Privacy: the missing layer of institutional finance

Source: AI generated

The privacy coin sector is the only part of the crypto market trading above last year's peak, and the US market's main settlement house has just launched a tokenisation service on a confidential blockchain. Hiding transactions, long seen as a red flag, is starting to look like a condition for institutional adoption.

Charles-Henry Monchau, CFA, CAIA, CMT
Chief Investment Officer
charles-henry.monchau@syzgroup.com

Assia Driss
Syz Research Lab Team Coordinator
assia.driss@syzgroup.com

Romain Marcozzi
Syz Research Lab Team
romain.marcozzi@syzgroup.com

Syz PRIVATE BANKING

Since Bitcoin peaked in October 2025, almost every corner of the crypto market has lost ground. One sector has done the opposite. According to 21shares, privacy coins stood 236%, while the average crypto asset, excluding stablecoins, had fallen 26%. On 28th October, the Depository Trust & Clearing Corporation (DTCC), which settles most US securities transactions, launched its tokenisation service on the Canton Network, a blockchain designed so that each participant sees only its own transactions. Twenty institutions, including JPMorgan, Citi and Morgan Stanley, have signed up, CoinDesk reports. The two stories share a common thread. Public blockchains expose every balance and every transfer, which a retail trader may tolerate but a financial institution cannot. Privacy technology addresses that weakness. Once treated as a regulatory red flag, is onchain privacy becoming a necessity for institutional finance?

What is the onchain privacy sector?

Crypto tokens and tokenised assets rest on the same foundation, a blockchain, which is a shared ledger maintained by a network of computers instead of a single institution. Native tokens such as bitcoin exist only on that ledger, while tokenised assets are digital representations of shares, bonds or funds held by a custodian. Their appeal lies in settlement within minutes and markets that never close.

That openness comes at a price. On public blockchains such as Bitcoin or Ethereum, anyone can see every transaction. Wallets carry strings of characters rather than names, but once an address is linked to a person or a company, its full history and balance become readable. Pseudonymity, in practice, offers little protection.

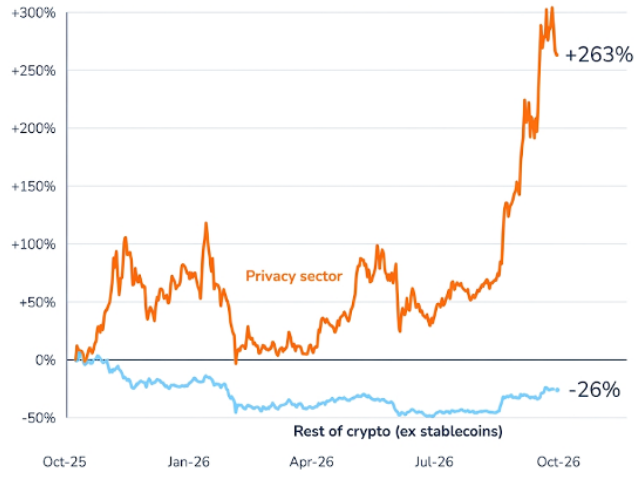
The privacy sector covers technologies that hide transaction amounts, the addresses involved, or both. Most rely on zero-knowledge proofs, a cryptographic method that proves a statement is true without revealing the information behind it. Applied to a payment, the network can confirm that the sender owns the funds and has not spent them twice, without learning who paid whom or how much.

This capability long gave the sector a poor reputation. Privacy tools became associated with darknet markets and money laundering, and in August 2022 the US Treasury sanctioned Tornado Cash, a service that mixes Ethereum transactions to obscure their origin. The sanctions were lifted in March 2025, after a federal appeals court ruled that the Treasury had overstepped its authority by targeting immutable software.

The distinction for institutions is between anonymity and confidentiality. Anonymity hides information from everyone, regulators included. Confidentiality hides it from the public while keeping it accessible to authorised parties such as auditors or supervisors, through viewing keys or permissioned access. This is what separates institutional use from criminal use.

The sector's main actors reflect that divide. Monero, a cryptocurrency launched in 2014, makes every transaction private by default. Zcash, launched in 2016, whose coin trades under the ticker ZEC, makes privacy optional and lets users share viewing keys with third parties. Canton, whose shared infrastructure went live in July 2024, was designed for banks, with each participant seeing only the transactions it is involved in. 21shares values the privacy sector at about $35bn, of which Zcash represents around $24bn. That still represents a small fraction of the crypto market excluding stablecoins, around only 1.4%.

