Where Privacy Belongs

AUGUST 2026

Canton

Presented by The Tie

Table of Contents

Introduction

Blockchain's Privacy Misconception

There's a persistent misconception that the radical transparency of crypto is a virtue when it comes to on-chain financial markets - that a financial system functions best when every transaction is publicly visible, forever. Regulators, for their part, warn about the opposite extreme: fully opaque transactions that no one can reliably audit or oversee. To successfully scale systemically important financial markets on-chain, institutions and regulators cannot accept the trade-offs that exist at either end of this spectrum. They seek the middle ground, where the trust, accuracy and velocity benefits of shared ledger networks are balanced with the controls to operate securely and with independence.

In traditional finance, control over privacy, or rather what data is revealed to who and when - is the default. Your bank doesn't publish your transactions. Your employer doesn't broadcast your salary. Yet on most public blockchains, all of this remains visible to anyone with an internet connection. A freelancer paid in USDC has their income visible to every future client who checks their wallet.

No one really chose this. Blockchain users simply lost the protections that every other financial system provides by default. The industry has been trying to retrofit privacy onto public blockchains ever since they opened for business.

2. The Regulatory Middle Ground

In February 2024, Binance delisted Monero. Kraken followed for European users in October, citing MiCA compliance. OKX had already dropped it in January. The pressure extended beyond privacy coins. Anonymity-enhancing technologies built on top of transparent chains — mixers that break the on-chain link between sender and receiver — were being used to launder funds and evade sanctions, and enforcement followed: OFAC sanctioned mixing services including Blender.io and Tornado Cash, and the Justice Department prosecuted mixer operators. Regulatory agencies were not targeting on-chain financial privacy as a whole. They were using blunt tools, like sanctions, to specifically target anonymity.

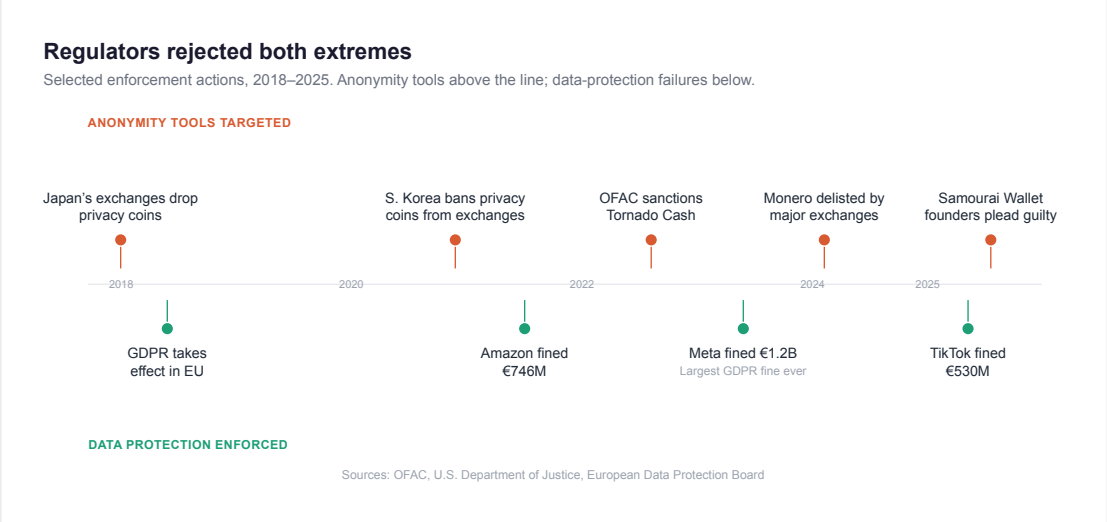
At the same time, data protection law in Europe pulled against the radical transparency ideology. GDPR enforcement continued to fine companies for exposing user data. In 2023, Ireland's Data Protection Commission hit Meta with a €1.2 billion fine, the largest GDPR penalty ever issued, for transferring European user data to the U.S. without adequate privacy protections.

GDPR carves out lots of room for compliance controls, explicitly permitting the lawful collection and retention of data for anti-money-laundering purposes. Its fines landed on companies mishandling consumer data, rather than financial institutions where such compliance work is already so deeply entrenched in operations. The law assumed the model regulated finance already runs on: protect private data and ensure controls are in place to make data available on a need-to-know basis, to parties with a legitimate need to see it.

