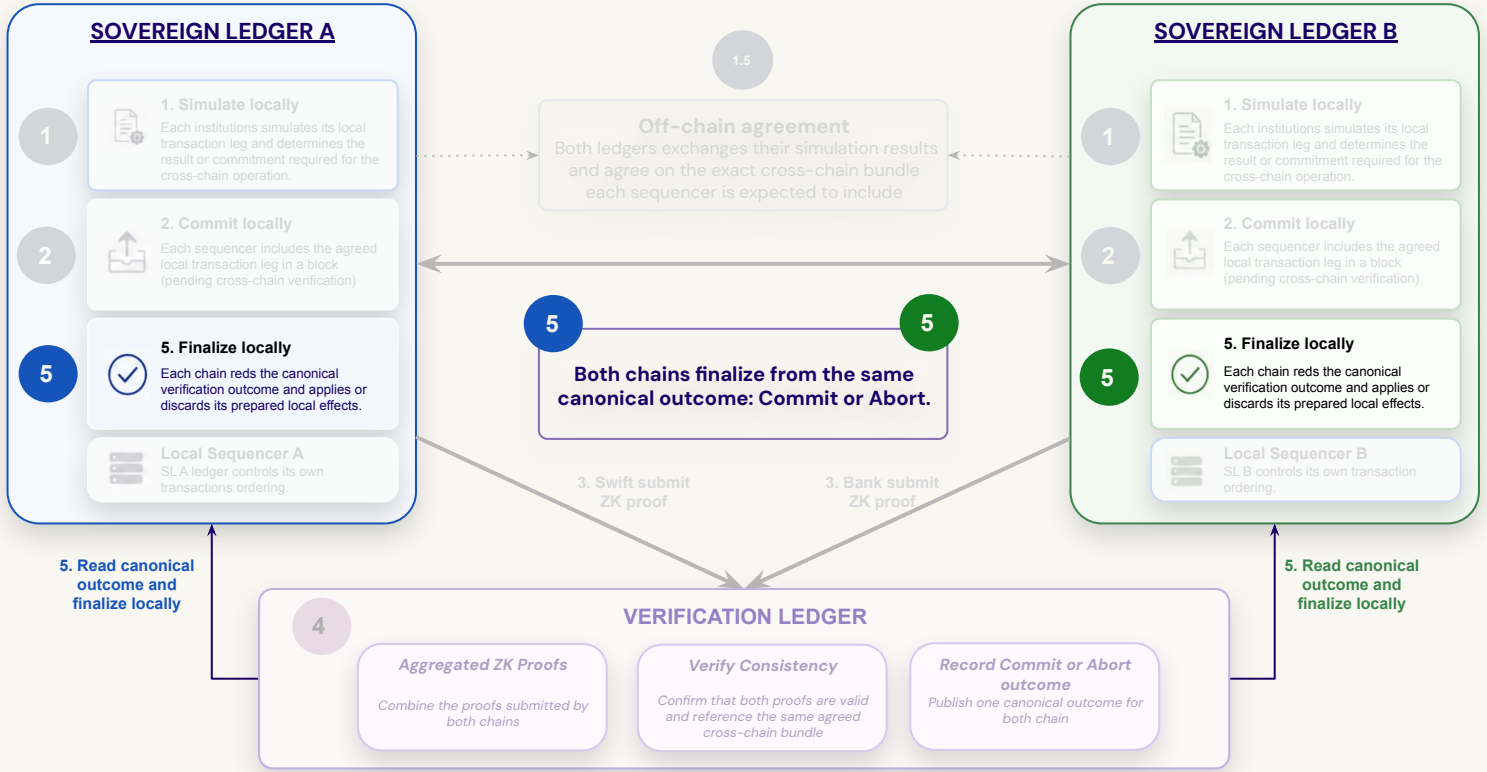
Interoperability across sovereign ledgers

