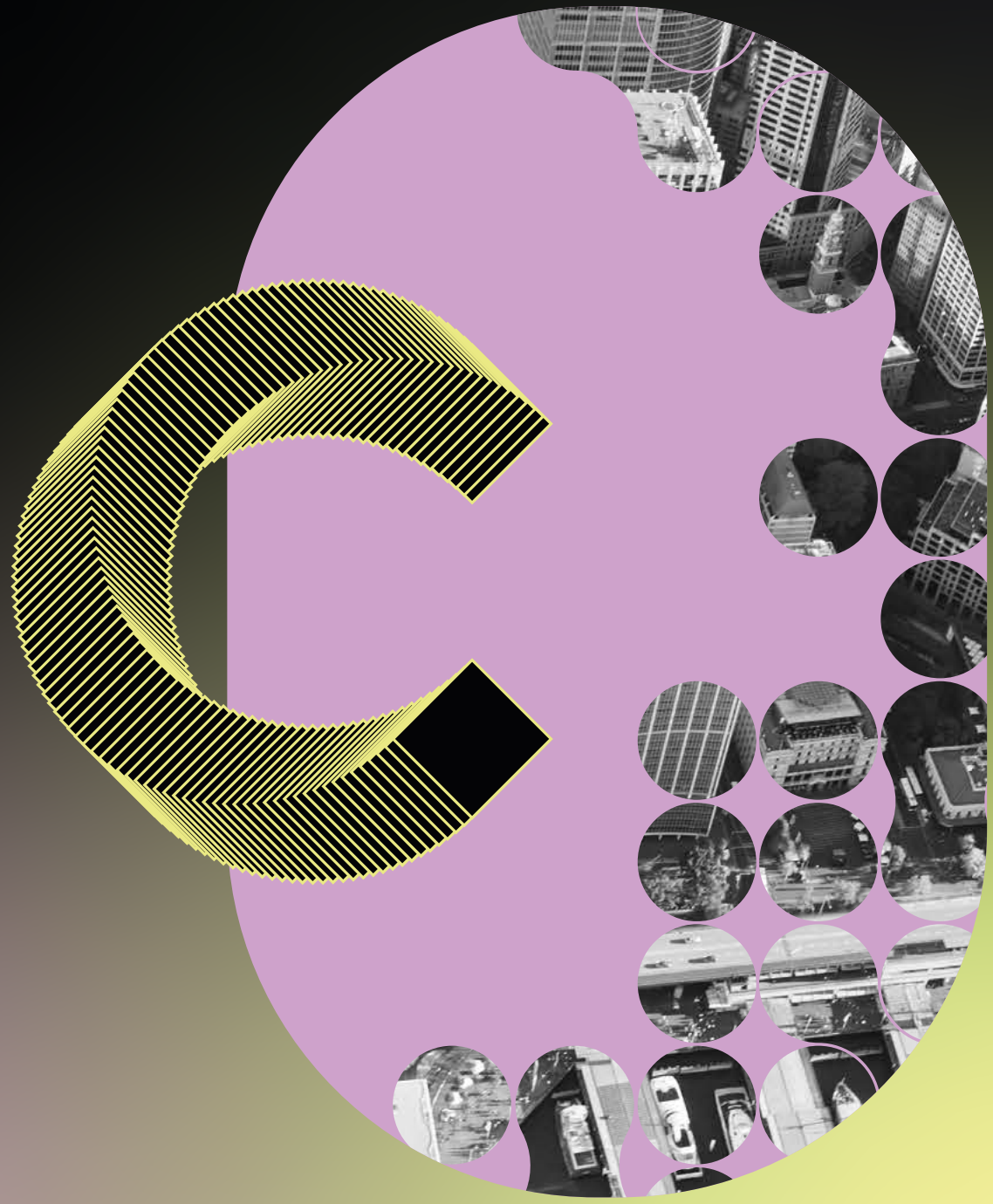
Canton

The Case for Canton

where finance *flows*



Abstract

Canton is the only public, permissionless blockchain with privacy that is proven to work for financial institutions.

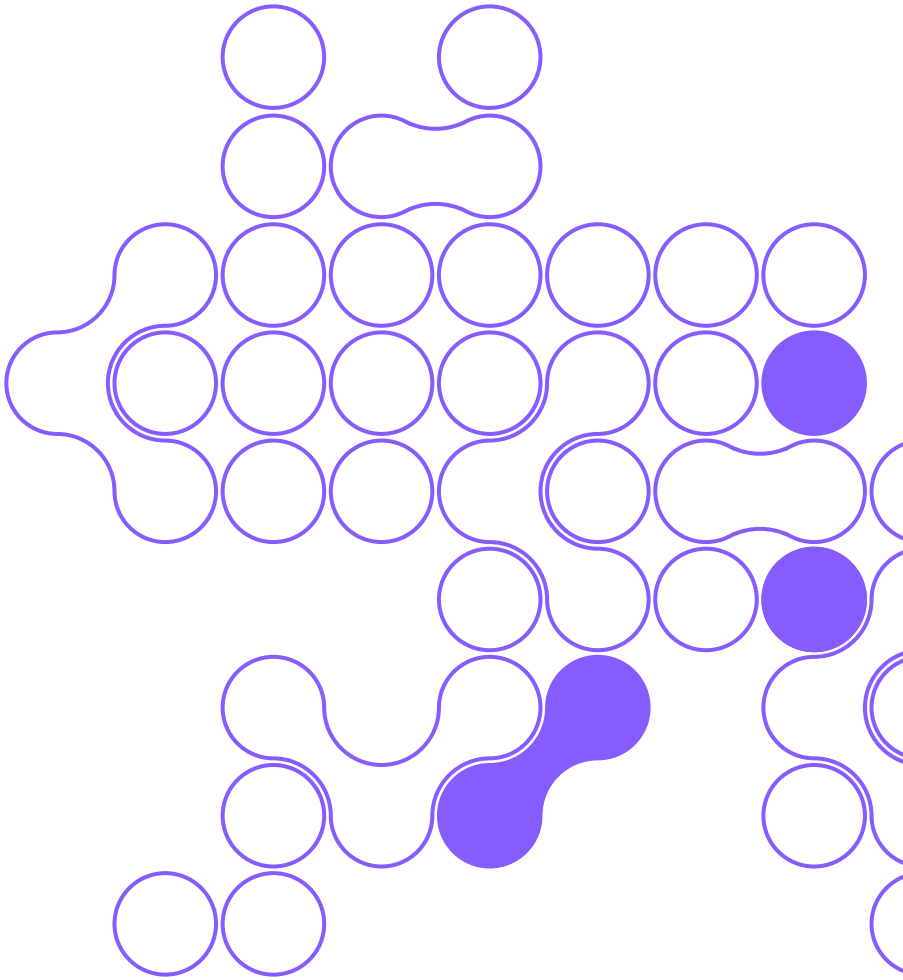
The network is purpose-built to connect independent applications into an interoperable financial ecosystem.

Like the Internet - where public websites and private banking portals can run side by side - Canton provides an open network that lets each application control its own privacy, governance, and compliance.