These were not contradictory signals. Enterprises considering on-chain transactions were left with a false choice between radical transparency or anonymity tools increasingly exploited by illicit actors. Regulators, meanwhile, rejected both extremes. They sought neither secrecy nor full disclosure, but control over who could see what, when, and under what legal authority. TRM Labs, a blockchain compliance firm, made the same case in a February 2026 framework paper. Every stakeholder: users, regulators, law enforcement - needs something different from privacy. But only the right design can serve all of these stakeholders without forcing a choice between opacity and exposure. At the extremes, privacy coins implement total opacity with no way to grant access. Fully

transparent chains give total visibility with no native, proven way to configure who should actually see what. Neither works in practice for regulated payments or financial markets.

U.S. policymakers and regulators have since recognized that configurable privacy on blockchains is critical to the growth of the digital asset ecosystem. At the SEC Crypto Task Force's December 2025 roundtable on financial surveillance and privacy, Chairman Paul Atkins observed that public blockchains provide more transparency than any legacy financial system ever built, and pointed to selective disclosure, and compliance-preserving wallet designs as methods to let users prove what they must without exposing everything else; language that reinforces the **selective-state** model presented at the center of this paper.



3. The Wrong Question

For years, the blockchain industry treated privacy as a property of the asset. Monero or Zcash? Ring signatures or zk-SNARKs? These were the wrong questions and the wrong abstraction. Assets move across networks. They sit in wallets. They interact with applications. If the underlying network is transparent, bolting privacy onto individual assets creates friction, fragmentation and regulatory complexity.

The better lens to look through is not where privacy can sit on top of the stack, but how a system fundamentally handles state — the record of who transacted with whom,

and who owns what. Broadly, there are three approaches, with critical trade-offs to understand:

1. Hidden-state privacy encrypts the ledger itself. Monero and Zcash hide transactions cryptographically; Solana's confidential transfers and other zero-knowledge designs do the same at the asset or smart-contract level. This delivers confidentiality with public verifiability, but **at the cost of auditability**, complicating regulatory compliance. In addition, composability suffers, cryptography is complex, and **a flaw in a circuit can be both unprovable and unrecoverable**.

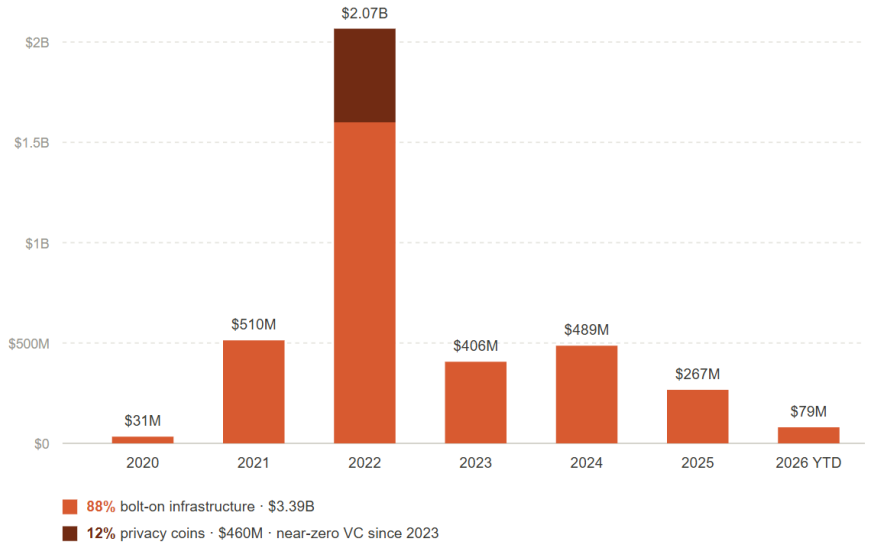
App- and wallet-level privacy adds concealment on top of a transparent chain. Mixers like Tornado Cash and Railgun break the on-chain link between addresses; ZK wallets obscure individual transactions. The state underneath stays public, so **privacy is bolted on after the fact**, with fragmentation, compliance friction, and **all-or-nothing opacity as the trade-offs**.

Selective-state privacy partitions the ledger so each party sees only the state it is entitled to. Canton takes this approach: **data is protected at the source and shared only on a need-to-know basis** as defined by the contract, while the network still maintains a single, globally consistent record. An app on Canton can be fully transparent if it needs to be. It can also be fully private, or any configuration in between. Financial institutions party to a transaction can **share the relevant information to meet their compliance obligations**.