Step 4 – Verify consistency and record the outcome



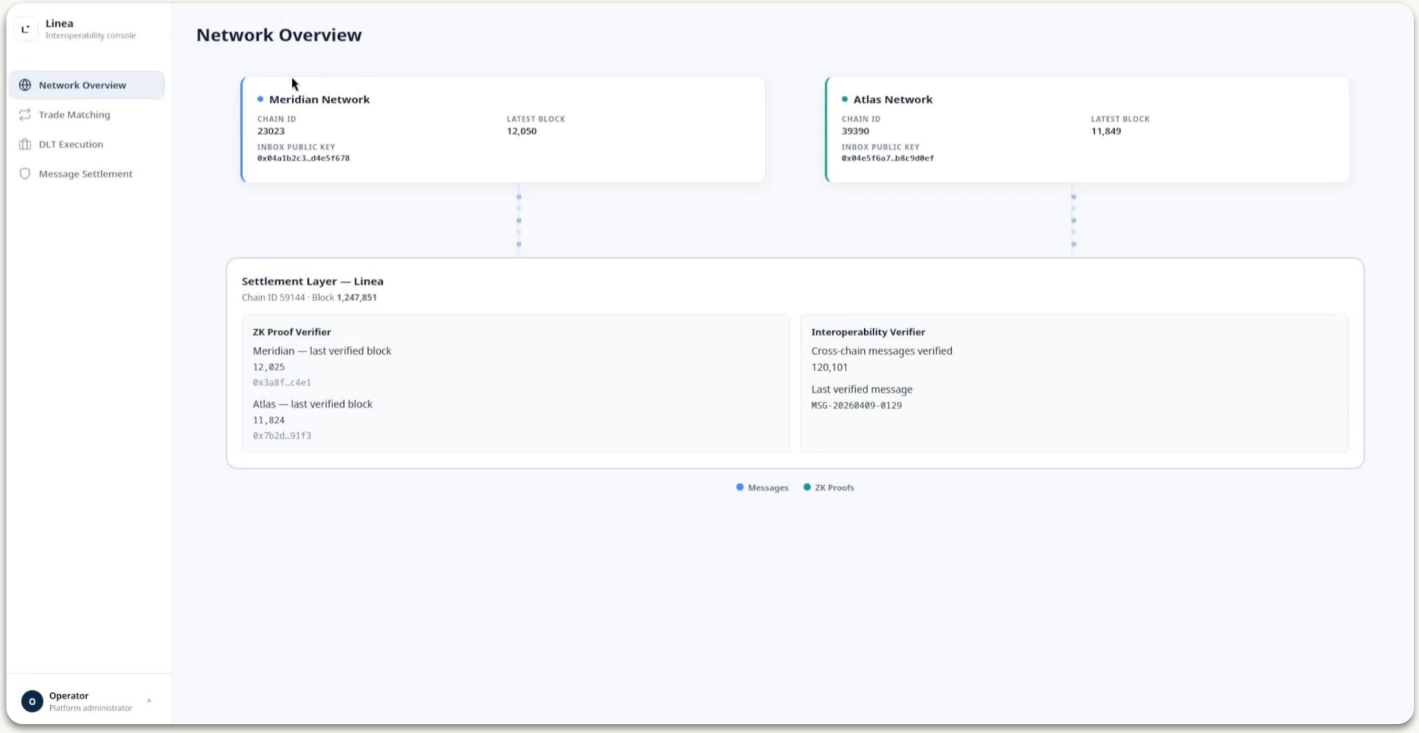
Interoperability across sovereign ledgers

Step 5 – Read the canonical outcome and finalize locally



Two networks, one verification ledger

Meridian and Atlas stay independent while the Verification Ledger provides the shared interoperability and settlement view



Context

The opening view establishes the operating model: Meridian and Atlass are separate networks, each with its own participants, chain identifiers, and block progression.

