



BLOCKDAEMON

WHITEPAPER

Canton

A Guide for Institutions

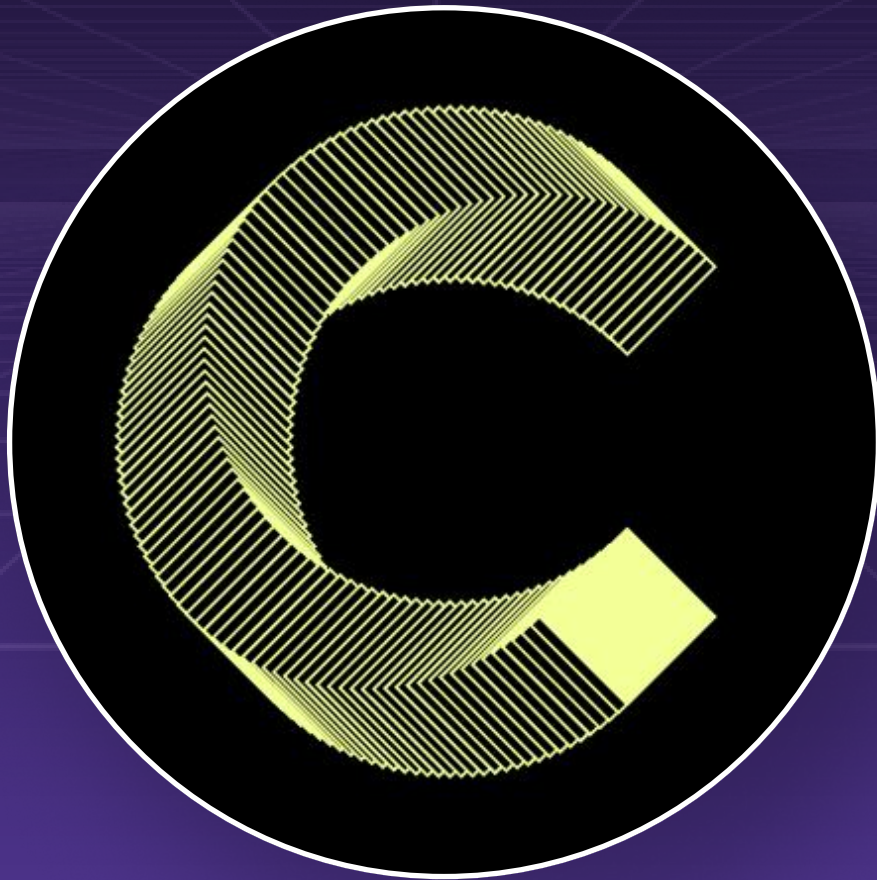


Table of Contents

1. Introduction	1
Canton Ecosystem At A Glance	1
2. Daml: Canton’s Privacy Preserving Smart Contract Language	2
2.1 The Active Contract Set (ACS)	2
3. Consensus: Proof-of-Stakeholder	3
3.1 Stage 1: Stakeholder confirmation	4
3.2 Stage 2: Sequencing	4
3.3 Use cases	4
4. Global Sync	5
4.1 Roles in the Global Synchronizer	6
4.2 Who runs and governs the Global Synchronizer?	6
4.3 How fees work	6/7
5. Conclusion	8

Canton is a privacy-enabled public network for institutions.

The name “Canton” is derived from the Swiss system of federalism, where largely autonomous, semi-sovereign cantons form the Swiss Confederation. The country is composed of “Cantons”, each with its own governance rules, yet all remain part of a larger federation. Similarly, on the Canton Network, each application (or “Canton”) independently defines its own parameters for privacy, permissions, governance and fees.

Canton is a network that targets the missing primitives that have limited institutional adoption: selective data visibility so parties can transact without exposing sensitive information, apps that atomically interoperate but also have independent control over how they operate, and incentives that reward the builders and users who create value.

Most public blockchains are designed for radical transparency, and optimized for mobility. Canton pairs the core innovation of asset mobility with privacy and fair, aligned incentives for apps builders and users. On Canton, validation happens on a need-to-know basis - more like a sealed envelope than a public postcard - delivering privacy proven at institutional scale.

Canton’s tokenomics are designed to create a true application network, not a speculative validator network. Two-thirds of rewards go to the apps and users creating real utility - meaning when applications and assets drive network traffic, they earn in the process. Canton Coin is the utility token used to pay for Global Synchronizer usage and other network costs, and the protocol distributes issuance to apps, operators, and users over time, based on the utility they bring to the network. Every Canton Coin in circulation has been earned.