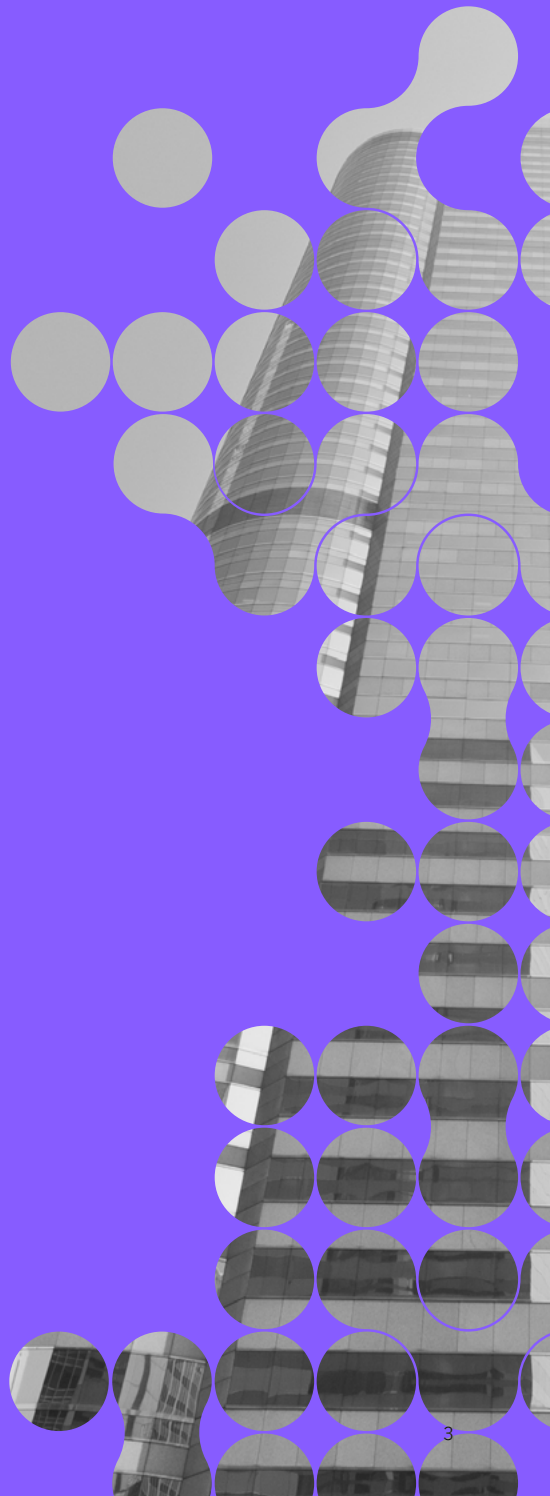
Since the launch of Mainnet in July 2024, Canton has quickly become a preferred path for both financial institutions and crypto-native builders to bring real-world finance on-chain with crypto-style speed and efficiency, without forcing a one-size-fits-all model.

This paper explains:

- The network architecture, covering how independently operated applications and the decentralized Global Synchronizer work together;
- The network's privacy and safety model, proven in live institutional environments;
- Canton Coin (CC): a utility token designed for sustainable, use-based incentives;
- The network's open governance framework, run through Canton Improvement Proposals (CIPs) and stewarded by the Canton Foundation (CF).



Contents



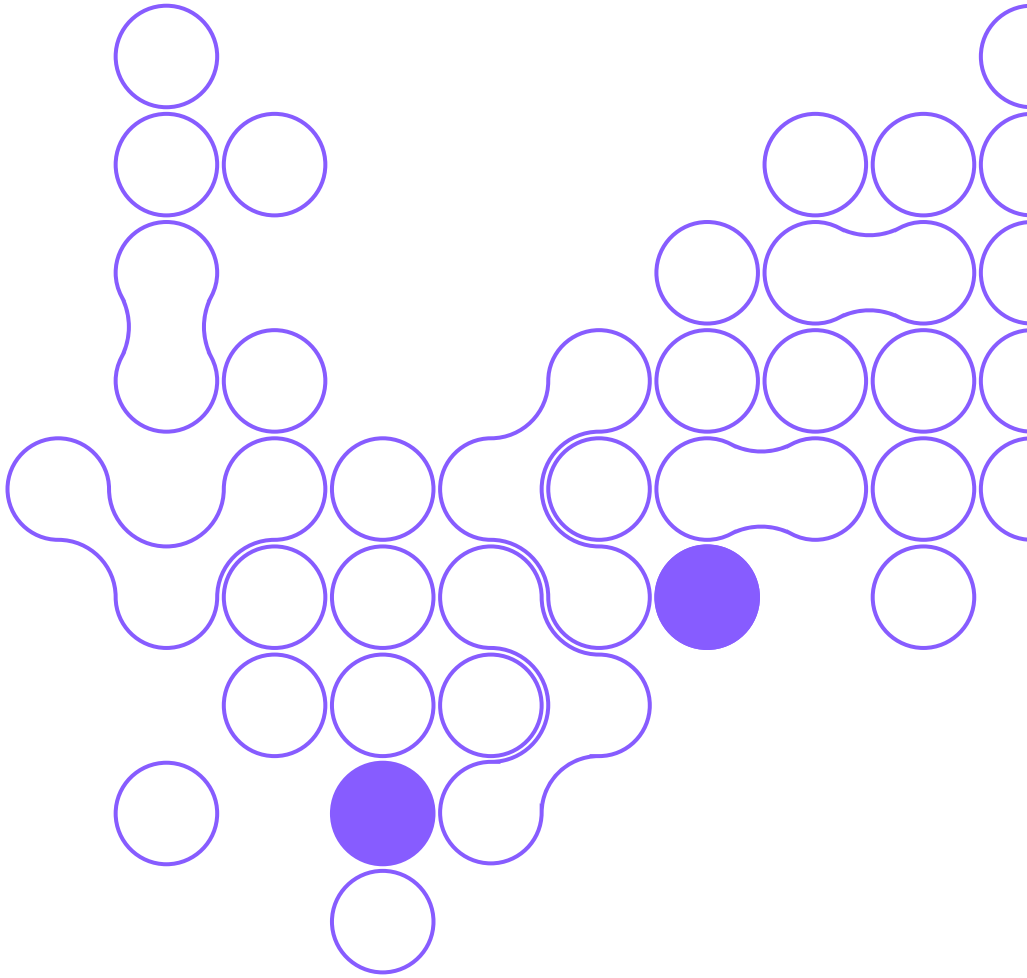
1. Introduction

Public blockchains make it possible for financial applications around the world to connect, but they force every participant to do things in the same way.

Real-world finance needs something more flexible: the ability for different types of applications to connect globally, while choosing their own rules and privacy settings.

Canton reconciles these needs: it is a public, permissionless network that lets anyone build and operate, while allowing each application to choose its own permissioning, data-sharing, and operational policy.

In other words, apps can be permissioned even though the network itself is permissionless - much like launching a permissioned fund on Ethereum does not equate to Ethereum itself being a permissioned network.