What this demonstrates

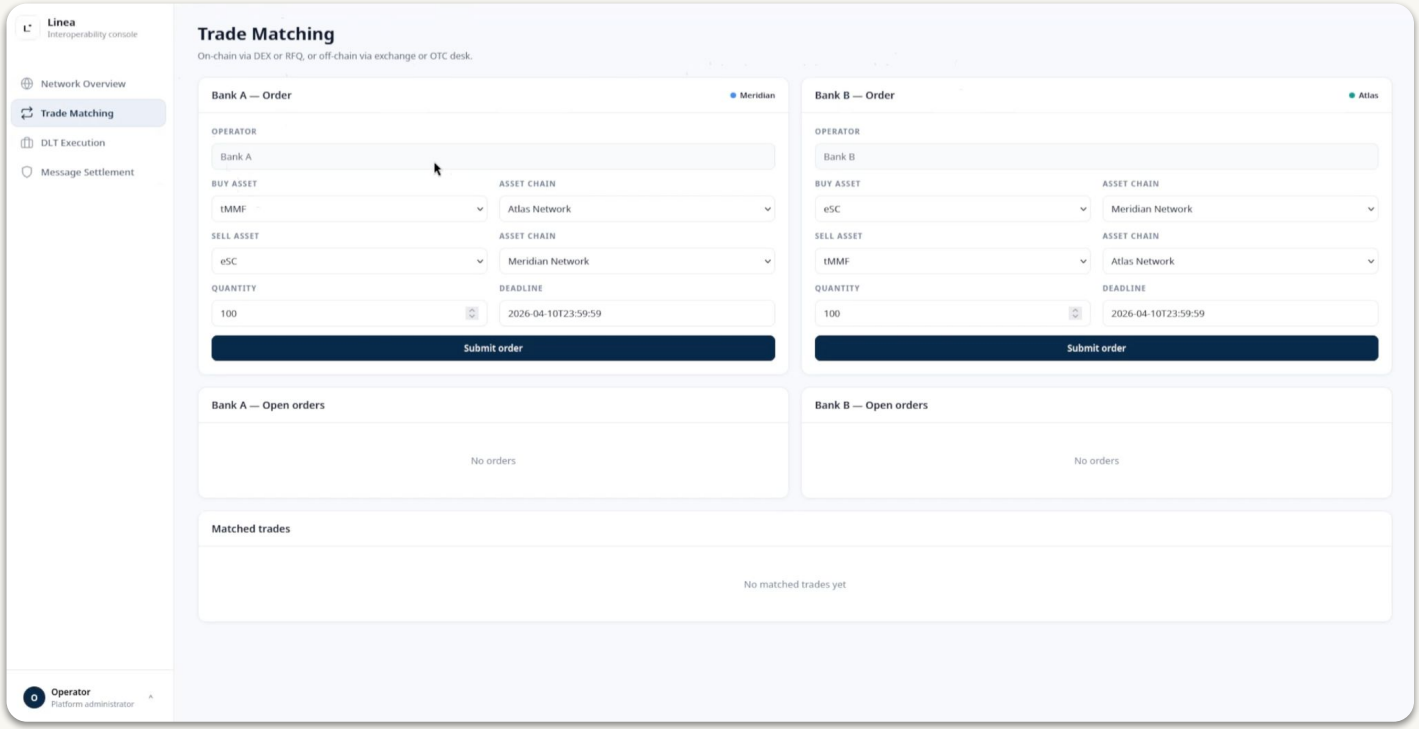
Ethereum provides a shared settlement and verification ledger. The operator can see network health, proof verification, and cross-network message from one console.

Takeway

Interoperability is presented as an observable control layer, not a black-box bridge.

Trade Matching: Bilateral order

Both sovereign chains enter the same trade terms: the system matches buyer, seller, asset, quantity, and price.



Context

This screen represents the pre-settlement business step. Bank A & Bank B enter mirrored orders and the platform compares the economic terms before execution.