Canton is purpose-built infrastructure for money and markets - a public network where institutions can connect, transact, and compose applications with privacy and control. It enables the atomic, programmable movement of value to convert high-quality collateral, stablecoins, and onchain assets, unlocking 24/7 onchain capital markets.

Public blockchains have proven the value of asset mobility through stablecoins. Canton adds privacy built in at the L1 level, removing one of the biggest barriers to adoption at global capital-markets scale.

Canton Ecosystem At A Glance

\$6T+ in tokenized assets processed onchain	575+ validators	30+ super validators
\$135M Digital Asset Canton Network’s creators raised in June 2025		

2 Daml: Canton's Privacy Preserving Smart Contract Language

Canton implements Daml, an open-source language and ledger model, designed for multi-party applications.

A Daml contract is a codified multi-party workflow. Each contract names:

1. **Signatories (must authorize create/archive).**
2. **Observers (can see it).**
3. **Controllers for specific choices (the actions that can be exercised on a contract).**

Signatories can be a single entity or a consortium with a multi-sig policy, so assets can be issued and controlled centrally or by federations. Authorization is explicit and fine-grained.

2.1 The Active Contract Set (ACS)

A transaction **creates** a contract (it becomes active). Later transactions may **archive** it. The set of all active contracts is the **Active Contract Set (ACS)**, derived from a **transaction graph**. New transactions are atomic appends to this graph and can reference prior contracts (inputs) as dependencies.

Transactions are **tree-structured** and partitioned by entitlement. Each party sees only its **sub-transaction** and can validate just that subtree. No party holds the full network graph. No participant sees the full transaction graph, only their entitled view. That aligns with Canton's institutional privacy message. Every party holds a private, valid subset (its "view") that is locally verifiable against contract logic and authority. The below figure illustrates Alice and Bob each seeing only parts of two transactions yet ending with a consistent ACS.

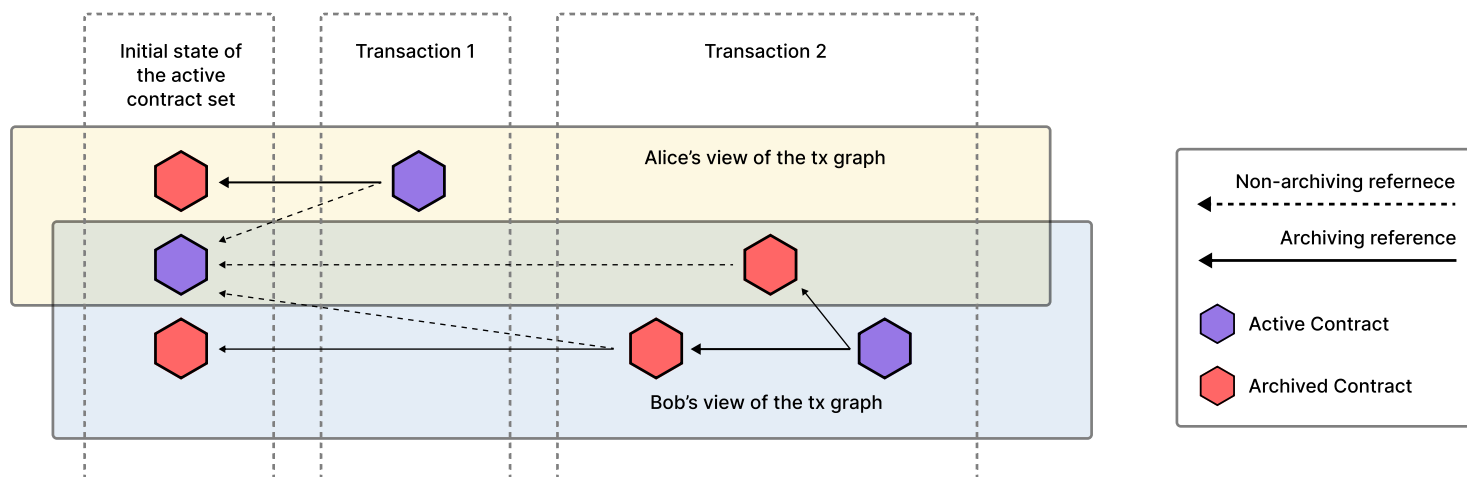


Figure 1: Example transaction graph with sub-transaction privacy. Alice and Bob each have only a partial view of the full transaction graph. Initially there are three active contracts; each party sees only two of them. (Source: Canton Network Whitepaper, 2024)

On receiving a (sub-)transaction, a validator node verifies three things locally:

1. **It's consistent with the party's current view.**
2. **It conforms to the Daml contract logic.**
3. **It's properly authorized (right signatories/controllers).**

This requires no trust in other parties' data beyond what the protocol and signatures prove.

