OWNERA

WHITE PAPER

Multi-Chain Need-to-Know Privacy

Privacy across all chains, not just one

Need-to-Know Privacy: only the parties to a trade see the trade.

If you believe the market will be multi-chain, this is the architecture that matches that vision: the privacy you need, with the liquidity, throughput, technology and economics of all chains.

1 · THE REQUIREMENT

What Need-to-Know Privacy means

> **"Only the parties to a trade can see the trade."**

Need-to-Know Privacy means that only the participants in a transaction can see it. Who those parties are, what each of them can see, and which blockchain is used can all vary. What does not vary is that everyone without permission should see nothing. It is, quite literally, **none of their business**.

For market participants this is the most basic, common-sense business requirement there is. It is far simpler to understand and to govern than the cryptographic machinery (zero-knowledge proofs, encryption schemes) that may power it under the hood. That machinery matters to technology teams. The business requirement is the same for everyone: **my trades are visible to my counterparties and to me, and to no one else.**

Privacy has to live in two places

Any serious privacy architecture has to deliver at two distinct layers, and it is the relationship between those two layers that separates a single-chain model from a multi-chain one.

1 · BUSINESS LOGIC

Off-chain applications and legacy interfaces

Each party's own systems need the private trade data in raw form: to run business logic and risk analysis, negotiate with counterparties, keep regulatory records, run analytics, feed institutional AI platforms, and so on.

2 · SETTLEMENT

The on-chain ledger

The blockchain has to provide the privacy-enabled, immutable ledger: finality, smart-contract functionality and cryptographic proof, while hiding the private information from everyone outside the trade.

The multi-chain model enforces privacy **once**, at the application business logic, as a privacy umbrella above all the ledgers, and then activates each chain's own native privacy tools for settlement.

You can then route trades to wherever counterparties, liquidity and pricing are best, while holding signed confirmations of every trade, so you can recover from chain issues and switch chains if needed.

Need-to-Know Privacy within one network

Canton is an example of a blockchain that implements Need-to-Know Privacy:

- Each institution runs its own **node**.
- Only the nodes participating in a trade can see its details: messages are end-to-end encrypted.
- The network's **synchronisation layer** (on Canton, the Synchronizer) orders the encrypted messages and coordinates confirmations. It sees metadata and encrypted payloads, not trade content.

The trade-offs

When privacy is built only at the chain layer, the challenge is not the privacy itself but its scope: **the privacy works only inside the network**. Three consequences follow:

1. **Assets and liquidity have to be on the chain first**
   Every asset and pool of liquidity must already be on that chain, or be brought there. Assets, cash and counterparties elsewhere have to be migrated in, even when trading them where they are would be better, and "bridging" carries costs, delays and third-party risks.

2. **Applications are built in the chain's language**
   Applications, business logic and cross-party orchestration are built in the network's language (such as Daml on Canton or Solidity on EVM chains), and work only inside that network, within its framework, performance envelope and throughput.

3. **The chain's pricing and business model**
   Applications, and every transaction they generate, including moves between chains, run on the network's fee model and token economy.

What we enable: Keep the privacy you built on and extend it to all other chains – without the trade-offs.

SECTION 3
THE MULTI-CHAIN MODEL →

SECTION 6
CANTON-FIRST ORGANISATIONS →

Ownera: Need-to-Know Privacy, one layer above the chains, extended across all of them