Only selective-state privacy is designed at its core to overcome the regulatory risks, trapped funds, and liquidity fragmentation that have dogged the other two approaches while retaining global transaction composability - the critical feature that makes public blockchain so compelling in the evolution of financial markets.

$3.85B in crypto privacy VC since 2020

Annual VC investment in crypto privacy.
Coins (Monero/Zcash-style) atop bolt-on infrastructure (ZK rollups, FHE, mixers, ZK identity).



Privacy infrastructure includes general-purpose ZK rollups.
Canton / Digital Asset ($397M cumulative since 2018) is not shown — classified as institutional infrastructure, not privacy.

Source: The Tie Fundraising Dataset; 76 unique companies, 182 funding rounds. Excludes M&A. 2026 figures are Q1 YTD.

Since 2020, $3.85 billion in venture capital has gone into crypto privacy across 76 companies and 182 rounds. Almost all of it was directed at adding privacy to chains that weren't originally engineered for it. Such funding has been declining for the last two years. Money now flows more to projects with growing institutional adoption.

In its 2026 outlook, a16z crypto called privacy the most important moat in crypto, arguing that as throughput and fees converge across chains, privacy becomes the durable differentiator — one that locks users in, because secrets are far harder to move than assets.

Where earlier techniques failed to meet the demands of global financial workflows, Canton's selective-state model already runs at scale in production. In June 2026, Digital Asset, the developer behind Canton, closed a $355 million round at a roughly $2 billion valuation led bya16z crypto. The firm's general partner called Canton one of the clearest examples of blockchain product-market fit in regulated finance.

4. Hidden-State Privacy: The Total-Obsfuscation Problem

When privacy is part of the asset, you get total opacity. Every Monero transaction hides the sender, receiver, and amount using ring signatures and stealth addresses. This sounds interesting until you need to prove something to someone. A business can't demonstrate tax compliance. An institution can't satisfy AML requirements. An individual can't prove the source of funds for a mortgage. The privacy is absolute, which means disclosure is impossible.

Regulators responded predictably. Japan banned privacy coin trading in 2018. South Korea followed in 2020. By 2024, Binance, Kraken, and OKX had all delisted Monero in major jurisdictions. MiCA in Europe explicitly prohibits crypto service providers from supporting privacy coins. Monero still exists, but it's cut off from the regulated financial system. Users who want privacy and access to exchanges or compliant services can't have both.

Zcash took the opposite approach: optional privacy on a transparent base. After a 2025 adoption surge driven by a shielded-by-default wallet, around 30% of ZEC supply now sits in shielded pools, though fully shielded transactions remain a minority of network activity. In December 2025, Arkham Intelligence announced it had tagged more than half of Zcash transactions and $420 billion in volume to specific entities. However, the shielded cryptography did work, as Arkham's coverage came from tracing the transparent activity around the pool, not the fully shielded transactions.

ZK implementations carry their own technical risk, and the same total obfuscation that provides privacy makes failures invisible. Early designs required a trusted setup ceremony to generate the cryptographic parameters that secure the protocol; if any participant retained the underlying secrets, they could counterfeit the asset, undetected. In 2018, Zcash cryptographer Ariel Gabizon discovered a flaw in exactly that part of Zcash's setup that could have allowed unlimited counterfeit ZEC. The flaw had been embedded since the protocol launched in 2016, and the team kept it secret for seven months while shipping a fix. This risk is not confined to trusted setups, or to history. In March 2026, a researcher disclosed that Zcash nodes had been skipping proof verification on the network's legacy Sprout pool since 2020. Roughly 25,000 ZEC sat exposed to counterfeit withdrawal. Three months later, Zcash revealed a soundness

bug in its flagship Orchard shielded pool — live since 2022 — that could have allowed unlimited, undetectable counterfeit ZEC. An emergency hard fork patched it within days. But the pool is fully shielded, so there is no cryptographic way to prove the flaw was never exploited, and ZEC fell roughly 40% on the disclosure.

Part 3 of this series, on the privacy imperative for stablecoin payments, examines these zero-knowledge trade-offs — trusted-setup risk, limited auditability, and composability constraints — in greater depth.

5. App- and Wallet-Level Privacy: Privacy-Enhancing Bolt-Ons

One alternative has been to add privacy on top of transparent chains. For example, Tornado Cash lets Ethereum users deposit ETH into a pool and withdraw from a different address, breaking the on-chain link. ZK wallets generate proofs that hide transaction details. L2 solutions promise private smart contracts.

