THE CANTON NETWORK SERIES

PART 1 OF 5

Transforming Real-World Assets Through Compliant Tokenization and a Mobility-Focused Network Infrastructure

Canton

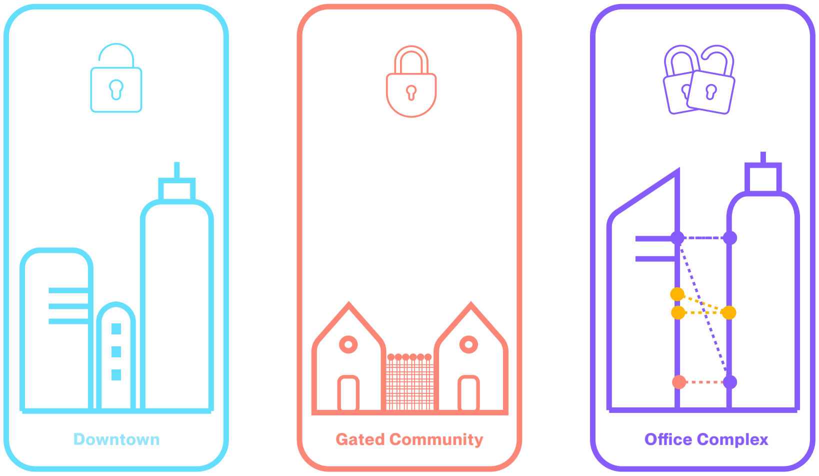
Presented by The Tie

The world of digital assets is growing fast, with the Boston Consulting Group predicting asset tokenization of illiquid assets like real estate, land, commodities, and more will reach $16 trillion by 2030.

As more and more companies offer tokenized Real-World Assets (RWAs), they must be careful to fit within the framework of regulators. However, making these assets fit all the ever-evolving regulations banks follow takes a lot of work.

INTRODUCTION

The Basel Committee on Banking Supervision, which sets standards for banks in over 100 countries has made it clear that the choice of blockchain network is crucial for tokenizing traditional assets. To realize the benefits of tokenization, without incurring punitive capital charges, banks must use networks with appropriate controls and features. This is a significant challenge that providers of tokenized financial products and so called RWAs, like commodities and real estate, must address to enable growth in the sector. Simply put, tokenized RWA providers must choose the right network that aligns with regulatory requirements.