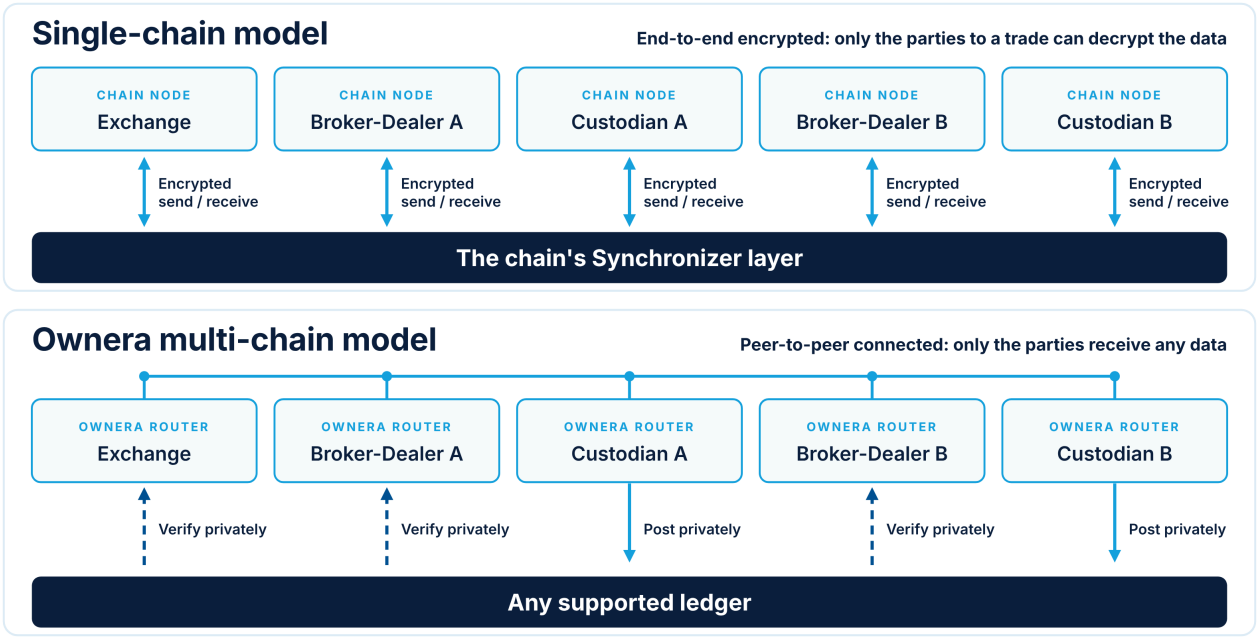
We believe the market is multi-chain and will stay multi-chain: no single network will hold every asset, every pool of liquidity and every counterparty. Institutions need an **umbrella of Need-to-Know Privacy across every ledger they use**: public blockchains, private blockchains and legacy systems alike.

Ownera's Routers separate the business logic and orchestration from settlement on any specific chain.

The model is similar to Canton's – only one layer above – for all the chains:

- Each institution runs its own **Ownera Router**.
- Only the Routers participating in a trade see the trade. Connections are **peer-to-peer**; there is no central hub – information is physically shared only between the participants.
- At settlement, the Routers use **each ledger's native privacy capabilities** and share the resulting proofs with the trade participants only.

  This means that the Routers can interconnect, under the same Need-to-Know Privacy umbrella, any chain that can keep the settlement private at the ledger level: private networks such as Besu, and public chains where privacy is now available or arriving, based on zero-knowledge proofs or encryption, including Ethereum and its L2s, Canton, Stellar, Solana, Hedera, Avalanche, Aptos, Aleo, Arc, the XRP Ledger, ZKsync Prividium and others.



A five-party trade under a single-chain model (top) and Ownera's multi-chain model (bottom).

4 · SIDE BY SIDE

Same privacy guarantee, wider scope

On the question that matters to the business ("Who can see my trade?") the two models give the same answer. The differences are in what the multi-chain model adds: everything a single chain offers, plus the same privacy over every other chain you use.

	SINGLE CHAIN PRIVACY	MULTI-CHAIN PRIVACY
Who sees the trade	Only the participants in the trade	Only the institutional Routers in the trade
Who sees metadata	Whoever orders the chain's transactions: its validators, sequencer or synchroniser	Similar. Some chains now offer hidden metadata as well. Ownera, as a software provider, sees nothing
Where privacy applies	Assets on that one chain only	Every chain and legacy ledger, including DvP between chains and moving assets between chains
Where assets and cash live	On that chain, or moved there first, natively or bridged. The move itself may be public	Wherever they already are: traded in place through cross-chain DvP, or moved privately when that is better
Resilience	One chain	Each institution holds signed confirmations of every trade on every chain. If a chain is compromised, it has the data to recover and can move trading to another chain
Liquidity	One chain	The sum of all connected chains
Throughput	One chain's limits	The sum of all connected chains
Application language	The smart-contract language of that chain	Business logic written once, in your stack, using "business intents", settled on any chain
Fee per transaction	The economy and gas fees of that chain	The fee of whichever chain the trade settles on: fractions of a cent on many chains and no gas fees on private networks such as Besu
Record of trades	On-chain, on that chain	On-chain on each chain, plus an off-chain log per institution with counterparty-signed cryptographic proof of every trade across chains

Ownera extends the Need-to-Know Privacy model across multiple chains and legacy platforms, adding broader liquidity access, technology choice and flexibility.

5 · UNDER THE HOOD

How multi-chain privacy works in detail

The Ownera model separates business logic and multi-party orchestration from blockchain settlement. The off-chain business logic, orchestration and privacy are **developed once for all chains**; each blockchain is then responsible only for delivering private, immutable ledger functionality.