Relative Performance: Privacy Sector vs. Mainstream Crypto Index

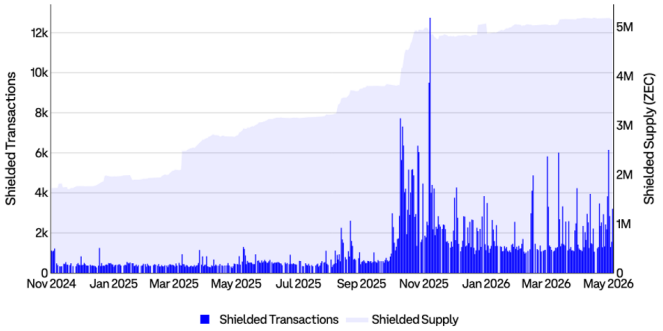


Source: Glassnode

Financial privacy meets institutional demand

For financial institutions, full transparency is a practical obstacle. No bank will trade on a network where competitors can watch its positions in real time and anticipate its orders. Companies face a similar problem, since payroll, supplier payments and treasury operations reveal commercial information that no firm would choose to publish. Individuals have their own reasons, as a visible balance makes its owner an easy target for hackers, scammers and, increasingly, physical theft.

Usage data suggests this demand is not purely speculative. On the Zcash network, users can choose to keep their coins in "shielded pools", where balances are hidden. 21shares estimates that 28% of all ZEC in circulation now sits in these pools, up from 9% in 2023. Coins moved into these pools tend to stay there, which points to holders who value privacy enough to actually use it.



Source: ZecHub, Coinbase, as of May 2026

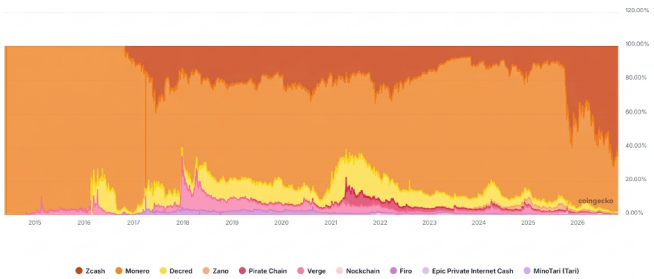
Investor access is broadening too. In August, Grayscale launched the first US-listed spot Zcash ETF, giving traditional investors exposure to ZEC without holding the cryptocurrency directly. By late October, the fund had accumulated more than $750mn in assets, providing another source of demand for the token.

The broader growth of tokenisation adds to this demand. McKinsey expects tokenised financial assets, excluding cryptocurrencies and stablecoins, to reach around $2tnby 2030 in its base case, and up to $4tn in a more optimistic scenario. Every bond, fund or share that moves onchain raises the same question of who can see the trade. The more traditional finance relies on blockchains, the more confidentiality becomes a basic requirement.

Three ways the sector is taking shape

Exposure to onchain privacy comes through three quite different channels. The first is dedicated privacy coins such as Zcash and Monero, traded on crypto exchanges. They are the purest form of onchain privacy and rely on technology tested over a decade. They are also the sector's main regulatory target. Several large exchanges have stopped offering them for trading since 2024, with OKX removing Monero and Zcash and Binance removing Monero, which limits liquidity and access.

Top Privacy Coins Market Cap Chart



Source: Coingecko

The second is institutional infrastructure, led by Canton and its token, Canton Coin (CC). Here, the assets exchanged are tokenised securities instead of crypto tokens, and privacy is built into the design. Adoption is concrete. JPMorgan is bringing its JPM Coin deposit token to the network, Broadridge runs its repo platform on it, and DTCC has now launched its tokenisation service there. Broadridge's platform alone processes more than $8tn a month on Canton, Blockworks Research estimates. Nevertheless, this figure needs context. Most of it comes from repurchase agreements, or repos, which are very short-term loans backed by government bonds. Because the same bonds are lent again day after day, they are counted many times over. The value of tokenised assets actually held on the network is much lower, at about $367bn, based on data from RWA.xyz. CC holders also capture only a small part of this activity, through the fees banks pay to use the network.

The third is generalist blockchains such as Ethereum, Solana and NEAR, which have put confidential transactions on their roadmaps. They bring a large user base and carry far less regulatory stigma. The drawback is dilution, since privacy is one feature among many and will rarely drive the value of these networks.

The institutional segment has the most durable demand, as confidentiality is a precondition for banks to operate onchain. It is also where the link between adoption and token value is the weakest, as banks use Canton for its infrastructure and have no need to hold CC beyond paying fees. Zcash occupies an interesting middle ground. Its optional privacy, combined with viewing keys, sits closer to what regulators can accept than Monero's default anonymity. Unlike Canton, its usage also benefits the token directly, since anyone who wants Zcash's privacy has to hold ZEC. Its blocker is that European rules do not currently make that distinction.