But bolt-on privacy has different types of problems. It's complex. Users must bridge assets, generate proofs, and deal with specialized interfaces, and it also fragments liquidity. Shielded pools sit separate from main-chain liquidity.

The base layer already saw the deposit, and you can obscure the link, but the original transaction is permanently public. That footprint is enough for forensic firms to trace it back. After Lazarus Group stole $625 million from the Ronin Bridge in March 2022, the hackers moved much of it through Tornado Cash. Chainalysis and Elliptic traced the funds anyway, and law enforcement recovered about $30 million within six months. Roughly 30% of all funds ever sent through Tornado Cash have been linked to illicit actors, and de-mixing tools are now a standard offering at blockchain analytics firms.

These tools also carry regulatory risk. OFAC sanctioned Tornado Cash in 2022, and even legitimate users found their addresses flagged by exchanges and analytics tools for years, even after OFAC lifted the sanctions.

Canton Network argues that you can't and shouldn't retrofit chains inherently designed for radical transparency to try to meet the exacting and granular privacy and compliance

requirements of global finance by layering obfuscation on top. Apart from the complexity, the bi-product are unwanted trade-offs around global composability - the most impactful innovation of public blockchains - and ongoing network auditability.

6. Selective-State Privacy: The Inheritance Model

There is a third option. Instead of making the asset private or bolting privacy onto apps, you build apps that leverage privacy baked into the network protocol and smart contract language itself. This is privacy as it already works across the internet: every application operator holds its own data and can decide, based on business and regulatory needs, who else has access and where in the world that data is physically domiciled. When you do this, every application, wallet, and asset running on that network inherits control and configurability over privacy as standard, without bolt-ons or workarounds.

This is how Canton works. The network doesn't replicate all transaction data across all nodes. Validators only see transactions they're party to. Data is encrypted and shared on a need-to-know basis defined by smart contracts. Privacy is the default. Disclosure is the action, granted on purpose, to specific parties, on the user's terms.

7. How Canton Does It

The world already knows how to do privacy: application operators store their own data and selectively disclose it based on business and regulatory requirements.

> *What Canton reinvented is how to achieve consensus on private data. Most blockchains started from Nakamoto-style consensus — fully transparent — and have been trying to add privacy ever since; Canton started from classical privacy and added consensus.*

Canton uses a smart contract language called Daml that defines who sees what at the sub-transaction level. When a transaction executes, the parties involved are specified

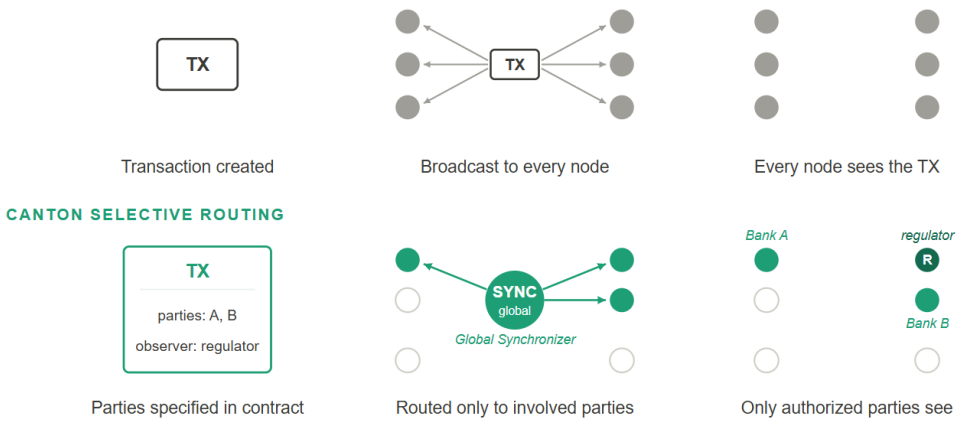
in the contract, and only those parties can see the relevant data. The regulated financial institution has access to the transaction information for its customers and the assets it issues; a regulator can be granted witness access to a transaction between a bank and a customer, while each party sees only what it needs to.

The protocol enforces this architecturally rather than through encryption alone. Canton doesn't replicate all transaction data across all nodes, and validators only see transactions they're party to. There's no public mempool broadcasting pending transactions. The network's decentralized infrastructure, the Global Synchronizer, coordinates atomic settlement across applications without exposing transaction details to uninvolved parties.