What this demonstrates

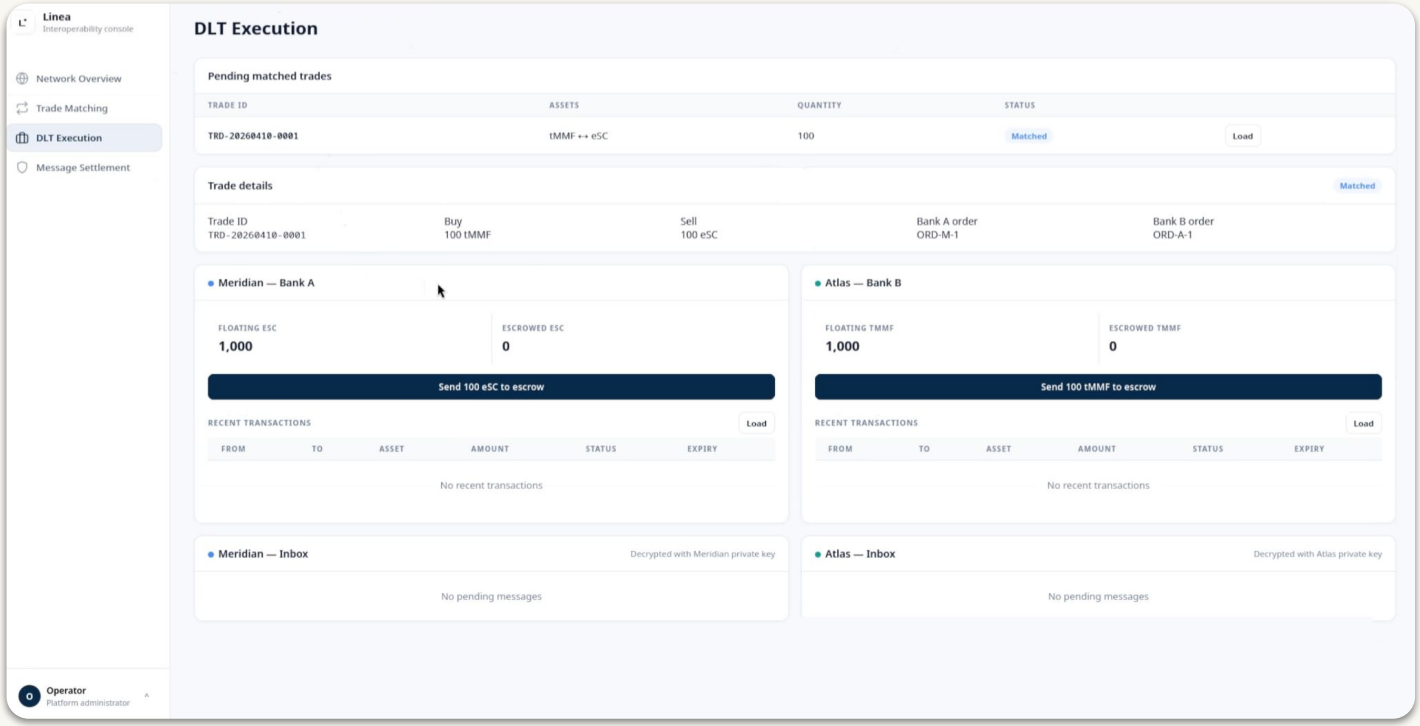
The workflow separates trade agreement from settlement. Only a matched trade becomes eligible for the next step, reducing the chance of operational breaks downstream.

Takeway

The demo connects familiar capital-markets workflow to programmable settlement.

DLT Execution

The matched trade is translated into token movements and escrow actions across the two networks



Context

Once the trade is matched, the platform turns the business instruction into executable DLT actions. Each side of the transaction is displayed with its own balances and escrow state.