Because transactions declare their dependencies, independent workflows can be processed on separate infrastructure in parallel. This is why Canton can scale horizontally without a single global bottleneck.

Consensus: Proof-of-Stakeholder

Canton's consensus mechanism, called **Proof-of-Stakeholder**, ensures that all parties maintain a consistent view of the global Active Contract Set (ACS) while preserving data privacy. Unlike proof-of-work or proof-of-stake blockchains, where every transaction is broadcast to the entire network, Canton only involves the parties who actually need to see and validate a given transaction.

Rather than maintaining a single global state, Canton separates consensus into two complementary layers:

- **Validity layer:** Contract stakeholders validate the business rules relevant to them, but only over the data slices they are permitted to access.
- **Ordering layer:** A **synchronizer** provides routing and ordering for encrypted transaction requests. Its role is to keep validator nodes "in sync" by assigning a consistent order to transactions across participants. Crucially, the synchronizer does not validate business rules or inspect contract contents.

At the core of this process are the **validator nodes**. Validators host both the Daml smart contract code and the associated contract data. For each transaction, only the validators that are stakeholders in that particular leg of the workflow take part in validation, and they alone are responsible for confirming its correctness. The synchronizer then ensures that these validators' updates are coordinated, so everyone who needs to agree moves forward together in the same order.

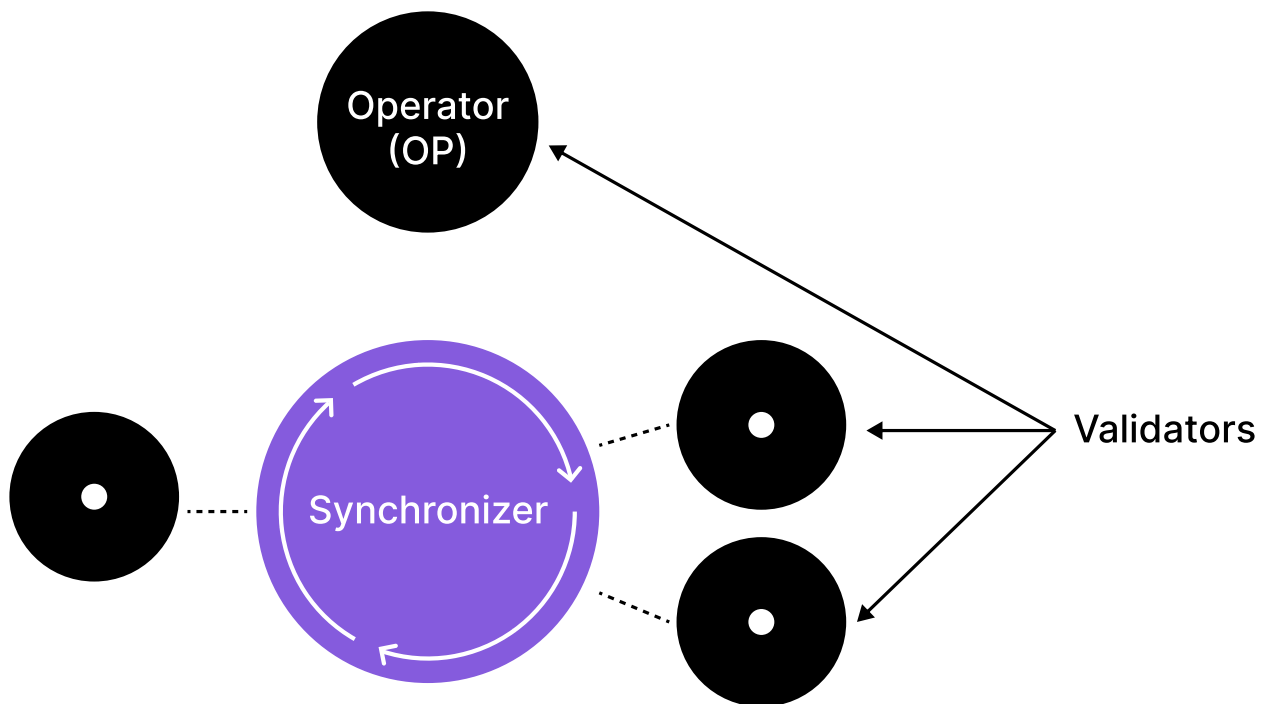


Figure 2: Validators connecting to a single synchronizer. Source: [Canton.network](https://canton.network), 2025