The premise is the opposite of how most blockchain privacy works. Standard chains broadcast every transaction to every node for consensus and then try to encrypt or obscure parts of that broadcast. Canton shares only what each party needs to see, when they need to see it.

Canton routes data only to parties who need it

Three-step comparison of the standard broadcast model and Canton's selective routing.



Sources: Canton Network architecture; TRM Labs, On-chain Privacy and Financial Compliance (Feb 2026)

That architectural choice has compliance consequences. Privacy systems that encrypt the full transaction graph protect data well, but make retroactive auditing structurally hard.

TRM Labs' February 2026 framework paper notes the limitation directly.

> *A zero-day bug or logic flaw in a zero-knowledge circuit can't be retroactively investigated, because the protocol's own anonymity erases the evidence.*

Canton's selective-disclosure model preserves the audit trail for parties with authorized access without exposing it publicly. The TRM paper describes this kind of design, protocol-level privacy combined with selective disclosure controls and tiered access, as the most promising path for hybrid compliance. TRM is putting that into practice on Canton itself: in an April 2026 analysis, it detailed how its integration uses a designated "guardian" and a trusted execution environment to surface AML risk signals while accessing only the data it needs, letting privacy and compliance reinforce each other rather than compete.

The result is a public blockchain where data and transactions are only disclosed on a need-to-know basis, but auditable by design. Participants and application providers decide who gets visibility rather than the protocol deciding for them.

7a. The Privacy Range

Canton doesn't lock users into a single privacy setting. The same network supports a full range of configurations.

- At the **end-user** level, a user transferring a private asset through a wallet like FiveNorth's Loop runs a personal payment visible only to the parties who need to see it: the sender, the receiver, their wallet providers if they choose to use third-party providers, and, depending on the asset, its issuer or administrator. Rather than the opacity of a privacy coin, the model mirrors traditional banking — the sender and receiver see the payment, a trusted party can see what it needs to, and the rest of the network cannot. How much is shielded depends on the asset:

a privacy-preserving stablecoin keeps amounts and counterparties confidential, while a public, permissionless asset like Canton Coin is more transparent by design.

- At the **business** level, a business sending vendor payments through Bitwave for example using Brale's SBC stablecoin keeps amounts and counterparty identities visible only to the parties and a designated auditor; competitors see nothing, and the internal accounting team gets full reporting through ERP integrations like NetSuite and QuickBooks.

- At the **organizational** level, a DAO can run a fully transparent treasury where every transaction is visible to members or the public.

Configuration is what changes, but the user, the assets, and the underlying network stay the same.

Regulators are starting to ask for this kind of model: programmable disclosure that meets compliance requirements without exposing sensitive data publicly.

7b. What's Live Today

Canton's privacy model is in production, and assets are arriving on the network because of it.

On the asset side, DTCC has started to run its tokenization service, bringing DTC custodied US Treasuries to Canton. Franklin Templeton's iBenji platform, which distributes its tokenized U.S. government money market fund, is in production for use as a collateral and liquidity tool across Canton's growing global network. BitSafe's cBTC and onRails' cETH bring wrapped Bitcoin and Ether onto the network for settlement and new products and workflows where positions must stay confidential.

On the cash side, Circle's USDCx, a USDC-backed stablecoin issued through Circle's xReserve protocol, settles institutional payments and out-of-hours financing on Canton with amounts and counterparties shared only on a need-to-know basis. Brale's SBC stablecoin runs with native privacy for institutional payments, and Brale has been used

to launch ten other stablecoins on the network for the same reason. The confluence of privacy and composability is also leading major commercial banks to tokenize deposits for use across Canton too. First Lloyds, then LSEG's DiSH platform put on-chain cash to work on Canton. Now J.P. Morgan has natively deployed its JPM Coin deposit token on the network, while HSBC has begun its own journey.

Privacy alone isn't why these assets are starting to move here. This core primitive on Canton is combined with the network's native composability. Assets and cash need to swap atomically, with the right disclosures. This is why the pull to Canton is so strong today, where use cases that take advantage of this combination are unlocked: collateral mobility for intraday and out-of-hours financing, leveraging DTC-custodied U.S. Treasuries - and settled atomically against tokenized bank deposits or stablecoins through live repo apps like Tradeweb, or emerging trading venues like Temple.