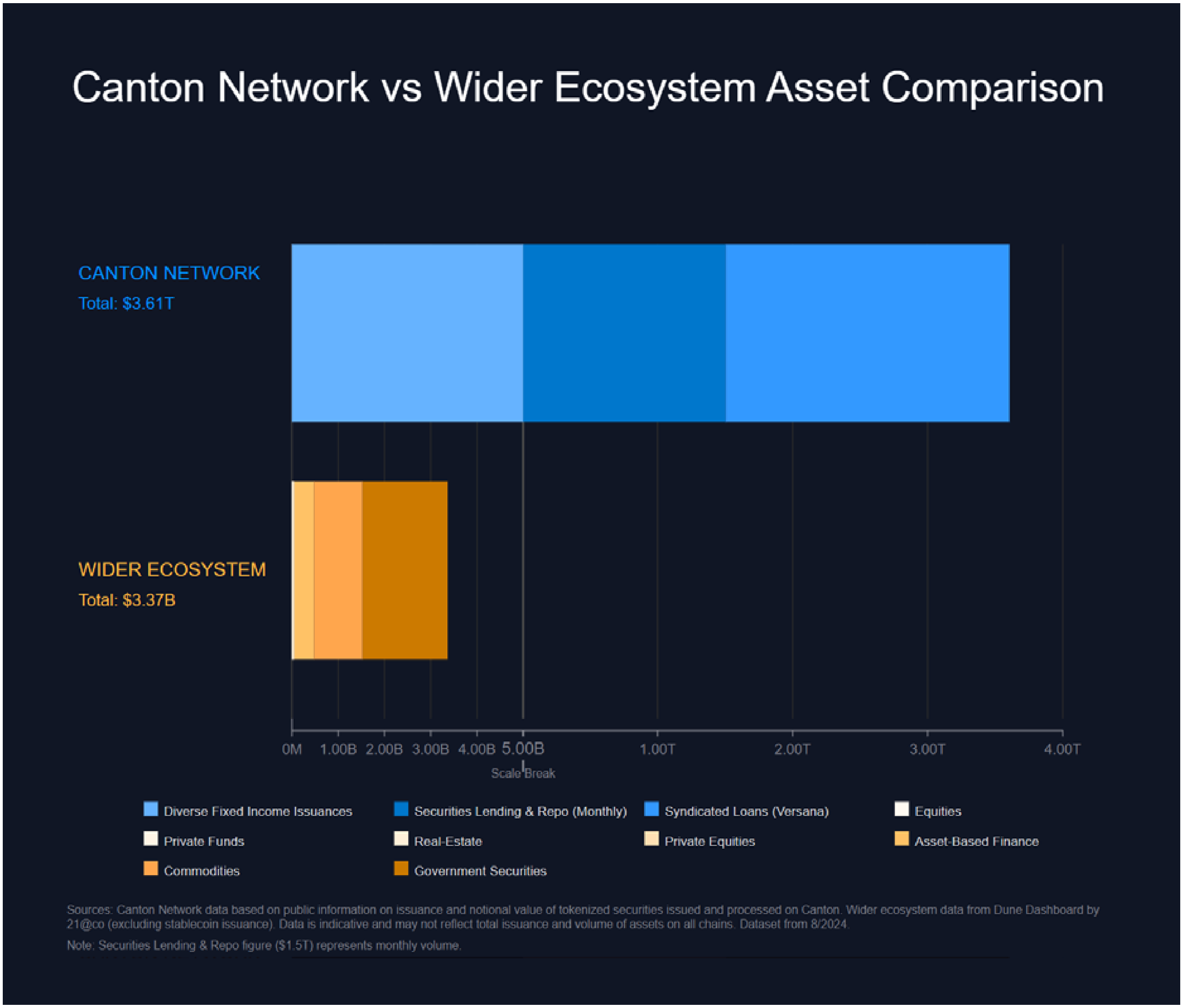
PUBLIC PERMISSIONLESS

PRIVATE PERMISSIONED

PUBLIC PERMISSIONED

Blockchain technology offers a compelling solution for digitizing and managing RWAs by eliminating the need for time-consuming reconciliation processes between multiple parties that cause delays and tie up assets and capital. It enables precise and risk-free value transfer through synchronized, shared ledgers. To realize the full benefits of tokenized traditional RWAs while operating within the bounds of today's regulatory guardrails, we need a combination of the tight controls provided by private networks and the interoperability and synchronicity of systems and transactions offered by public networks like Ethereum.

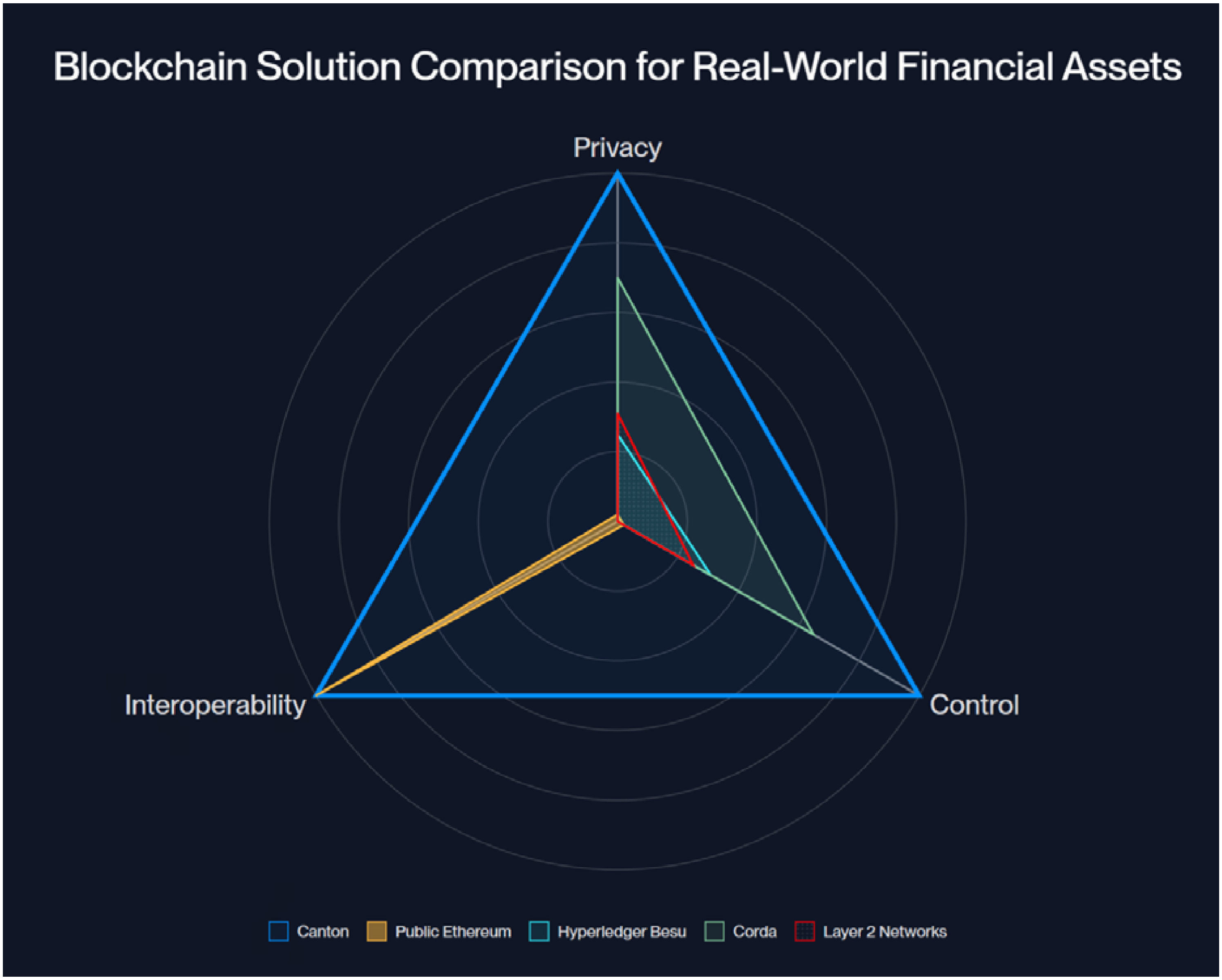
The Canton Network tries to do just that. It gives application makers tight controls to satisfy regulators while also offering the benefits of an open network, which app makers and participants need to successfully build their businesses.