At the orchestration layer, one level above the blockchains

- Every institution runs a Router, and **only the Routers participating in a transaction see the transaction.**
- **Each Router is operated by the institution that owns it.** Ownera supplies the Router as software, installed on-premises or run as a managed service, and is not a party to any trade: no Ownera system sits between the Routers, sees the data or holds the keys.
- Privacy is managed explicitly at the **pre-trade and trade stages**, not just at settlement: it covers wallets, smart-contract addresses, settlement contracts and all other off-chain information the trade needs.
- The participating Routers agree a **distributed orchestration plan**. As the plan executes, they share between themselves the data and ledger proofs each party needs, and nothing more. A party that depends on a step it cannot see receives a signed proof of that step.
- At settlement, the selected blockchain hides the information from the world while providing immutability, whatever smart-contract functionality the chain offers and cryptographic proofs.
- **Atomic swaps are the preferred option**, but when the asset is on another chain, moving an asset may cost time and money, may create third-party wrapping risks, and may hold liquidity on the source chain for longer than needed. The Router offers the option to settle almost instantly where each asset lives, as a DvP, in which the cost, timing and risk profile may be superior, or even be the only option.
- **Each party keeps a complete off-chain evidential record** of every trade across all blockchains, with cryptographic proofs signed and delivered directly by its counterparties. If a blockchain were compromised, the institution would still hold proof of every trade with every counterparty.

> **This architecture natively preserves the Need-to-Know Privacy protection when adding a blockchain, adding a counterparty or adding an application.**

5 · UNDER THE HOOD

At the blockchain layer: hiding the trade from the rest of the world

Each ledger hides the information in its own way, and the Router and its ledger connectors manage this for the institution. The main approaches:

PRIVATE CHAINS

Private participants and private access

Private networks such as Besu are private by nature. Some installations also add authenticated "private access" so that each user sees only its own trades.

PUBLIC CHAINS

Zero-knowledge settlement

Public blockchains now support a range of zero-knowledge capabilities that hide private data on-chain. Different chains offer different models with different trade-offs between performance and features. The Router abstracts the choice.

CUSTODIANS

Omnibus accounts

Custodians hide transaction-level detail inside omnibus structures. **Most privacy in both crypto and traditional markets is delivered this way**: it is how most crypto exchanges give their clients privacy on Bitcoin, a public ledger, by trading inside their own custody ledgers.

PRIVACY-FOCUSED CHAINS

Native privacy, under one umbrella

On chains built for privacy, such as Canton, the Router uses the chain's own privacy natively, through the chain's standard token actions, such as transfer, hold, release, cancel, mint or burn. Around that, the Router can orchestrate private cross-chain asset movement and DvPs – all under the same Need-to-Know umbrella.

WHEN THE ASSETS FOR A TRADE LIVE ON DIFFERENT CHAINS

Bring the assets to the trade

Move the assets to the same chain and execute an atomic swap. The Routers can orchestrate it when needed, but while the swap may be risk free, the move isn't always possible, free or private: it may add costs, delays, locked liquidity and asset-wrapping.

Bring the trade to the assets

The Routers can orchestrate a cross-chain DvP, using HTLCs or committed holds, that settles each leg where the asset lives. Nothing is wrapped, nothing moves, and everything stays within Need-to-Know Privacy.

6 · CANTON-FIRST ORGANISATIONS

Canton-first? Keep everything, and gain the rest

Canton describes itself as an open network with published token standards, and Ownera connects to it exactly that way. A Canton-first institution gives up nothing: not its applications, its participant or its privacy model. It gains assets, pools of cash and counterparties that are not on Canton.

YOUR APPLICATIONS

Nothing to rewrite

Your existing Daml applications keep running. The connector runs beside them on your own participant, calls the registry's own contracts, and adds no business logic to Canton.

TOKEN STANDARDS

Standard actions, no custom Daml

On its core path the connector runs no custom Daml: transfers, holds, settlements, cancels, mints and burns go through CIP-56 and CIP-112, so any compliant registry works.

YOUR DAML TEAM

Owns the on-ledger proof layer

An optional Daml module records the plan on Canton, witnesses counterparty holds with your own node's validation, and gives auditors or regulators a read-only view. Yours to deploy and extend.

GOVERNANCE

Your participant stays in charge

The connector deploys nothing you have not vetted, checks every counterparty's participant before a plan is approved, refuses breaking upgrades and never downgrades.

NEW APPLICATIONS

Build multi-chain apps

If you need to build a new, natively multi-chain app, build the business logic and orchestration once using Ownera multi-chain intents. Daml stays the authority for every Canton-side native action. Contact us for code templates.