2. Design goals

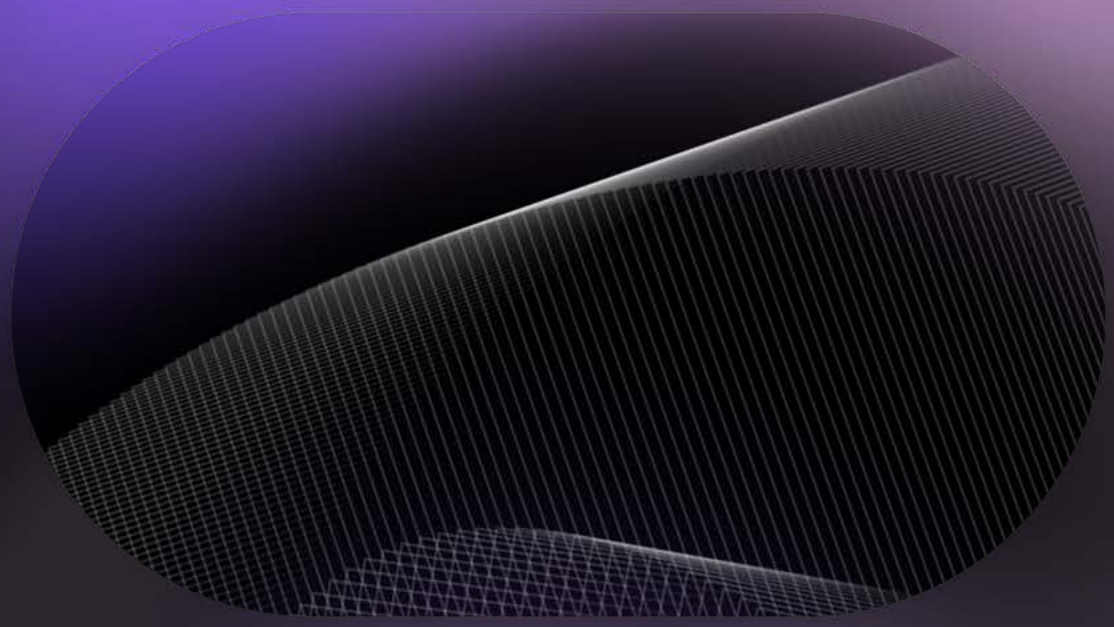
The network's design draws on deep experience implementing Canton at scale with global financial institutions.

It addresses the barriers that have limited institutional adoption of other public networks, where radical transparency and openness create trade-offs in privacy, control, and composability.

At the same time, Canton preserves the asset mobility and composability that define public blockchains. Canton was designed from inception to bust the trade-offs of other networks by combining:

1. **Open participation at the network layer:** Permissionless access to run Validators, build apps, and contribute to governance and proposals.
2. **Configurable transparency and controls at the application layer:** App developers configure who can see what in their applications, and what they can do.
3. **Deterministic cross-application safety:** Atomicity and consistency across independently governed apps and infrastructure.
4. **Independent scaling:** Busy apps don't throttle others; computation and data are partitioned by design. Any user of the network can add network capacity as their app scales.
5. **Sustainable, value-aligned tokenomics:** Token economics that tie issuance and incentives directly to real network activity. The goal: a sustainable and aligned model that supports long-term growth for all participants.

"Canton Network is the proven link between the power of global finance and the real value of blockchain. It's where finance flows - 24/7, atomic, with privacy."



3. Architecture overview

Network of networks

Canton is a protocol that connects many independently operated applications.

Each smart contract application on Canton has its own governance, SLAs, and operating policies.

Applications interoperate atomically across the network, only sharing data between participants on a need-to-know basis.

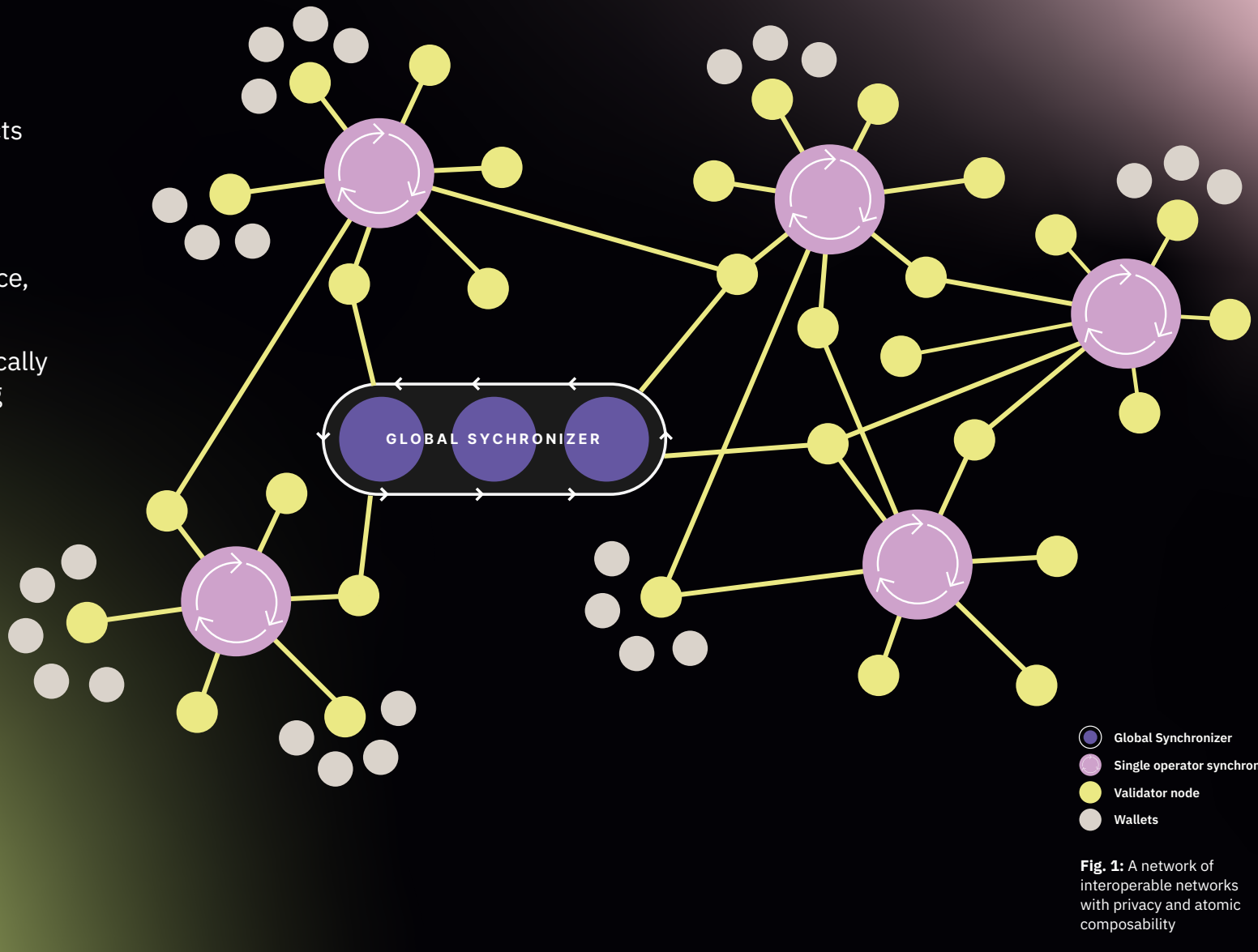


Fig. 1: A network of interoperable networks with privacy and atomic composability

The Global Synchronizer

The Global Synchronizer is a decentralized deployment of the Canton protocol. It time-orders cross-application transactions to keep participants in sync and prevent conflicts. It doesn't replicate data globally; instead, it coordinates proofs between participants, preserving privacy and ensuring everyone reaches the same outcome.

Smart contracts

Applications on Canton are written in Daml, a smart-contract language delivered with three core differentiating attributes:

Data minimization - meaning only the parties who need to see a transaction ever do.

Built-in authorization - where the rules for who can do what are encoded into each contract and enforced by the protocol. Contracts specify who may see, create, exercise, or archive rights. Only parties to a contract (and designated observers) have access to a contract's data; everyone else just sees cryptographic commitments, sufficient for global consistency.