Canton Network vs Wider Ecosystem Asset Comparison

Sources: Canton Network data based on public information on issuance and notional value of tokenized securities issued and processed on Canton. Wider ecosystem data from Dune Dashboard by 21@co (excluding stablecoin issuance). Data is indicative and may not reflect total issuance and volume of assets on all chains. Dataset from 8/2024.

Note: Securities Lending & Repo figure ($1.5T) represents monthly volume.


Blockchain Solution Comparison for Real-World Financial Assets
Privacy
Interoperability
Control
Canton
Public Ethereum
Hyperledger Besu
Corda
Layer 2 Networks

For banks and other regulated companies to bring traditional assets onto the blockchain and move them around efficiently, we need to combine the openness of networks like Ethereum with the control of private, permissioned networks. This blend is essential for following rules about money laundering, maintaining control over operations, and data visibility. All of this affects how assets are classified under Basel's rules according to their soundness and perceived risks.

The Basel Committee, which sets global banking standards for banks in over 100 countries worldwide, issued a standard in December 2022 that categorizes tokenized assets into two groups:

i. Group I — This includes tokenized traditional assets (Group 1a) and crypto-assets with effective stabilization mechanisms, such as stablecoins (Group 1b). The capital requirements for this group are based on the risks of the underlying asset, assuming the underlying network provides the appropriate levels of permissioning and control.

ii. Group II — Unbacked assets like Bitcoin don't meet the standard. They are severely penalized with up to 1250% risk weighting, based on the fact they are issued on permissionless blockchain networks.

Networks that want to attract regulated companies and/or assets within the purview of today's regulators try to solve the regulation problem by creating private networks with extensive access control either with private blockchains, or forks of public permissionless blockchains with additional privacy and permissioning mechanisms. But both of these solutions have issues.

Private networks don't offer the ability to deliver high-fidelity interoperability with other networks. Each private network is siloed and thus fails to fully unlock the connectivity potential of tokenized assets, data, and cash. Furthermore, their privacy controls often do not satisfy regulatory standards for banks and other institutions, allowing participants who are allowed on the network the ability to see everything that is happening within that private network or channel.

To get the full benefits of tokenization, digital asset networks need to connect in a way that delivers the same synchronicity across applications and blockchain infrastructure as within a private network. Connectivity should not be at the expense of control. On the internet, if you create applications, you expect to have full control over how your application or website operates and who can access it while relying on the common infrastructure underneath to connect across applications when required and agreed upon.