The network now processes north of $9 trillion in tokenized real-world assets every month, across more than 800 institutions, executing around 3 million daily transactions. Broadridge's Distributed Ledger Repo platform alone processes about $350+ billion in daily U.S. Treasury repo on Canton rails with institutional overnight funding now running on-chain. Some of the 55+ Super Validators now include JPMorgan, BNP Paribas, DTCC, Tradeweb, Société Générale, Cumberland DRW, Circle, and Visa.

Composability + Privacy in Practice: Tokenized Treasury Financing

In December 2025, a Canton Network Industry Working Group (Bank of America, Brale, Circle, Citadel Securities, Cumberland DRW, Société Générale, Tradeweb, Virtu Financial, M1X Global, and Digital Asset) completed the second phase of fully on-chain U.S. Treasury financing. The group executed five synchronized transactions, including the first real-time rehypothecation of tokenized U.S. Treasuries across counterparties: Treasuries were pledged, released, and immediately repledged. Multiple stablecoins (SBC, USDM1 and USDC) provided settlement liquidity, with direct Treasury-to-stablecoin conversion taking place within the transaction itself.

Seven months later, in July 2026, those concepts moved beyond industry working

groups into production. DTCC successfully processed initial live trades on Canton using DTC-tokenized U.S. Treasuries and equities, with more than 30 participating institutions.

Together, these milestones demonstrate what institutions need to move capital on-chain: composable assets and smart contracts that can interact across applications and counterparties, combined with the privacy that allows firms to execute transactions without exposing positions, pricing, counterparties or trading strategy to everyone else on the network.

8. Why Retail Users Should Care Too

Privacy at the network layer matters for retail users too. If you've been paid in USDC on Ethereum, your salary is visible to anyone who looks up your wallet. Your landlord can see it. Your employer can see your spending. Merchants you pay can (and already do) analyze your purchase history.

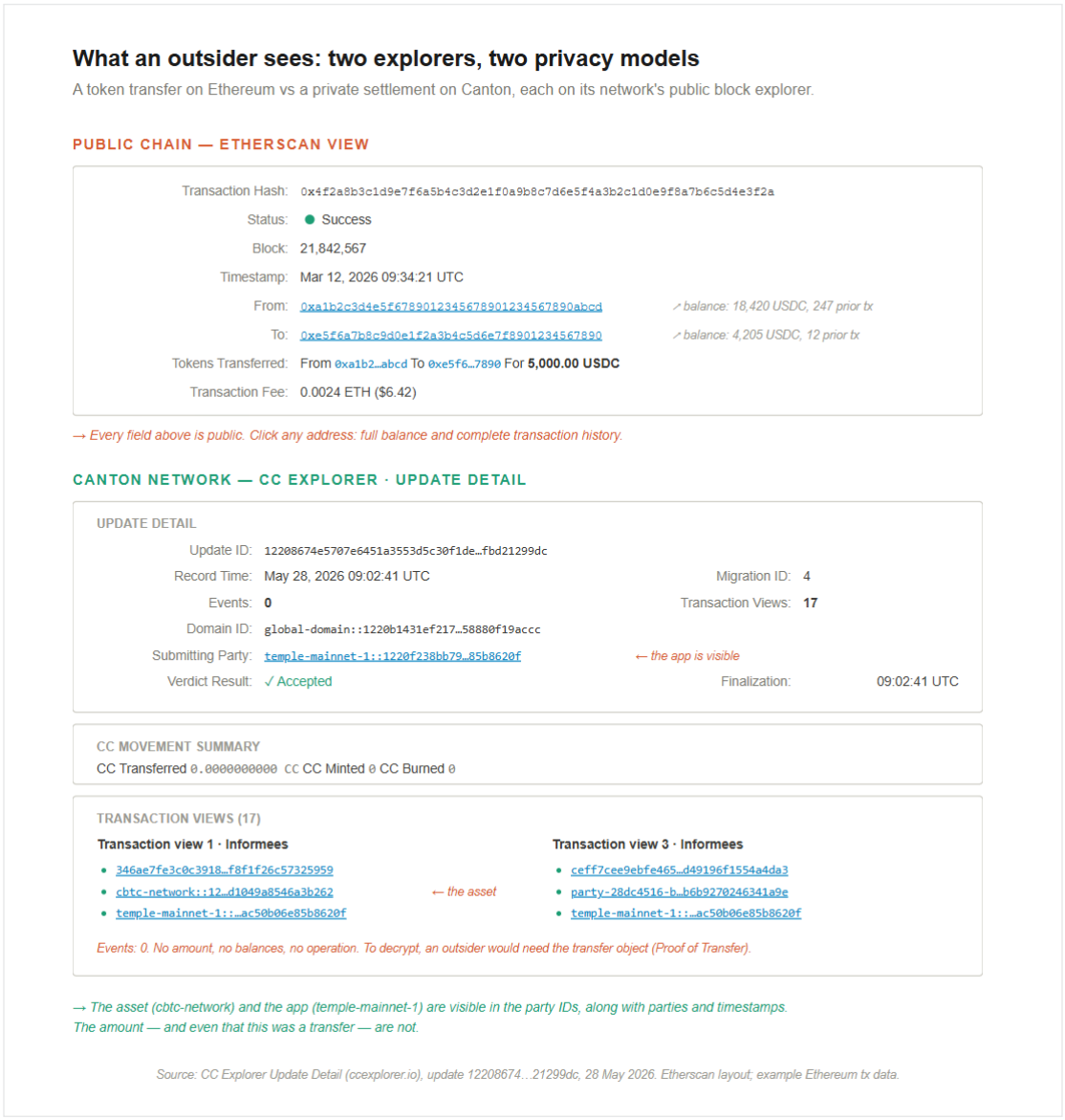
Recurring payments to a therapist or medical services could expose your health information. Pharmacy purchases can imply a diagnosis. Political and religious donations make affiliations visible. Each of these becomes a permanent record on a transparent chain, available to current and future employers, insurers, family members, and anyone running on-chain analytics.