3.1 Stage 1: Stakeholder confirmation

A business who is allowed to submit signs the request. Their validator node encrypts the request and sends it to a synchronizer. Each signer gets only the part they are allowed to see. At each signer's node, that private slice is decrypted and checked against three simple rules: it must match the node's current view, it must follow the Daml contract rules, and it must be properly authorized by the right people. If these checks pass, the node returns a signed "yes." If the needed "yes" votes do not arrive in time, the whole thing rolls back. A Mediator in the synchronizer coordinates this two-step commit so everyone either moves together or not at all. All messages remain encrypted to the infrastructure, the Mediator cannot read payloads.

3.2 Stage 2: Sequencing

Next, Sequencers give each request a logical timestamp and builds one total order inside that domain. With one order, all nodes handle conflicts the same way. In a consortium run, distributed synchronizer, the sequencer is a replicated byzantine fault-tolerant (BFT) service - so it keeps working even if some parts fail and no one operator has control. In a single-operator setup, it can be a centralized, for very high-throughput service. In both cases, payloads stay encrypted, so operators cannot read transaction contents. A request that is both confirmed and ordered commits for all signers at the same time; otherwise, it is rejected.

3.3 Use cases

Canton supports a number of growing institutional use cases, such as:

- **Goldman Sachs DAP:** End-to-end tokenization platform enabling T+0 settlement (sub-60s) for bonds and expanding to multiple asset classes, reducing operational risk and costs while being interoperable across permissioned and public blockchains.
- **HSBC Orion Platform:** Tokenization platform using Canton/Daml, enabled the first GBP-denominated digital bond, combining a private encrypted ledger with mirrored public disclosure for transparency, reducing admin costs, widening investor access via fractional ownership, and streamlining issuance.
- **Broadbridge DLR:** Broadridge's Distributed Ledger Repo (DLR) platform settles more than \$280B in average daily repo transactions (\$5.9T monthly), accelerating collateral velocity, improving liquidity management, and reducing trade processing costs for the global repo market.

4 Global Sync

Private sync domains provide a permissioned synchronizer for application operators and their app users. Historically, regulated financial institutions started by running their own domains. One core innovation and differentiator of Canton is the ability to enable these domains to work together atomically, while retaining its core feature of privacy. For example, a delivery-versus-payment needs asset, cash, and trading apps to all update at once.

Those private deployments act as subnetworks inside the bigger Canton Network. Applications can dynamically choose which domains they use for different transactions, including the Global Synchronizer which provides a fully decentralized interoperability service across applications and subnets. It delivers atomic smart contract composability across apps and domains, unlike message based bridges used to connect subnetworks in other networks. It's a highly resilient, 'trustless' service any validator can use to coordinate transactions.