Blockchain should be no different. App makers shouldn't have to make a trade-off between control over their apps and network, how it operates, and the ability to seamlessly transact with other useful assets or applications to unlock efficiencies or new opportunities.

The Canton Network is fundamentally designed to work within existing regulatory frameworks rather than trying to solve for regulations as an afterthought. Compliance is not a band-aid solution or a patch applied to the network; it is an integral part of Canton's architecture from the ground up.

Regulators expect financial institutions to maintain control over their business operations, and Canton enables this control while still providing the benefits of a more automated, synchronized, and decentralized system. With Canton, institutions don't have to sacrifice their sovereignty over how they do business to leverage the advantages of blockchain technology.

Canton's compliance-centric design is evident in several key aspects:

Privacy: Canton uses a smart contract language called Daml, which allows for granular control over who can see data. Transactions are encrypted, and data is only shared on a need-to-know basis. Each app maker can define exact data permissions, ensuring they follow privacy rules like GDPR. Canton then synchronizes contract execution across stakeholders on a strict need-to-know basis so parties only ever see what they are entitled to see.

Control: Canton is built from the ground up to work within existing regulatory frameworks. Unlike other blockchains, it provides the necessary controls regulators require over validator nodes, network access, and data privacy. This allows tokenized assets on Canton to keep their regulatory status and avoid significant capital risk weightings.

Interoperability: Canton provides the rails to connect independent blockchain applications and financial systems, allowing them to work together seamlessly. This means tokenized assets can be directly moved and traded across different institutions and platforms without losing control or privacy or introducing some kind of third-party bridge.

Scalability: Canton is designed to enable a "network of networks," similar to the Internet. Each app maker has complete control over their own app, infrastructure, and data. Like the Internet, which scales with each new network switch and server added, Canton scales as more apps and nodes are added, growing network capacity and processing power without hurting performance or security.

By addressing these key aspects, Canton enables financial institutions to unlock the benefits of blockchain and asset tokenization without having to change the regulatory rule book. This has made it an attractive solution for those looking to innovate responsibly in the world of digital assets without being held back by regulatory uncertainties and changes.