This is the Venmo problem at scale, and it's already changing user behavior. Crypto workers receiving stablecoin salaries face a binary → spend directly from the salary wallet and expose their income to anyone with a block explorer, or route funds through centralized exchanges in multistep workarounds that defeat the point of using stablecoins in the first place. Venmo made payments private by default after years of user complaints. Today, most public chains still default to this public broadcast approach.

Canton fixes this at the protocol level. A Bron wallet sending USDC to another Bron wallet on Canton hides the amount and the contract details by default. Network observers can see that two parties interacted and which asset was involved, but not the

amount, the contract details, or even that the activity was a transfer. The same payment between two MetaMask wallets on Ethereum is fully public, queryable by anyone and traceable forever.

In February 2026 a global enterprise executed the first private payroll transaction on Canton, paying its workforce in stablecoins through a partnership between payroll provider Toku, wallet provider Cantor8, and Digital Asset. Salaries settled in under two minutes at a fraction of traditional cross-border costs, with no salary data exposed to a public ledger. Toku CEO Ken O'Friel described the blocker that had stopped this for years: "Every public company CFO we talk to gets excited about stablecoins until they realize their payroll would be public. That's where the conversation ends."



Fundamentally, this model preserves lawful oversight. Amounts and contract details are shielded, but a regulator or law enforcement body that needs more can still identify the application or regulated financial institution involved in a transaction, enough information to direct a request to the right party. That is the same path authorities use in traditional finance today.

9. The Trader's Problem: MEV and Front-Running

Transparency also costs traders money. On Ethereum, when you submit a swap to a DEX, your transaction enters the public mempool before it executes. Bots see it, calculate your expected price impact, place a buy order ahead of yours to push the price up, then sell into your trade. This is a sandwich attack, which extracts value from every user who swaps tokens.

Between November 2024 and October 2025, EigenPhi tracked more than 95,000 sandwich attacks (60,000 to 90,000 per month). The total extracted from Ethereum users in 2025 reached roughly $40 million. Thirty-eight percent of attacks hit low-volatility pools like stablecoins and wrapped assets, where users expect minimal slippage. Most of the extracted value flows to block builders through gas fees rather than to the searchers running the bots, but the user is the one paying.

The Ethereum ecosystem has responded with bolt-on protections: Flashbots Protect, MEV-Boost, BuilderNet, and threshold-encryption proposals like Shutter all attempt to shield user transactions from the public mempool after the fact. These tools have cut monthly sandwich extraction from around $10 million in late 2024 to $2.5 million by October 2025. But the underlying architecture still exposes order flow by default, and retail traders using standard wallets remain the primary victims.