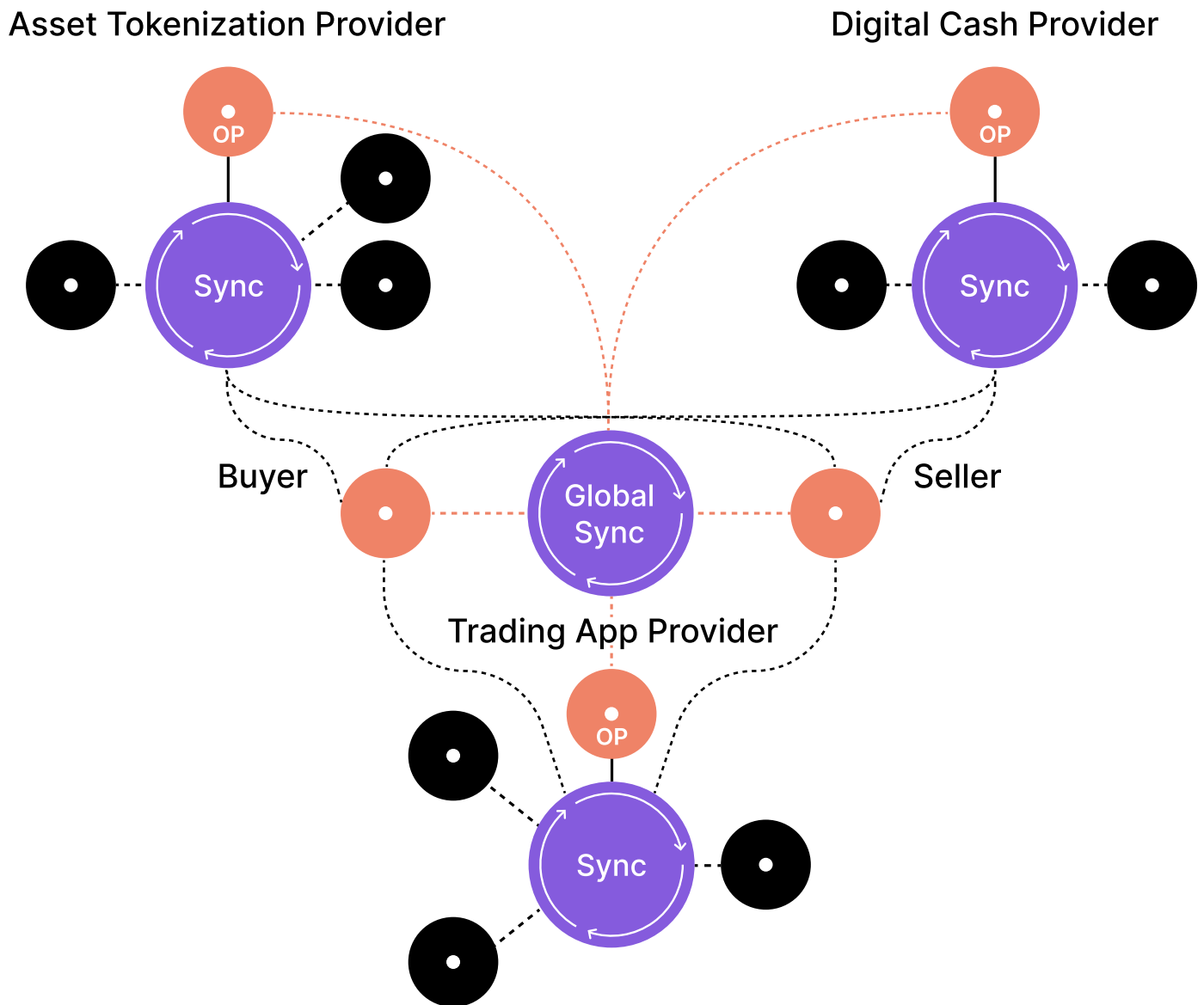


Figure 3: Interoperability across apps using the Global Synchronizer. Source: [Canton.network](https://canton.network)

4.1 Roles in the Global Synchronizer

The Global Synchronizer is supported by three primary participant types. Each contributes to the growth and operation of the network and, as a result, gains the ability to mint Canton Coin.

- 1. Super Validators:** Known and diverse set institutions that secure and operate the decentralized synchronizer infrastructure.
- 2. Full Node Validators (app users):** Entities that run validator nodes to directly participate in apps and validate transactions to which they are a party.
- 3. Application Providers:** Teams that deploy smart contract apps and tokenized real-world assets (RWAs).

4.2 Who runs and governs the Global Synchronizer?

The Global Synchronizer is run as a fully decentralized service by Super Validators - known organizations, including household names in finance and fintech. Governance comes from the Canton Foundation, with facilitation by the Linux Foundation. The Canton Foundation lists its members publicly and also runs a super validator to represent member interests. Today, validator requests are routed through the Canton Foundation. Over time, access will move toward **permissionless** entry for new participants.

4.3 Use cases

Like other public networks, the Global Synchronizer charges a fee. Unlike others, the fee is based on transaction size and paid in **Canton Coin**, the network's native utility token, while pricing is expressed in **USD terms** to keep costs predictable for institutions. Under Canton's fair-launch token model, every coin in circulation has been earned through measurable utility.

Rewards are distributed across Super Validators, Validators, and application providers, with the balance shifting over time from infrastructure operators to app developers as the ecosystem matures, as shown in figure 4.