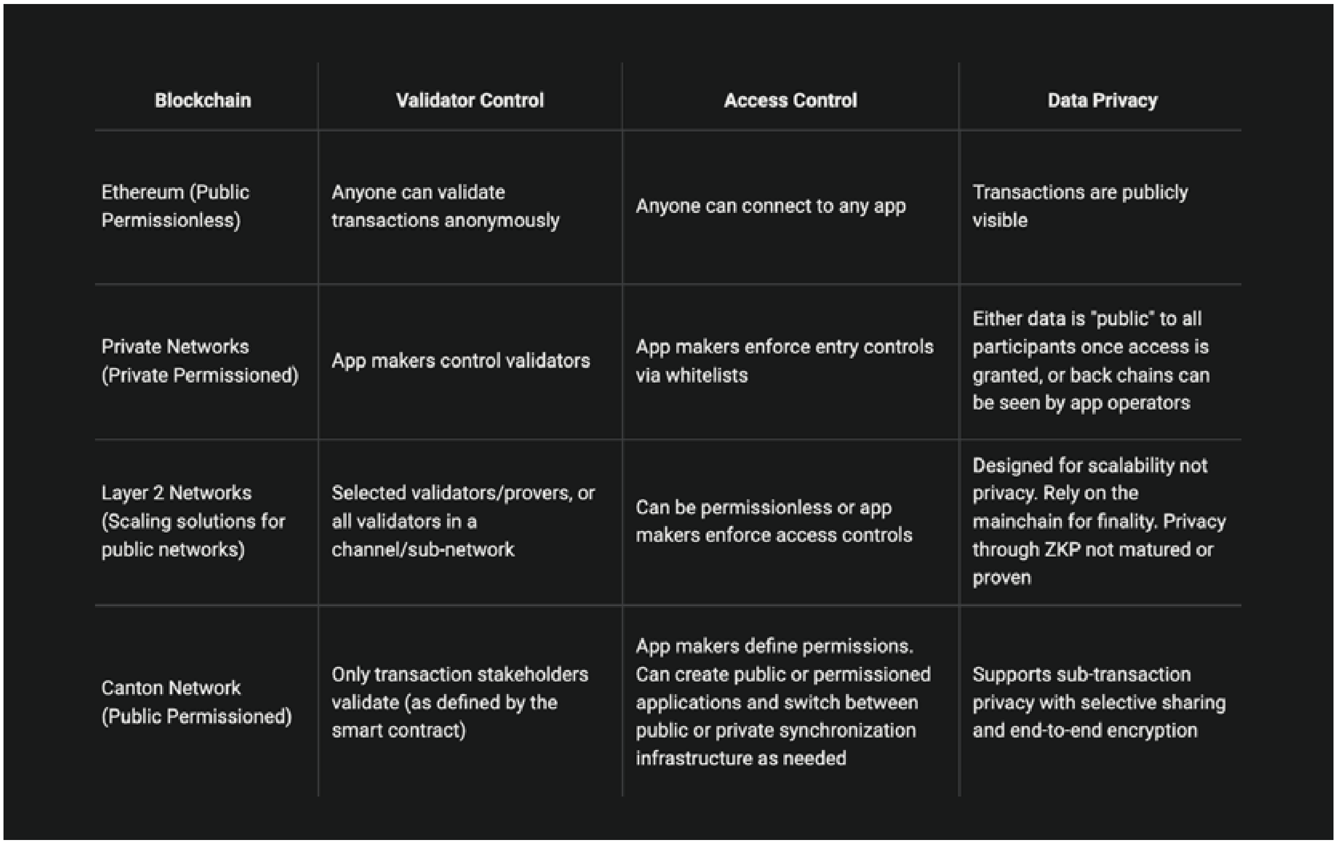
COMPARING DIFFERENT BLOCKCHAINS WITHIN THE CONTEXT OF THE BASEL STANDARD

To illustrate how different blockchains fall within the Basel ‘22 Standard, we will examine Ethereum, Private Networks, Layer 2 Networks, and Canton through three key factors:

i. Validator Control: Who secures the network and validates transactions to the app.

ii. Access Control: Who can connect to the network.

iii. Data Privacy: Who can read data from the network.



Blockchain	Validator Control	Access Control	Data Privacy
Ethereum (Public Permissionless)	Anyone can validate transactions anonymously	Anyone can connect to any app	Transactions are publicly visible
Private Networks (Private Permissioned)	App makers control validators	App makers enforce entry controls via whitelists	Either data is "public" to all participants once access is granted, or back chains can be seen by app operators
Layer 2 Networks (Scaling solutions for public networks)	Selected validators/provers, or all validators in a channel/sub-network	Can be permissionless or app makers enforce access controls	Designed for scalability not privacy. Rely on the mainchain for finality. Privacy through ZKP not matured or proven
Canton Network (Public Permissioned)	Only transaction stakeholders validate (as defined by the smart contract)	App makers define permissions. Can create public or permissioned applications and switch between public or private synchronization infrastructure as needed	Supports sub-transaction privacy with selective sharing and end-to-end encryption

1. Ethereum (Public Permissionless):

Ethereum has a robust, interoperable network, and its industry-leading DeFi ecosystem is a testament to that. Ethereum is the prime choice for any app maker seeking to benefit from its network effects. While this innovation has shown the power of democratizing aspects of retail finance, there remain significant barriers to meeting threshold regulatory demands that provide safeguards in today's financial markets.

Validator Control: Anyone can validate transactions without restrictions. Anyone from anywhere can run a node, often anonymously.

Access Control: Anyone can connect to any app. Apps that use whitelists or KYC controls must create separate smart-contract controls, which hurts the network's interoperability.

Data Privacy: Transactions are publicly visible, allowing tools like Etherscan to widely show transaction details and identify everyone involved. Even anonymous apps like Tornado can be reverse-engineered to track their origin.

2. Private Networks (Private Permissioned):

Networks with Private Networks introduce more control in multiple ways but at the cost of interoperability. They also don't completely solve privacy concerns:

Validator Control: App makers can control validators, improving transaction security and compliance.

Access Control: App makers can enforce entry controls through whitelists.

Data Privacy: While initial control is maintained, once access is granted, anyone inside the private network can read its transactions, effectively making the network "public" to all participants using a given application. Some approaches tried to address this by using a centralized signing service and segmenting transactions so only parties to a transaction could see it. Still, ultimately, these solutions fall short by leaving the door open for app operators to be able to peek into the transaction history.