What this demonstrates

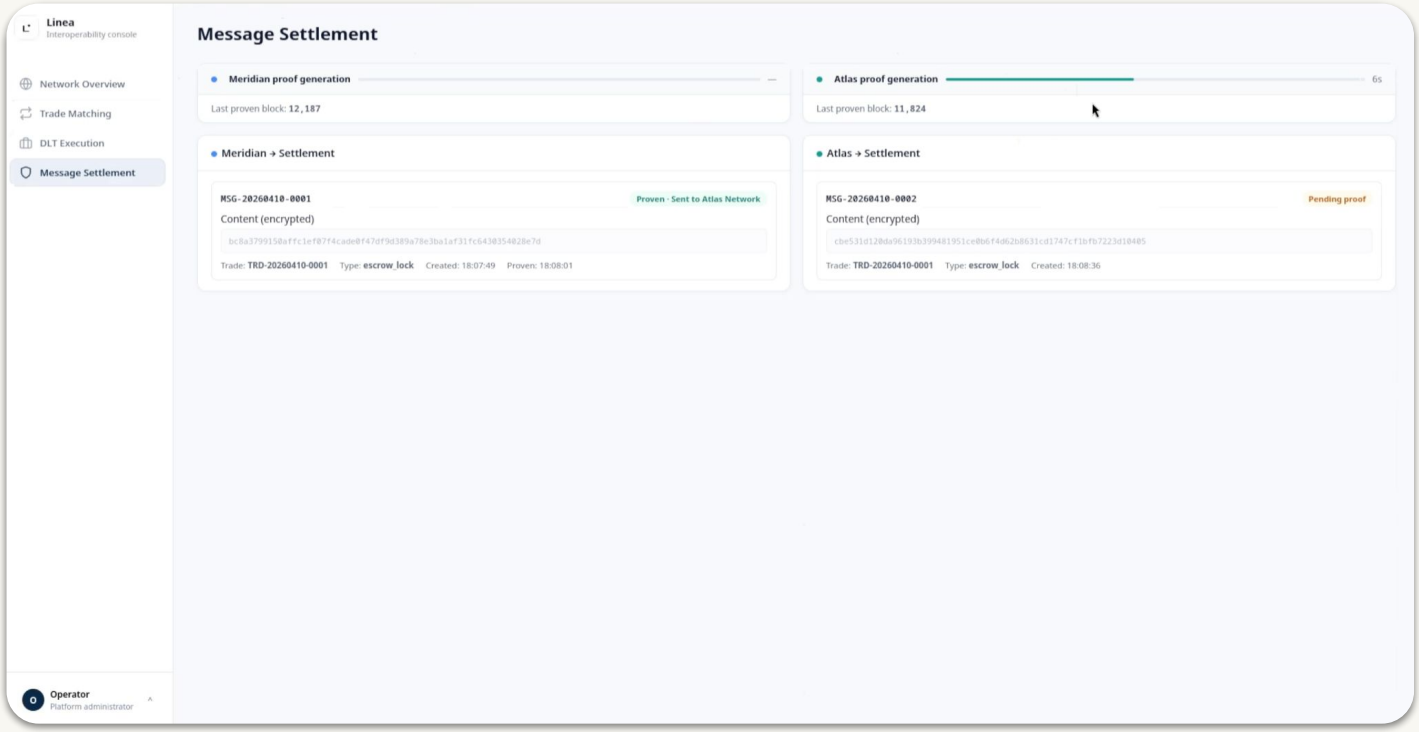
The operator can follow how the matched trade is decomposed into concrete token and transaction steps while both networks remain visible in parallel.

Takeway

Business intent is translated into traceable settlement instructions.

Message Settlement

Settlement messages are created on both sides, with status indicators showing progress toward confirmation



Context

The settlement step depends on cross-network messages. The screen shows message generation for both Meridian and Atlas, with progress indicators for each side.