Composable privacy - where two or more apps with different privacy rules can still compose transactions without leaking data across users and apps.

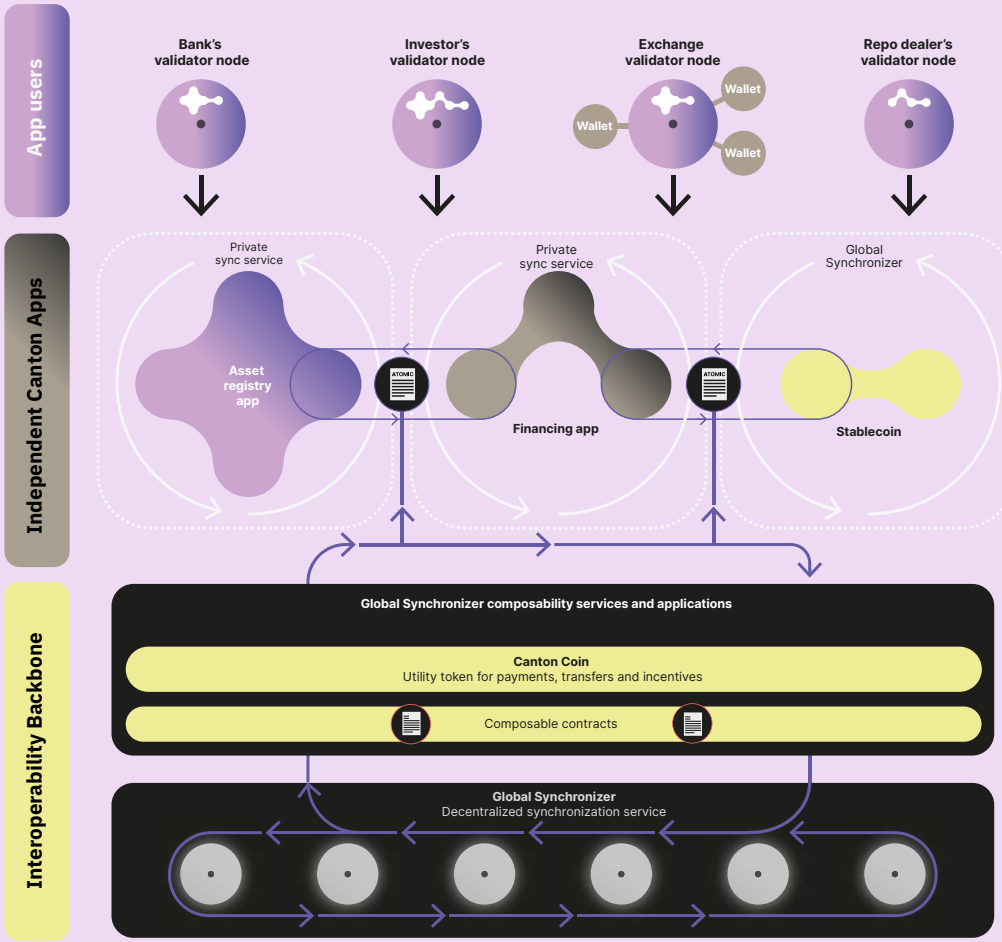


Fig. 2: Canton Network architecture overview

Connect

- One node, multiple apps. Stay in sync. Issue or connect user wallets.
- Your node = your private data.
- Canton Coin rewards for connecting to Global Synchronizer

Build

- Build and run private-permissioned, to public apps.
- Atomic cross-app transactions (via Global Synchronizer or other sync service).
- Continuous rewards and fee-revenue for builders. Global Synchronizer fees paid with Canton Coin.

Run

- Run decentralized infrastructure and network utilities, and participate in governance.
- Extend Canton Network's utility and reach contributing new services.
- Canton Coin incentives for running an node of the Global Synchronizer.

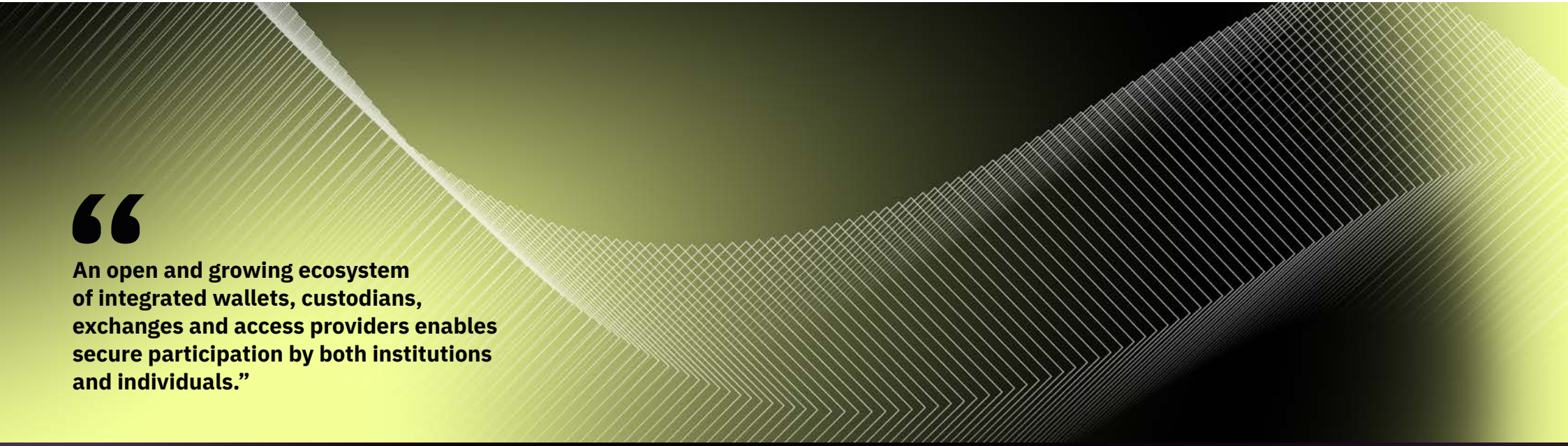
4. Public, permissionless network; selectively permissioned apps

Canton's baseline is public and permissionless: anyone can propose, participate, and operate infrastructure in line with the protocol and its governance. On this open base, apps define their own access and disclosure policies.

A KYC-gated money-market fund and an open-access developer tool can both live on Canton, interoperate when needed, and reveal only what each workflow requires. This separation is the core reason Canton maps cleanly to real-world finance while remaining an open network.

Network decentralization combines distributed consensus with transparent and open governance and access. Validators are distributed globally with no centralized control over consensus.

An open and growing ecosystem of integrated wallets, custodians, exchanges and access providers enables secure participation by both institutions and individuals.



5. Security. Privacy. Safety.

Security means system integrity. transactions can't be forged, changed, or tampered with.

Privacy means only entitled participants can see or act on relevant data, even as workflows span multiple applications.

Safety means transactions finalize atomically and consistently across apps - all at once or not at all - with results that are verifiable and auditable.

Built into Canton from day one, these properties let institutions deliver the real value of **blockchain and tokenization within existing regulatory frameworks**, at scale:

- **Configurable privacy:** Only entitled parties receive, store, and validate plaintext state.
- **Deterministic authorization:** Enforces per-action authorization at the language/ runtime level.
- **Atomic composability across apps:** Cross-application transactions either finalize everywhere, or nowhere.
- **Audit control with selective disclosure:** Applications can provide regulator/auditor access without placing sensitive data on a transparent public ledger, or needing to use complex cryptographic techniques like zero-knowledge proofs.