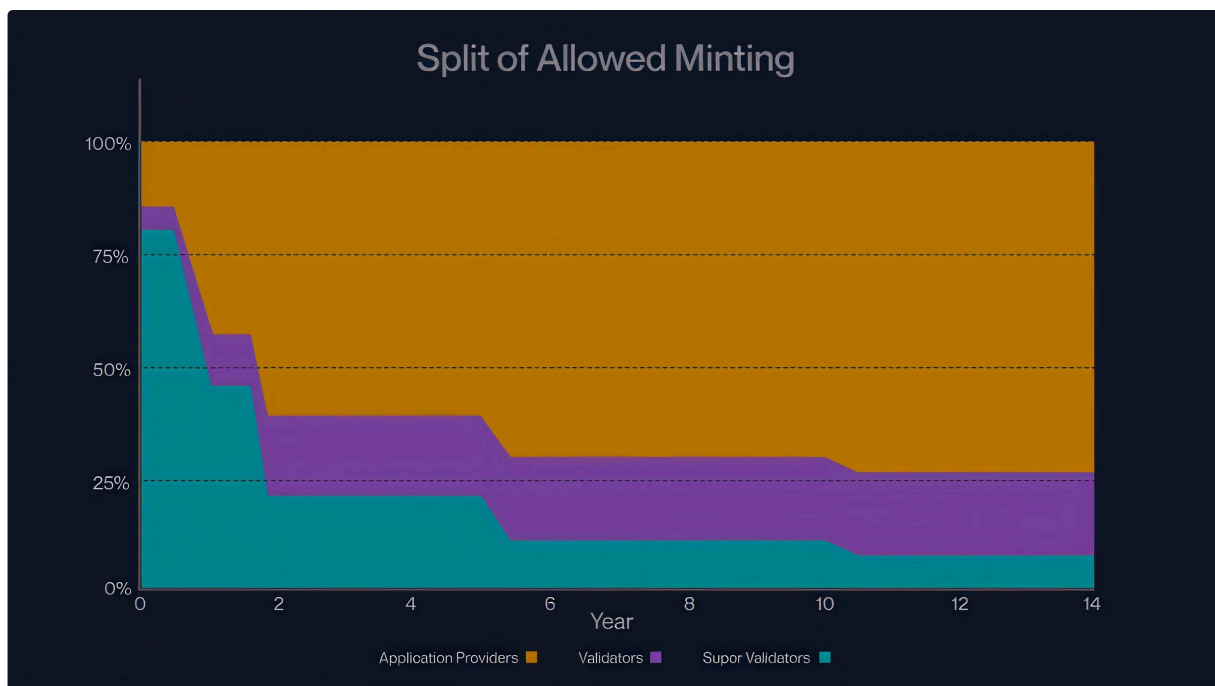


Figure 4: Interoperability across apps using the Global Synchronizer. Source: [Canton.network](https://canton.network)

Participant	Share of Rewards*	What Qualifies
Infrastructure providers (super validators)	35%	Operating and securing core network infrastructure
Application builders	50%	Deploying smart contracts, tokenizing assets, and running apps that generate activity
Users (transactors)	15%	Using apps and transacting on-chain

*Total reward split over a 10 year period. Reward share changes as per the published schedule, favoring app providers over time e.g 62% of rewards will go to apps between 2026 - mid-2029

Source: [Canton, 2025](#)

For organizations that cannot directly hold tokens, partners, such as Blockdaemon, offer wallet or validator-as-a-service solutions to enable use of the synchronizer without direct coin custody.

Behind the scenes, a **burn-and-mint equilibrium** ties supply to actual network usage, maintaining long-term alignment between token value, USD conversion rates, and real network utility.