What this demonstrates

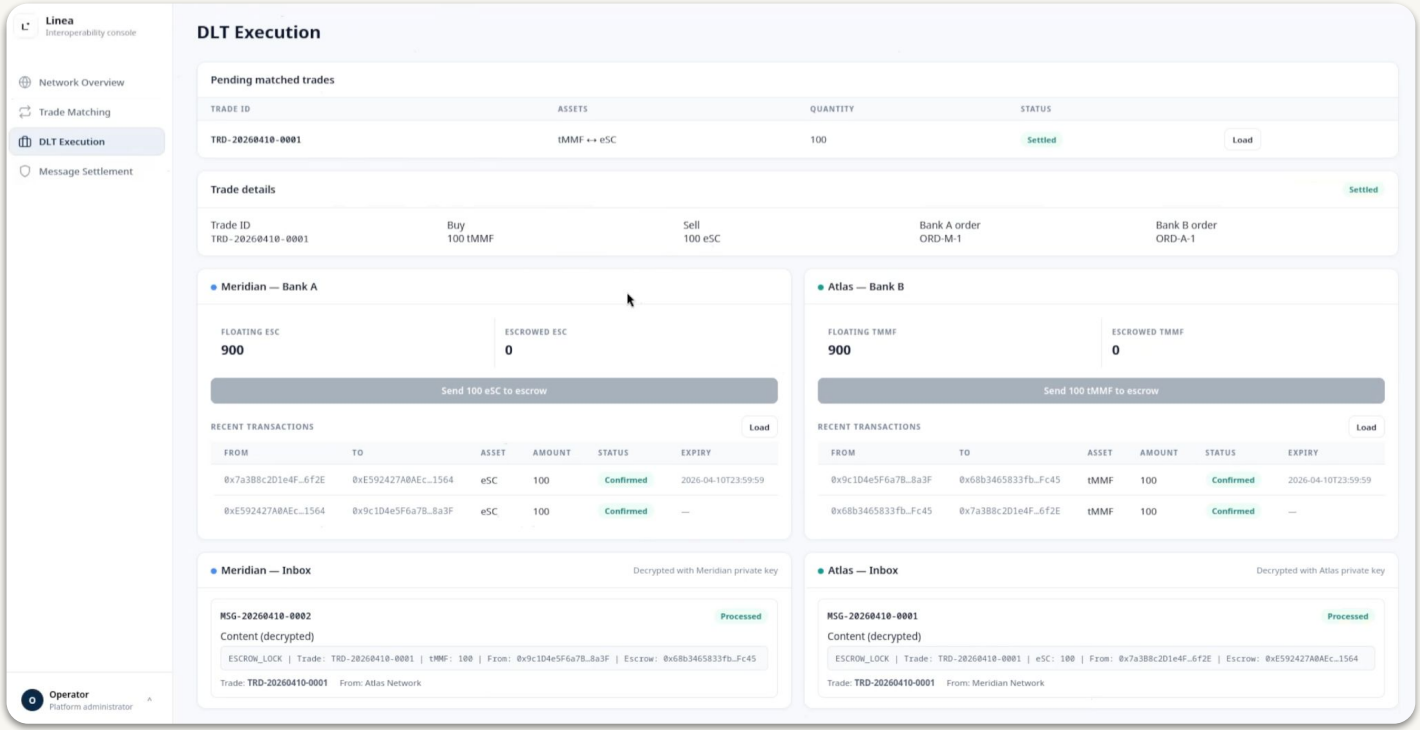
The console exposes the handoff between networks: messages can be pending, generated, or confirmed, giving the operator a clear view of settlement progression.

Takeway

Cross-network settlement becomes monitorable and auditable in real time.

End-to-end settlement is confirmed

The final screen shows completed transactions, updated balances, and confirmed cross-network messages.



Context

The final view closes the loop. The matched trade has moved through execution, message settlement, and confirmation across the relevant network components.

What this demonstrates

Completed transactions, updated balances, and confirmed message claims are visible in the same workflow, providing evidence that settlement has finished end to end.