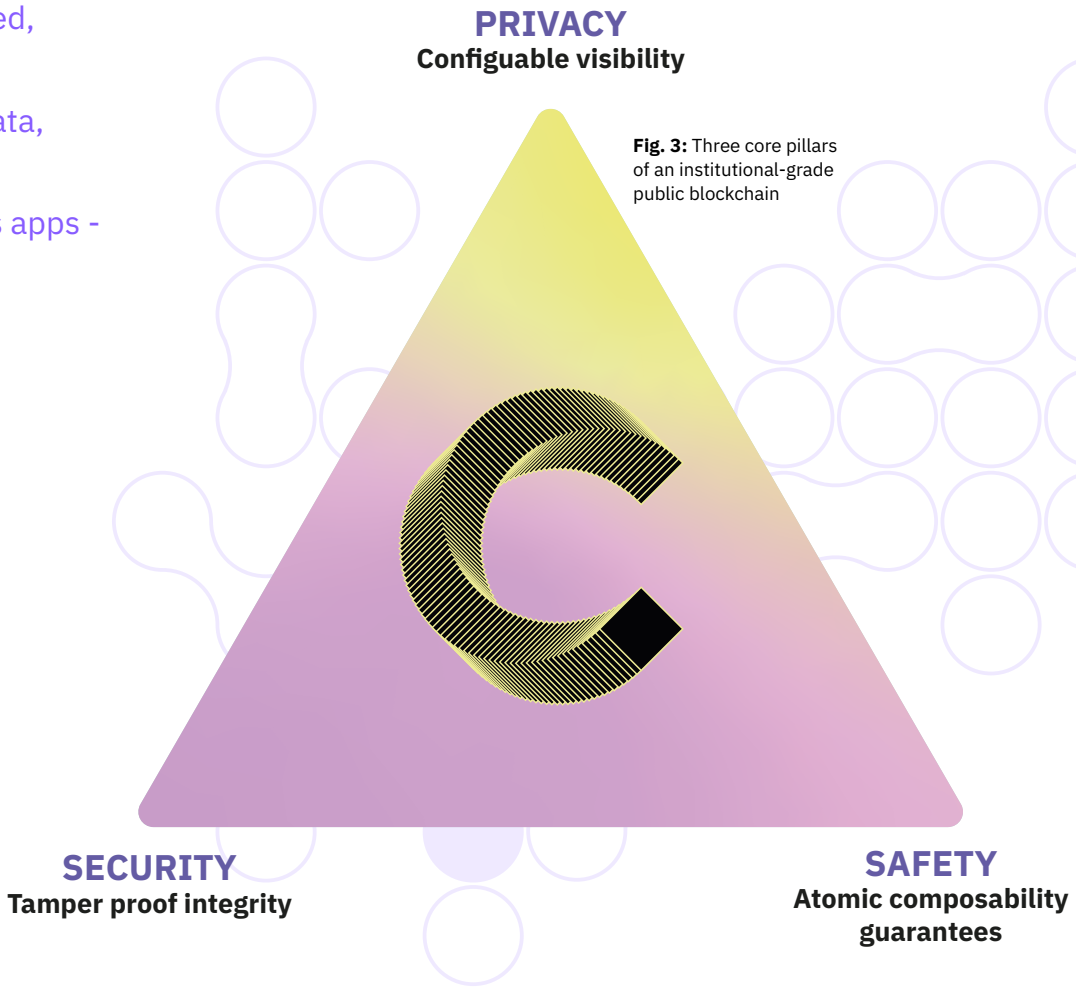


Fig. 3: Three core pillars of an institutional-grade public blockchain

6. Performance and scalability

Unlike conventional blockchains that require every transaction to be processed and agreed across a single global ledger, Canton is designed to scale through independently operated applications that coordinate seamlessly, but only when needed.

Each application maintains its own partitioned state and can deploy its own infrastructure, allowing the network to scale horizontally like the Internet (see Fig. 4).

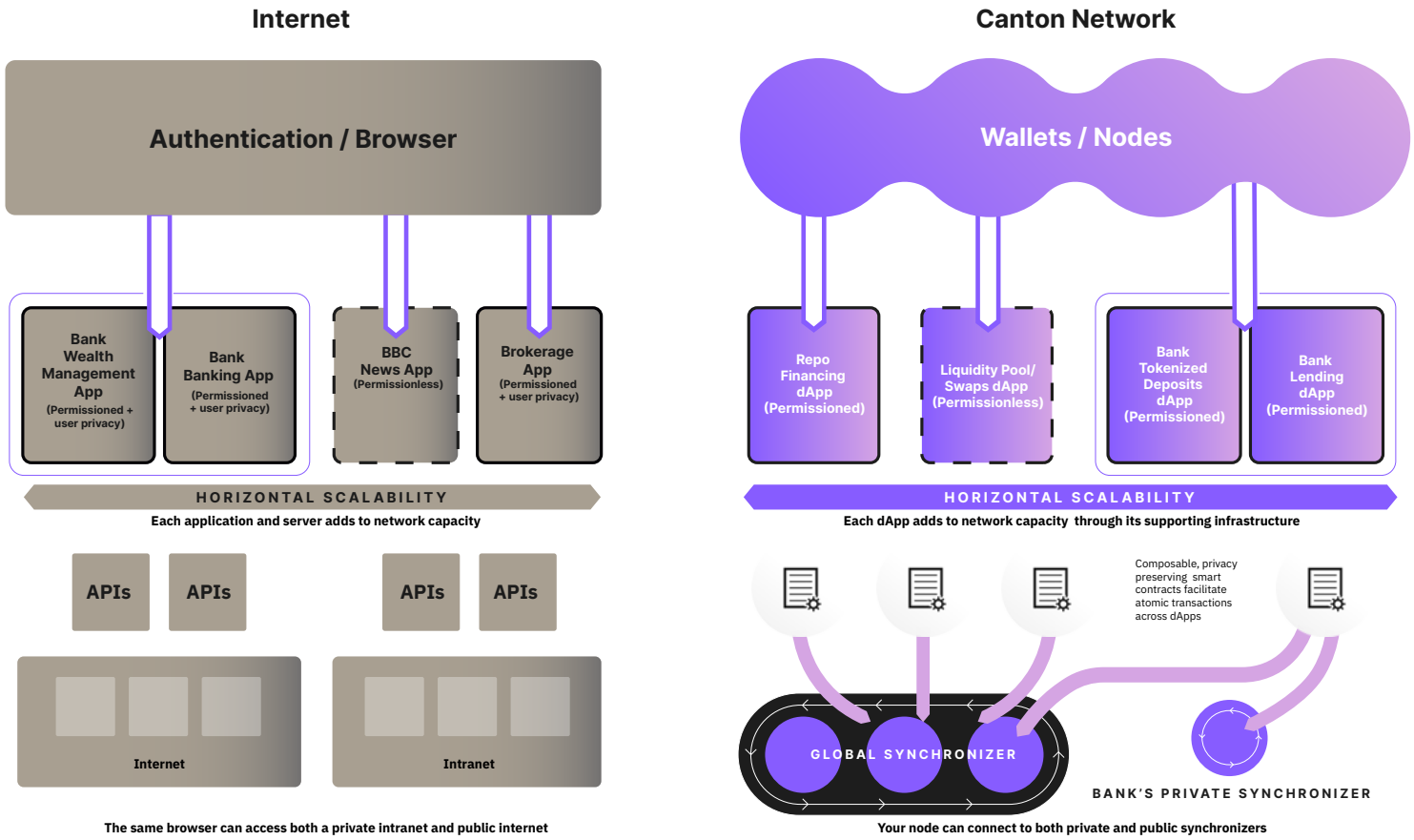


Fig. 4: Like the Internet, Canton delivers a scalable public network, with app operator control

Canton focuses on scaling real-world financial systems, where many entities need to interoperate securely. It enables high-volume applications to run in parallel, while ensuring atomic coordination when they interact. This delivers the performance, predictability, and resilience required, without compromising on privacy or consistency:

Partitioned state

Each application can scale its infrastructure independently; no global state replication across nodes like other public chains.