3. Layer 2 Networks (Scaling Solutions for Public Permissionless Networks):

Layer 2 networks are designed to alleviate congestion on Layer 1 blockchains like Ethereum by processing transactions off-chain or in separate sub-networks. While they offer enhanced scalability and reduced transaction costs, they often do not fully address privacy concerns. The reliance on the mainchain for finality and the experimental nature of privacy solutions like Zero-Knowledge Proofs (ZKP) present ongoing challenges.

Validator Control: Validator control in Layer 2 networks can vary. Some Layer 2 solutions, like rollups, use selected validators or provers, while others, such as state channels, allow all participants within a specific channel or sub-network to act as validators. Control is given to validators that are not necessarily party to transactions.

Access Control: Can be either permissionless or permissioned, depending on the design. In permissionless Layer 2s, anyone can participate in the network. App makers may implement their own access controls within their Layer 2 application but usually at the trade-off of protocol level interoperability.

Data Privacy: Layer 2 networks improve scalability but are not primarily designed for privacy. Transactions may be aggregated or processed off-chain, but final state or proofs are often submitted to the public Layer 1 blockchain, exposing some data. Nascent privacy technology such as ZKPs (Zero-Knowledge Proofs), are still maturing and not yet proven or widely adopted. As a result, sensitive transaction details might still be exposed to the broader network or third parties.

4. Canton Network (Public Permissioned):

Canton Network is designed to provide a comprehensive solution that addresses all aspects of the Basel standards:

Validator Control: Only parties who are stakeholders in a particular transaction (as defined by the Daml smart contract) need to validate it. This allows app makers to have certainty over how their app operates and gives users absolute control over their data as it is validated by the defined set of stakeholder nodes involved in a transaction, not by third-party validators.

Access Control: Like other permissioned networks, each app maker can enforce strict access controls. App makers have complete control over defining permissions for their applications. They can create either public or permissioned applications based on their specific needs. Furthermore, app makers and users have the flexibility to switch between public or private synchronization infrastructure as required during operation. This adaptability gives comprehensive control over the connectivity and access parameters of nodes in the network, allowing for dynamic adjustments to meet changing trust, regulatory or operational requirements.

Data Privacy: Canton supports sub-transaction privacy, where parties can only see the parts of the transaction that apply to them. All transaction data between nodes is end-to-end encrypted and selectively shared on a need-to-know basis. This allows for very granular and selective privacy, where each app maker can define precise visibility rules for each transaction. For example, a regulator can witness a transaction between a bank and a customer while allowing each party to see only what they need to see from the entire transaction.

The Canton Network isn’t just another blockchain – it’s a paradigm shift in how regulated financial institutions approach the tokenization of financial and real-world assets. By balancing the benefits of interoperability from public networks with the tight controls required by regulators, Canton enables a new generation of compliant and connected digital asset applications. While the industry has long grappled with the seemingly impossible task of balancing privacy, control, and interoperability, and often sacrificing one aspect to bolster another, Canton proves that these elements can coexist and even synergize. This makes it an attractive choice for institutions seeking to innovate in the digital asset space without compromising on compliance, or the need for liquidity and network effects.

As the world of digital assets continues to evolve, solutions like the Canton Network will play a crucial role in bridging the gap between traditional finance and the emerging world of tokenized assets. This is a world where cross-border transactions between financial institutions can happen in real-time, where tokenization encompasses the end to end lifecycle of assets and how they move, and where traditional reconciliation processes are a distant memory.

As we stand on the brink of a new era in financial technology, networks like Canton pave the way for greater institutional adoption and unlocking the full potential of real-world assets on the blockchain. By enabling atomic, risk-free transactions and value transfer across organizations while respecting regulatory boundaries, Canton isn’t just keeping pace with today’s financial technology – it is attempting to shape the future of institutional finance. For institutions looking to harness the full power of blockchain within a regulated environment, Canton offers a path to blockchain adoption that doesn’t sacrifice connectivity for compliance, but ultimately offers a platform that allows for both.

DISCLAIMER

This report is for informational purposes only and is not investment or trading advice. The views and opinions expressed in this report are exclusively those of the author, and do not necessarily reflect the views or positions of The Tie Inc. The author may be holding the cryptocurrencies or using the strategies mentioned in this report. You are fully responsible for any decisions you make; the Tie Inc. is not liable for any loss or damage caused by reliance on information provided. For investment advice, please consult a registered investment advisor. The Tie Inc. provides services to Digital Asset (US) Corp. In addition, The Tie Inc. operates as a founding super validator of the Canton Network and as such is eligible to mint and hold Canton Coin rewards based on the utility it provides to the Canton Network and its participants.