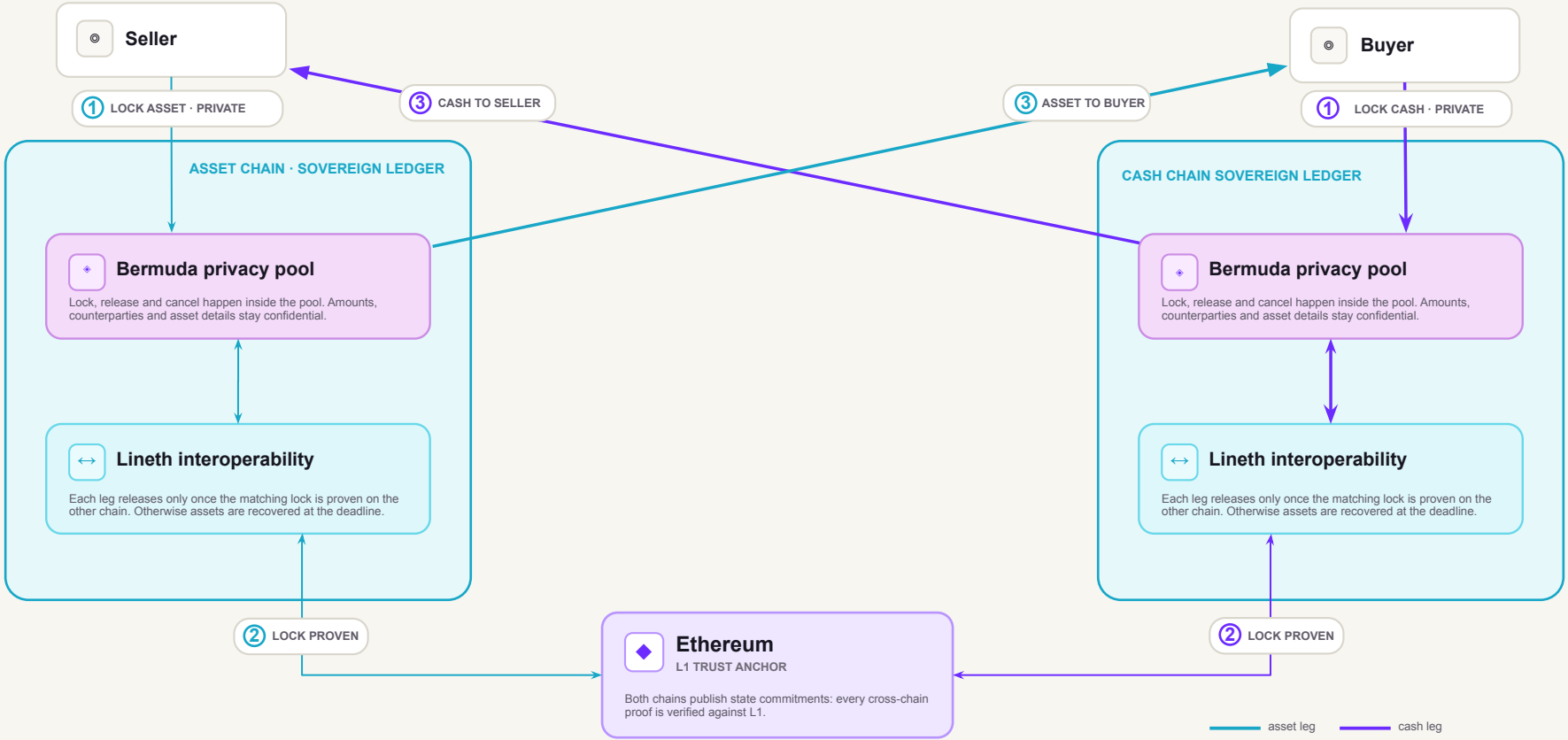
Takeway

The value proposition is operational certainty across independent networks.

consensys

Compatible with user-level privacy tooling

How Linea Mainnet and Bermuda demonstrate native interoperability across private and public chains

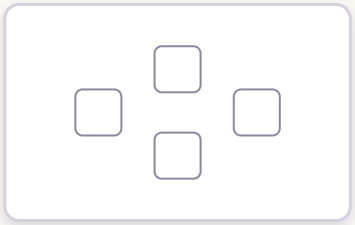


consensys

An upgrade, not a migration

Lineth turns on inside the Besu network users already run: same infrastructure, same control, now provable and connected.

TODAY

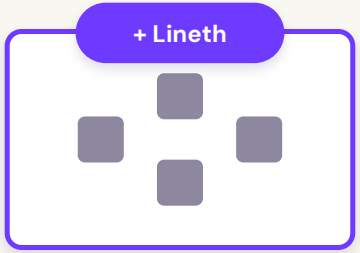


Your private network

You run a Besu network. You control it, and your data stays inside.

Upgrade

UPGRADE

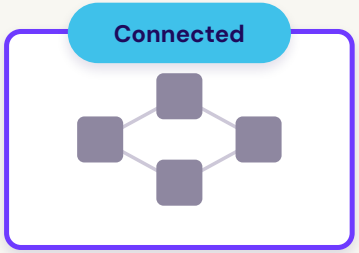


Turn on Lineth

A software upgrade to the same network. Nothing to rebuild, no migration project.

Connect

TOMORROW



Provable and connected

The same network can now prove its state and connect to Ethereum and partner institutions when you choose.

Same network, same team, same control. Lineth adds proof and reach without a rebuild.

The proof crosses the boundary. The data never does.

The hard part is making that survive settlement across sovereign ledgers. Let’s standardise the interface, let the implementations compete.

Privacy stops being the thing that isolates institutions, and starts being the thing that *connects* them.

Declan Fox - Consensys - X @DeclanFox14