Independent performance

When running on their own partitions, activity in one application does not contend with others over resources.

Global composability

Apps can dynamically compose transactions across synchronizers. The Global Synchronizer is a decentrally-operated synchronizer enabling any app to get started easily, while allowing applications to scale horizontally by dynamically deploying additional synchronizers as needed.

7. Canton Coin: Continuously rewarding utility

Canton Coin (CC), the network's native utility token, was designed to reward real network use and activity rather than speculation.

It aligns the success of the network with the participants who drive it forward, fairly rewarding application builders and users, as well as those operating decentralized infrastructure.

The result is a fundamentally different economic model where rewards flow to those creating value through real activity, not only to validators or early investors.

> **"For builders it aligns incentives in a model where every app builder benefits from the network's growth."**

Canton's tokenomics sidestep the pitfalls seen in earlier networks:

No pre-mine, no VC allocations:
Every token in circulation has been earned by delivering utility.

Burn-and-mint equilibrium:
Usage fees are burned, and new coins are minted based on participation. This keeps supply responsive to demand and ties value to network usage. (see Fig. 6 in the appendix)

Enterprise-grade transparency:
Even though transactions on Canton are private by default, reward distributions and Canton Coin fees are public, providing insight into what apps are driving value, without compromising user privacy.

The economics are designed to support a sustainable application ecosystem rather than an extractive validator-centric network. Over the first ten years, two-thirds of network rewards are allocated to application providers, divided up based on the relative network activity each application generates (See Fig. 5). This creates a continuous, fee-based revenue mechanism where increased app usage drives greater rewards. For builders, it represents a powerful alignment of incentives - a model in which every application benefits from the network's growth, and contributes to it in return.

As more assets, workflows, and users engage and transact across different apps, demand for synchronization capacity through the Global Synchronizer rises. CC is the unit that meters and rewards that capacity.

The goal is use-driven value: network usefulness precedes token value, not the other way around. Continue reading in the Appendix for a more detailed breakdown.

The Role of Canton Coin (CC)

As the permissionless, native utility token of Canton Network, CC is used to pay for and reward the services that keep the network coherent:

Application incentives: Apps that drive onchain activity receive rewards proportional to the fees they generate on the Global Synchronizer.

Synchronization fees: Synchronizer capacity is paid for in CC.

Infrastructure rewards: Super Validators earn CC for providing global ordering services and validating CC transactions.

Validator rewards: Validators earn CC for validating transactions on the smart contracts they are party to and for verifying their 'liveness'.

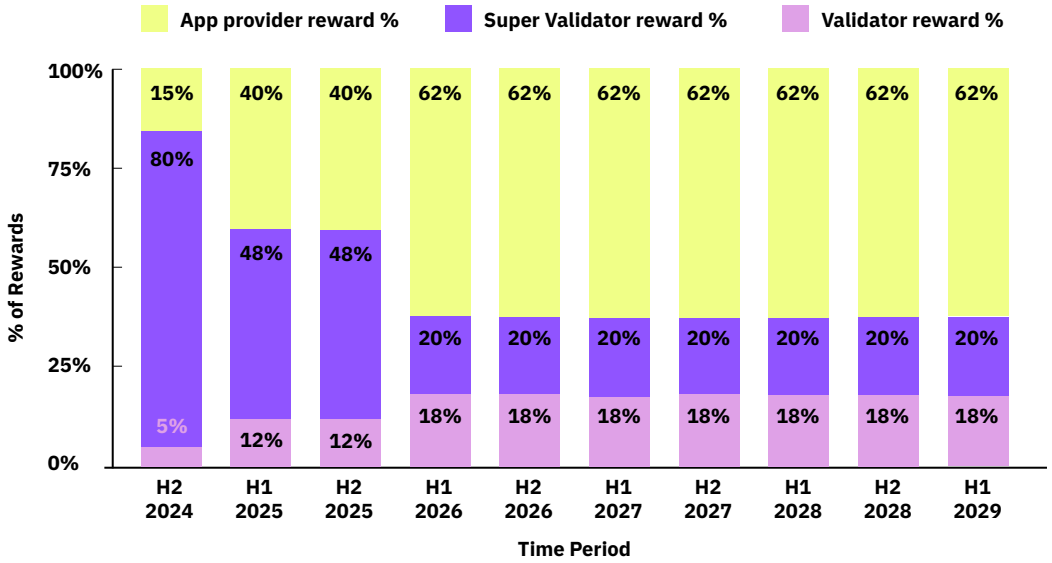


Fig. 5: Incentivising network utility: Canton Coin reward splits evolve over time

8. Open governance: The Canton Foundation and CIPs

The Canton Foundation (CF) stewards the network's evolution and incentive design, ensuring Canton remains open, neutral, and aligned with the needs of its participants.

Protocol and ecosystem changes are proposed through Canton Improvement Proposals (CIPs), a transparent process for introducing upgrades to tokenomics, configuration standards, and ecosystem programs.

Super Validators and the broader community participate in reviewing, testing, and adopting these proposals, with changes requiring approval and deployment by two-thirds of Super Validators.

The Foundation's membership reflects the unique diversity of the Canton ecosystem, spanning traditional and decentralized finance. It includes leading global banks such as Goldman Sachs and BNP Paribas, major financial market infrastructures including Euroclear and Tradeweb, and institutional crypto pioneers like Kaiko, Circle, and Chainlink. This mix ensures the Canton Network is governed by those building, operating, and using it - harmonizing TradFi and DeFi under a shared, transparent governance model.

“The Foundation's membership reflects the unique diversity of the Canton ecosystem, spanning traditional and decentralized finance”

9. Developer experience

Building on Canton is open and accessible, with continuous enhancements to developer experience and a rapidly growing community of contributors. Daml and Canton are open source, allowing anyone to build applications using transparent standards and shared tooling.