Canton handles this at the protocol layer. Order flow stays private right through to settlement. The public mempool doesn't exist on Canton; there's no exposed pending state for a bot to watch. Tradecraft, a Canton-native DEX built by Obsidian Systems, supports atomic multi-currency swaps across Canton Coin, Brale's SBC stablecoin, BitSafe's CBTC, and USDM1 with privacy by default. Counterparties, amounts, and trading strategies remain visible only to the parties in the trade.

On Canton, retail traders save a few dollars per swap. Active traders running volume save something more valuable: a strategy that can't be reverse-engineered by anyone watching the network.

10. Comparison Matrix

Each approach handles state differently, and that choice determines what is possible with the applications and assets that build on it.

Privacy at the hidden-state level (Privacy coins, ZK L1s) means private by default, but disclosure is constrained or fragmented. Regulatory status is either hostile or remains unconvinced. Composability is limited due to isolation. Adoption is niche, and declining in regulated markets.

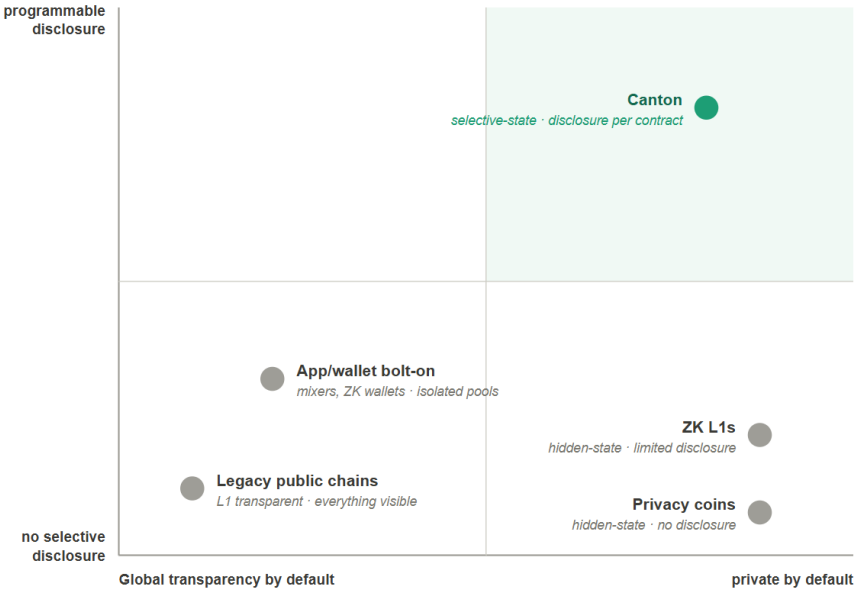
Privacy at the app- and wallet level (mixers, ZK wallets) means partial hiding inside isolated pools that don't compose easily with the rest of the chain. Regulatory status is uncertain. Composability is highly fragmented. Adoption is early, with most implementations on testnets or limited mainnets.

Privacy at the selective-state level (Canton Network) with native programmable disclosure controls means the same network can support fully private personal payments, B2B settlement with regulator visibility, or a transparent DAO treasury, configured per contract. Regulatory status is favorable: the model is built for compliance, with auditor access built in. Full composability across applications unifies liquidity. This framework is what makes it possible to process $9T+ in monthly on-chain assets, with major institutional participants.

Other approaches either expose everything or hide everything. But Canton lets you choose.

Mapping crypto privacy architectures

Five approaches positioned by how each handles state and selective disclosure of transactions.



Approximate positioning. Hybrid implementations may sit between categories.

11. Conclusion: Privacy as a Part of the Infrastructure

For Canton, the answer to the blockchain privacy dilemma was always architectural: a public blockchain that embeds privacy control at the network layer, and programmable disclosure through smart contracts.

The debate over how to add privacy to crypto - bolting it onto applications or baking it into the asset - missed the point. Privacy belongs in the protocol itself, enabling data visibility as selective-state disclosure, not a bolt-on to applications or specific assets.

When the protocol enables this control, compliance and confidentiality stop being a trade-off. The question for institutional users or retail users alike shifts from “how can I hide my transactions?” to “who should be able to see this?”.

INVESTMENT DISCLAIMER AND CONFLICT DISCLOSURE

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. is a service provider for Digital Asset (US) Corp. and operates as a founding super validator of the Canton Network. In addition, The Tie Inc. operates featured applications on the Canton Network. The Tie Inc. receives rewards as a validator and app provider related to utility and activity on the network. Accordingly, The Tie Inc. has a financial interest in the continued development and success of the Canton Network.