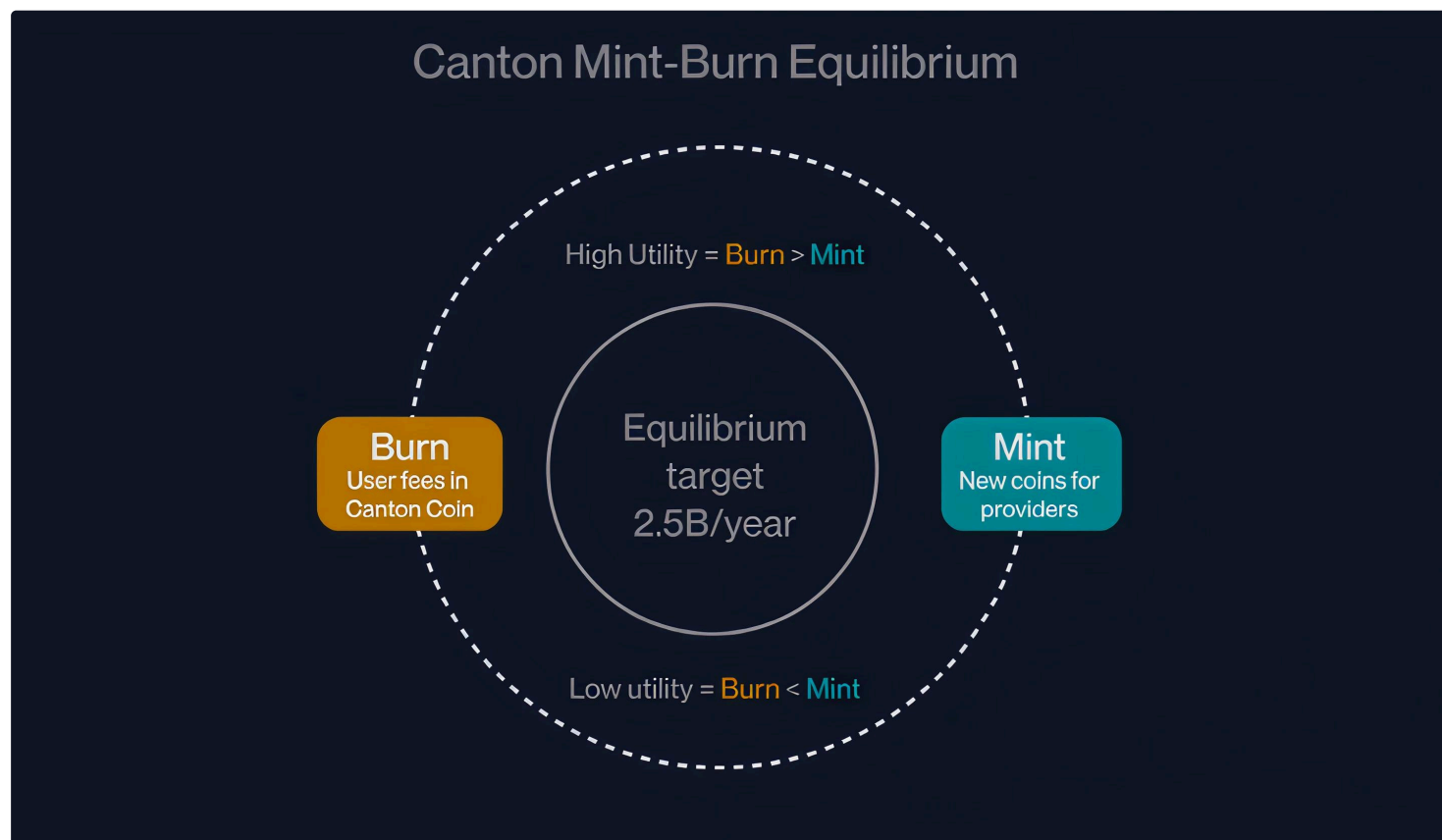


Figure 5: Burn & Mint Equilibrium. Source: [The Role of Canton Coin in the Network](#).

5 Conclusion

Canton gives banks and fintechs the privacy and institutional-grade rails they need for secure, private transactions at scale.

Blockdaemon is actively building out a full suite of infrastructure and security services for institutional participation in the Canton Network.

Blockdaemon's institutional Canton offerings include:

- **Validator Deployment & Management** – Blockdaemon supports turnkey validator setup and ongoing management through the Institutional Vault™.
- **MPC Wallet Integration** – Integration with Blockdaemon's non-custodial MPC wallet, the Institutional Vault™, enables secure key management and policy-enforced transaction workflows tailored for institutional Canton use cases.

Blockdaemon is working toward Super Validator approval, with infrastructure being built to meet the Global Synchronizer's performance and reliability requirements.

Together, these offerings will give financial institutions the tools to operate at the highest level in the Canton ecosystem – with trusted infrastructure, secure key management, and expert support.

If you are launching tokenized repo, private credit, fund tokens, or cross-border payments, Blockdaemon is the shortest, safest route from your compliance needs to Canton's network value. Book a call with Blockdaemon's team of Canton experts for a full, tailored evaluation.