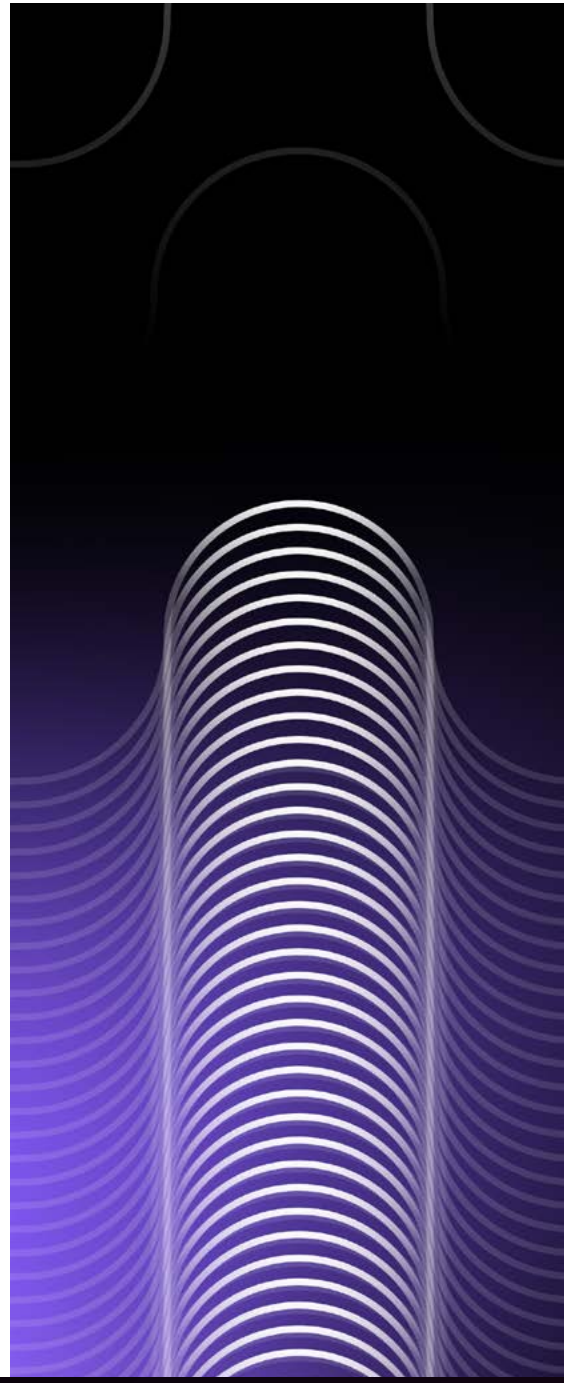
Daml's declarative design, concise syntax, and strong type system reduce code complexity and ambiguity, lowering the risk of smart contract errors. Its deterministic execution and built-in authorization model make applications safer and easier to verify - key requirements for builders across financial markets. Builders can spin up a Localnet to speed up development in an isolated environment, and then battle-harden applications on Canton's Testnet before moving to production.

Familiar paradigms:
Daml models contracts, rights, and workflows directly, making it well-suited for complex financial agreements.

Composable with independent control:
Developers can interact with other apps' interfaces and settle across domains without coupling strongly between application implementations.

Deployment flexibility:
Build permissionless or permissioned experiences, with optional SLAs and domain-level performance tuning.

Proven maturity:
Canton applications have operated in production with global financial institutions since 2020. The SDK and node infrastructure include enterprise-grade capabilities for supportability, observability, and integration, ensuring reliability and resiliency at scale.



10. The privacy and composability unlock: Workflows in production

Privacy and composability together make Canton work at scale for real financial markets. Other public networks force a choice between privacy controls and interoperability, either exposing sensitive data or limiting how assets can interact. Canton eliminates that trade-off.

Its configurable privacy model and cross-application atomic smart contract composability allow institutions to connect workflows and move assets across applications, without revealing confidential positions or counterparties.

This combination is unlocking high-value use cases that are impossible to securely implement on other public blockchains today - from private stablecoin payments, to 24/7 composable collateral and financing across financial markets:

1

Stablecoins with privacy: Privacy-enabled stablecoins that enable stablecoin providers to expand beyond early product-market fit, into institutional-grade use cases; from treasury and B2B payments, to securities settlement and collateral mobility.

2

Collateral mobility and 24/7 financing: Round-the-clock collateral movement and composability, without market-wide data leakage. Supported by instant creation and redemption of stablecoins and high-quality collateral assets such as onchain U.S. Treasuries.

3

Privacy layer for Bitcoin: Bridged, wrapped, or staked Bitcoin that can move privately and be used as collateral or liquidity within institutional workflows. This opens up the potential for Bitcoin holders to put BTC to work in higher-yielding markets and liquidity pools and expand use into repo, secured lending and structured financing in the future - all without exposing sensitive positions or counterparties.

> **This combination is unlocking high-value use cases that are impossible to securely implement on other public blockchains today**

11. How to evaluate Canton as a builder

Assess how privacy and compliance can expand your market

Canton supports compliant workflows with built-in privacy, enabling large-scale use cases in onchain payments, collateral mobility, institutional-grade Bitcoin, and more. Builders can design applications that meet institutional privacy and regulatory standards while maintaining the openness and composability of a public network.

Consider how privacy unlocks new categories of users, partners, and assets that other public chains can't support.

Evaluate the revenue potential of built-in app rewards

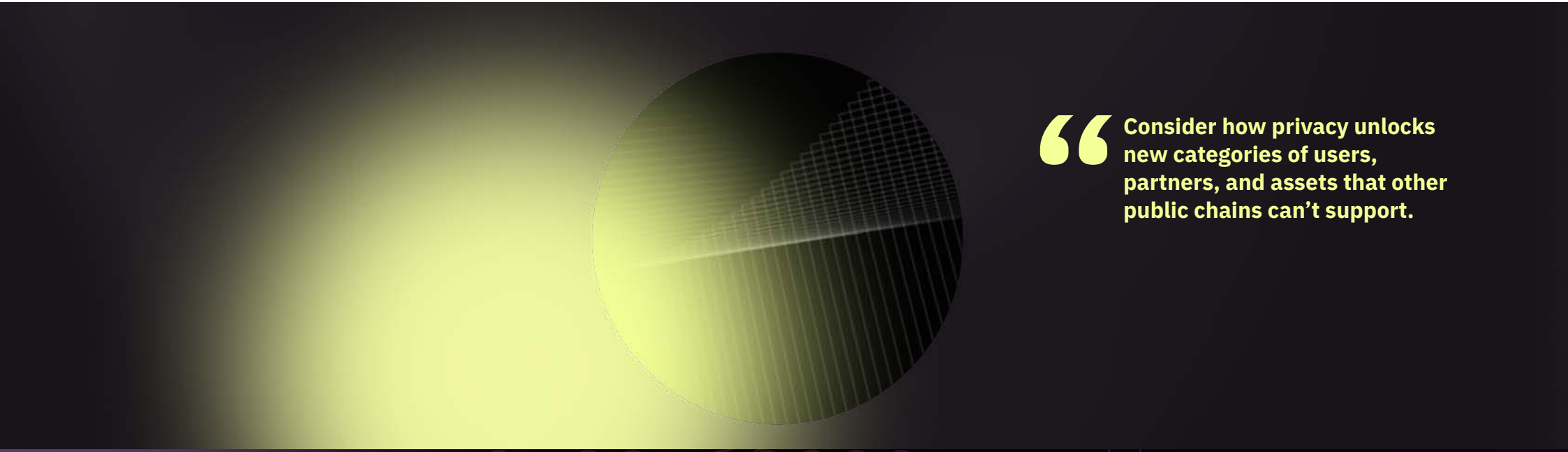
Applications receive a share of network fees every block, creating a sustainable, usage-based revenue model. This makes Canton ideal for stablecoins, wrapped crypto assets, tokenized securities, and other applications that benefit from native, per-transaction economics tied to real network activity.

Builders should model how onchain usage could translate into continuous, fee-based revenue streams for their applications.

Explore ecosystem access and integration opportunities

Canton brings together a broad ecosystem spanning crypto-native builders and global financial institutions. Builders gain access to deep liquidity, differentiated partners, and new distribution channels across both TradFi and crypto-capital markets.

Evaluate how connecting to this network could amplify your distribution, accelerate adoption, and expand your role in the broader onchain financial ecosystem.