EVERYWHERE ELSE

Private DvP against any chain

Canton assets stay on Canton with Canton's privacy, and trade against cash and assets on public or private networks and legacy systems, with no wrapping and no bridge: nothing moves, and nothing leaves the privacy umbrella.

For the Canton developer

You keep your Daml, your participant and your privacy model, and add privacy-enabled access to other chains, counterparties and applications – all through the same connector.

Next step: ask us for the connector's engineering guide: the API, token actions and proofs, line by line. **info@ownera.io**

7 · WHAT YOU GAIN

The multi-chain advantages, summarised

CHAIN CHOICE

Multi-chain by design

Choose the best chain for each task, and add a new one by adding a connector, with every application continuing to work unchanged.

LIQUIDITY

The sum of all chains

Aggregated across every connected chain and venue, rather than limited to the assets that have been migrated to one.

THROUGHPUT

The sum of all chains

Capacity scales with the chains you use, rather than being capped by the limits of a single network.

ECONOMICS

The fee of the chain you choose

Settle each trade where the combination of liquidity, features and price per transaction meets your requirements.

RESILIENCE

Your own record, with signed proofs

Signed confirmations of every trade, held by the institution itself. If a chain fails or is compromised, the record is intact and recovery is possible, and trading can continue on another chain.

BUILD ONCE, CONNECT ONCE

Reduced costs and time to market

Privacy-enabled business logic and orchestration are developed once for all chains, so **supporting a new chain** with privacy costs close to nothing. The same is true of counterparties: all parties speak the FinP2P orchestration protocol, so **new counterparties** can be added with minimal integration, reducing costs and time to market.

Proven in production

This is not a whitepaper architecture. Ownera Routers orchestrate collateral, intraday repo and private-market use cases with major global banks, and have powered the tokenised-collateral industry sandboxes in the U.S., EU and UK, interconnecting 50+ firms. The platform is ISO 27001, ISO 27017 and SOC 2 Type II certified, and runs managed, dedicated, or on-premises in your own Kubernetes, so all sensitive data, compute and execution authority stay inside your perimeter. Communication between the Routers is direct and peer-to-peer over gRPC or HTTP/1.1 over TLS, using the FinP2P open protocol.

8 · THE DECISION

The decision in one sentence

If you believe in a multi-chain future, you do not have to give up privacy to get there, or move your assets to keep it. Ownera brings Need-to-Know Privacy to every chain you use, with the liquidity, throughput, chain choice and economics of all of them.

Next step: a 60-minute architecture session with your teams, walking through a live multi-chain trade.

ABOUT

About Ownera

Ownera provides the open, multi-chain orchestration layer for tokenised markets. Every institution runs its own Router; Routers connect peer-to-peer over the FinP2P open protocol; connectors normalise every blockchain, custody platform and legacy system behind one API, with a set of ready-made institutional applications for collateral, repo, trading and settlement on top. Business logic is written once and settled on any chain, with Need-to-Know Privacy throughout.

ownera.io
Contact: info@ownera.io

IMPORTANT INFORMATION

This document is provided by Ownera for information only and is intended for institutional and professional audiences. It is not an offer or solicitation, and it is not legal, regulatory, tax or investment advice.

Privacy and security. Statements about privacy and confidentiality describe how the Ownera architecture is designed to work. What is visible to whom in a given deployment depends on its configuration, the blockchain or ledger used, custody arrangements, and the service providers and regulators each institution chooses to share data with. Some transaction metadata may remain visible on public networks. Institutions remain responsible for their own regulatory reporting, record-keeping and supervisory access.

Records. Cryptographic proofs and off-chain logs provide an evidential record of transactions. The legal effect of any transaction depends on the agreements between the parties and the applicable law.

Forward-looking statements. This document may describe products, features, integrations and third-party network capabilities that are in development or planned. These may change, may be delayed or may not be delivered. Fee and performance figures are illustrative and vary by network and market conditions.

Third parties. Information about third-party networks and products is based on publicly available sources believed to be reliable at the date of publication, and has not been independently verified. All third-party names and trademarks belong to their respective owners. Their use does not imply affiliation with or endorsement of Ownera. Client and partner names are used with permission.

Certifications. Certification and attestation details apply to the scope set out in the relevant certificate or report, which is available on request.

No warranty. This document is provided "as is", without warranty of any kind. To the extent permitted by law, Ownera accepts no liability for any reliance placed on it.

© 2026 Ownera. All rights reserved. FinP2P is an open protocol specification.