The compliance paradox

The growing demand for financial privacy comes at an awkward time for privacy coins. Banks need confidentiality to protect their clients, positions and transactions, yet regulators need sufficient transparency to enforce anti-money laundering rules. The same technology that makes a blockchain attractive to institutions can therefore make it harder to access through regulated financial channels.

From July 2027, the EU's Anti-Money Laundering Regulation will prohibit crypto-asset service providers from handling anonymity-enhancing coins or maintaining anonymous accounts, which is likely to push exchanges serving European clients to delist Monero and Zcash ahead of the deadline. The travel rule of the Financial Action Task Force (FATF), the international body that sets anti-money laundering standards, adds further pressure. It requires crypto platforms to share the identity of the sender and the recipient with each transfer. For banks, any association with money laundering or sanctions evasion is a reputational risk most will refuse to take.

Switzerland offers a useful parallel. Banking secrecy survived for decades but came under increasing pressure as international efforts to combat cross-border tax evasion intensified. In 2018, Switzerland began automatically exchanging financial account information with foreign tax authorities. If onchain confidentiality does not allow regulators to access information, it could face similar pressure and restrictions.

Market risks are just as significant. The sector is small and concentrated, with Zcash alone accounting for about two thirds of its value. Moreover, volatility is extreme. Crypto Briefing data shows ZEC falling from a late-September high near $1,680 to around $1,050 by mid-October. Value accrual is a separate concern, since institutional adoption of privacy infrastructure can grow while the associated tokens stagnate.

Technical risk is harder to detect. Bugs in zero-knowledge systems can remain invisible precisely because the data they protect is hidden. In May 2026, a researcher discovered a flaw in Zcash's main shielded pool that had existed since 2022 and could in theory have allowed counterfeit coins to be created undetected. ZEC fell 38% after the disclosure, according to Decrypt, and the network introduced an entirely new pool in its July upgrade. A similar flaw had already been fixed in 2019. Finally, if Ethereum and Solana integrate privacy natively, dedicated projects could lose the premium they enjoy today.

Conclusion

Onchain privacy is becoming a prerequisite for institutional finance, but only in its confidential form. Banks already use it at scale on Canton, and today's DTCC launch confirms the direction. Anonymity faces a very different future, with European regulators set to push it out of the regulated market from 2027. The sector is therefore splitting in two, between compliant privacy for institutions and anonymous privacy for individuals. The first looks durable, as banks cannot move onchain without it. The second will face tighter limits, but individual demand for financial privacy is likely to persist. The coming months will show whether DTCC volumes on Canton pick up, whether Zcash's shielded share keeps rising, and how strictly the EU applies its rules in 2027.

Welcome to Syzerland®

For further information

Banque Syz SA
Quai des Bergues 1
CH-1201 Geneva
T. +41 58 799 10 00
syzgroup.com

Charles-Henry Monchau, CFA, CAIA, CMT
Chief Investment Officer
charles-henry.monchau@syzgroup.com

Assia Driss
Syz Research Lab Team Coordinator
assia.driss@syzgroup.com

Romain Marcozzi
Syz Research Lab Team
romain.marcozzi@syzgroup.com

This marketing document has been issued by Bank Syz Ltd. It is not intended for distribution to, publication, provision or use by individuals or legal entities that are citizens of or reside in a state, country or jurisdiction in which applicable laws and regulations prohibit its distribution, publication, provision or use. It is not directed to any person or entity to whom it would be illegal to send such marketing material.
This document is intended for informational purposes only and should not be construed as an offer, solicitation or recommendation for the subscription, purchase, sale or safekeeping of any security or financial instrument or for the engagement in any other transaction, as the provision of any investment advice or service, or as a contractual document. Nothing in this document constitutes an investment, legal, tax or accounting advice or a representation that any investment or strategy is suitable or appropriate for an investor's particular and individual circumstances, nor does it constitute a personalized investment advice for any investor.
This document reflects the information, opinions and comments of Bank Syz Ltd. as of the date of its publication, which are subject to change without notice. The opinions and comments of the authors in this document reflect their current views and may not coincide with those of other Syz Group entities or third parties, which may have reached different conclusions. The market valuations, terms and calculations contained herein are estimates only. The information provided comes from sources deemed reliable, but Bank Syz Ltd. does not guarantee its completeness, accuracy, reliability and actuality. Past performance gives no indication of nor guarantees current or future results. Bank Syz Ltd. accepts no liability for any loss arising from the use of this document.