“Consider how privacy unlocks new categories of users, partners, and assets that other public chains can't support.

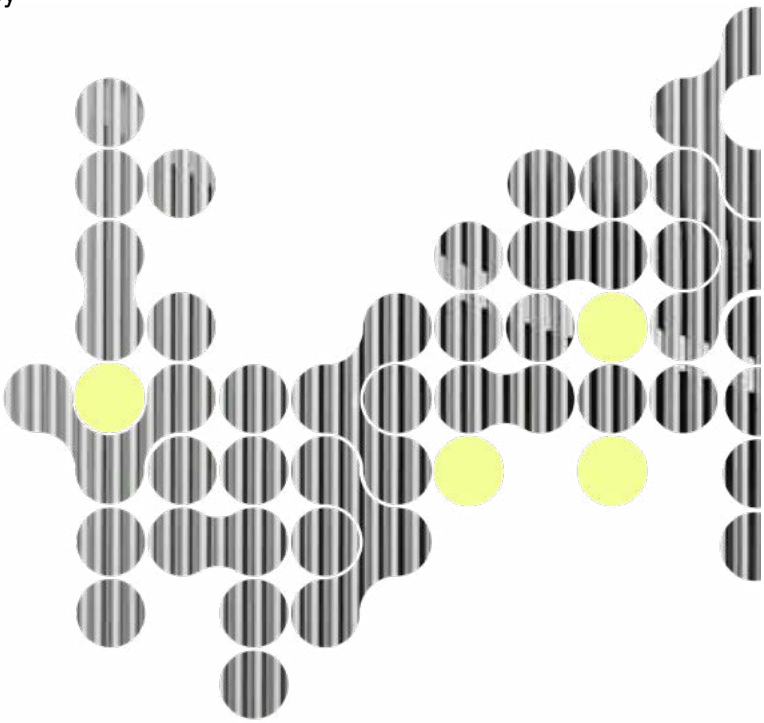
12. Conclusion

Canton's thesis is simple: public, permissionless coordination at the network layer and configurable permissioning at the application layer. This separation allows regulated finance and crypto-native builders to share a common fabric without compromising on their core requirements and threshold issues like control over privacy.

Canton Coin (CC) continuously rewards those who take advantage of the network's secure, private, cross-application synchronization - aligning long-term value with genuine adoption.

For application builders, this creates a unique flywheel of opportunity: as applications generate more onchain activity, they earn a proportional share of network rewards, creating a sustainable, usage-based revenue model built directly into the protocol.

As onchain finance accelerates at capital markets scale, Canton provides the neutral, open infrastructure where institutional workflows and crypto composability finally converge.



Appendix

A. CC Issuance Curve

Canton Coin (CC) supply follows a *declining issuance curve* designed to reward early contributors while trending toward long-term sustainability.

Issuance started high to bootstrap Validator participation and app development, then *halves periodically* to balance inflation and burn.

Over time, the share of new issuance *shifts from Super Validators (SVs)* to *Validators (Vs)* to *Applications (Apps)* as network maturity increases

Phase (Years)	Minting Rate (CC / year)	Phase Total Minted (CC)	Apps Share	Validators Share	Super Validators Share
0 – 0.5	40 B / yr	20 B	15%	5%	80%
0.5 – 1.5	20 B / yr	20 B	40%	12%	48%
1.5 – 5	10 B / yr	35 B	62%	18%	20%
5 – 10	5 B / yr	25 B	69%	21%	10%
Cumulative (0–10 yrs)	—	100 B total	≈ 50%	≈ 15%	≈ 35%
> 10	2.5 B / yr (steady state)	—	75%	20%	5%

B. Global Synchronizer Fees

Fee purpose: Users pay to have a transaction transmitted and finalized across the Global Synchronizer.

Fee basis: Fees are set in $ / MB terms, representing the dollar cost per megabyte of data transmitted.

Settlement: The onchain CC ↔ USD conversion rate determines how much CC must be burned for each transaction. Users burn that CC to have their transactions processed and finalized.

This structure directly links network usage to token supply. Higher throughput requires more CC to be burned, reducing CC supply and aligning economic value with real transaction volume.

C. Burn / Mint Equilibrium (BME)

BME is the dynamic balance between fixed, dollar-denominated fees and a floating CC market price against a known issuance curve.

Known supply curve: Minting follows the schedule in Appendix A.

Fees fixed in $ terms: Users pay a set $ / MB for transactions that use the Global Synchronizer.

Quantity of CC burned depends on market price: Users pay for network fees by burning the $USD equivalent of CC amount at the onchain conversion rate.

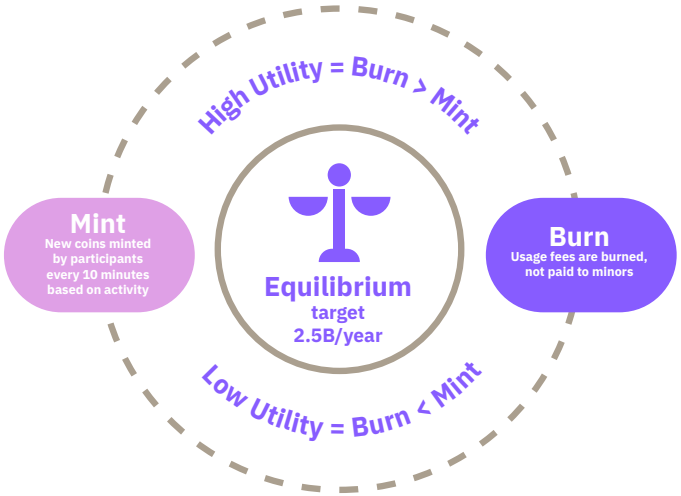
Dynamics

If *price is too high* relative to on-chain activity, then *mint > burn* (net inflation), creating downward pressure on price.

If *price is too low* relative to activity, then *burn > mint* (net deflation), creating upward pressure on price.

Over time, the system seeks an equilibrium where long-run net supply change approaches zero. Because equilibrium can occur at different price/activity combinations, the ultimate total CC supply is not predetermined.

Fig 6: Canton's burn-mint equilibrium targets long-term economic sustainability.



D. Further reading:

Canton privacy and architecture:
Canton Network: Technical primer (blog)
How privacy works on Canton (blog)
The privacy imperative for stablecoin payments - The Tie (Report)

Tokenomics:
Canton Coin - rewarding utility (Blog)
The role of Canton Coin in Canton Network - The Tie (Report)
Cantonomics for App Builders (Blog)
Flipping the script on tokenomics (Blog)
Canton Coin: How should we think about FDV?

Third party reports and case studies:
Lightshift - An independent overview of Canton Network
Coinmetrics - Canton Coin Analyst Report
Dfns - state of Canton (Gated report)

Deep dive whitepapers here:
Canton Network Whitepaper
Canton Tokenomics Whitepaper
Canton Coin MiCA Whitepaper
Canton Evolution to Multi-language Support Whitepaper
Canton Protocol Whitepaper

Canton

The Canton Network is the only public, permissionless blockchain purpose-built for institutional finance—uniquely combining privacy, compliance, and scalability. Governed by the Canton Foundation with participation from leading global financial institutions, Canton enables real-time, secure synchronization and settlement across multiple asset classes on a shared, interoperable infrastructure. The open-sourced network is powered by its native token, Canton Coin, and supports decentralized governance and collaborative application development. It's the proven link between the promise of blockchain and the power of global finance, enabling finance to flow as it should.

Follow us

www.canton.network

info@canton.network