

# Zcash

(ZEC)

## Tokenholder Report

This research report has been funded by GenZcash. By providing this disclosure, we aim to ensure that the information reported in this document is conducted with objectivity and transparency.

Blockworks Advisory makes the following disclosures:

1) Report Funding: The information reported in this document has been funded by GenZcash. The sponsor may have input on the content of the report, but Blockworks Advisory maintains editorial control over the final report to retain data accuracy and objectivity. All published token holder reports by Blockworks Advisory are reviewed by internal independent parties to prevent bias. 2) Researchers submit financial conflict of interest (FCOI) disclosures on a monthly basis that are reviewed by appropriate internal parties. Readers are advised to conduct their own independent research and seek advice of qualified financial advisor before making investment decisions.

Q4 2025

**Blockworks Advisory**

# Table of Contents

<b>02</b>	Executive Summary
<b>03</b>	Privacy & Monetary Adoption
<b>14</b>	Instituional & Governance Maturity
<b>17</b>	Zodl Wallet Adoption
<b>19</b>	Scaling & Tachyon
<b>20</b>	Investor Endorsements
<b>21</b>	Closing Summary & Outlook
<b>22</b>	Appendix

# Executive Summary

Q4 2025 marked a pivotal period for Zcash, strengthening its position as a leading privacy-focused blockchain. The quarter saw governance reforms, rising adoption of shielded transactions, and continued infrastructure development aimed at scaling private payments.

Like Bitcoin, Zcash is a supply-constrained Proof-of-Work asset, but it differentiates itself by enabling encrypted transactions by default. This allows ZEC to function as both a store of value and a medium of exchange that preserves financial privacy. Adoption this quarter was supported by the growing use of Zodi, Zcash's mobile wallet for shielded transactions, and continued development of Tachyon, a technical upgrade designed to reduce storage and bandwidth requirements and improve long-term scalability.

Governance also evolved significantly with the introduction of tokenholder voting as the primary mechanism for protocol decisions. Combined with community grants and token-based developer funding, this shift has realigned incentives across users, developers, and capital providers.

From a metrics perspective, Q4 2025 showed strong growth across key privacy indicators. Shielded pool holdings reached 5,067,532 ZEC (30.8% of circulating supply), with Orchard pools representing 87.1% of private holdings. Total shielded transactions increased 224.1% quarter-over-quarter, indicating meaningful adoption beyond speculative activity. The anonymity set also continued its monotonic growth, adding 407,686 notes in Q4, reinforcing the compounding privacy advantage that underpins Zcash's competitive position.

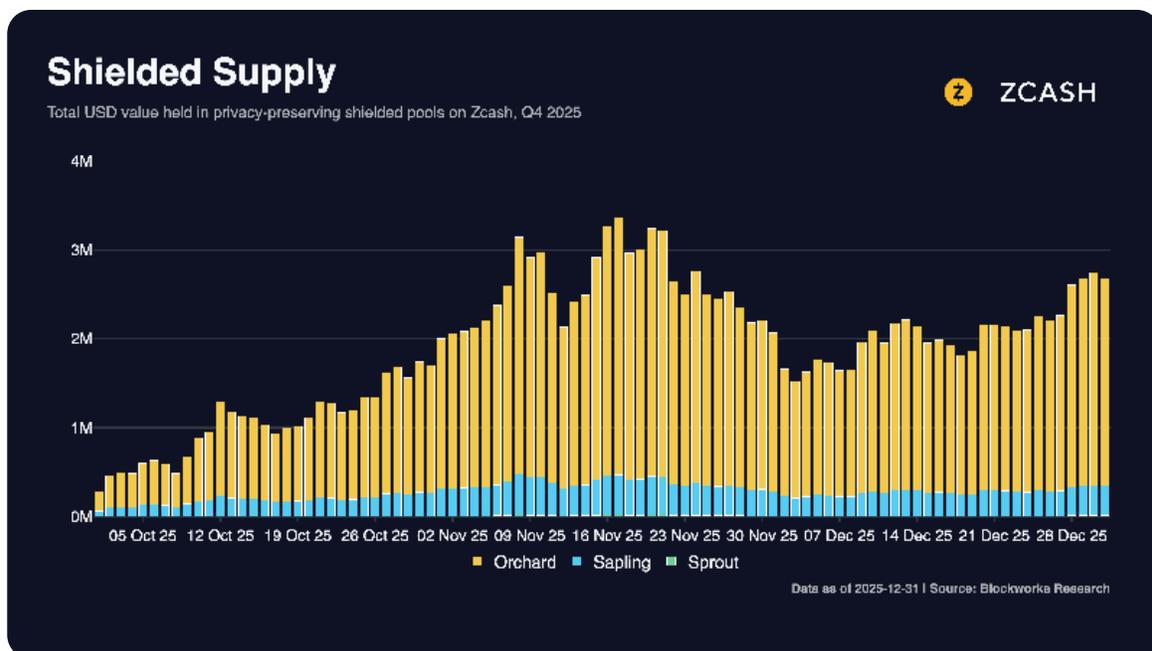


# Privacy & Monetary Adoption

Privacy is Zcash's core value proposition and primary competitive advantage. Unlike transparent blockchains where all transactions are visible, Zcash's shielded pools create a true "supply not for sale", ZEC held by users who value privacy enough to move funds into shielded pools and keep them there. This section examines the three critical metrics that demonstrate Zcash's privacy adoption and its implications for monetary integrity: shielded pool size (stock), shielded transactions (flow), and anonymity set growth (structural moat).

## Shielded Pool Size

The total amount of ZEC held in shielded pools represents the most direct measure of committed holder base and long-term conviction. Unlike transparent balances, shielded holdings cannot be easily tracked, sold under pressure, or targeted by regulators. This makes shielded pool size a critical indicator of Zcash's monetary premium and holder commitment.



Total USD value held in privacy-preserving shielded pools on Zcash, Q4 2025. Stacked by pool (Orchard, Sapling, Sprout). Source: [Blockworks](#)

During Q4 2025, shielded pool holdings reached 5,067,532 ZEC, representing approximately 30.8% of total circulating supply. The majority of this supply is held in Orchard pools, which offer the strongest privacy guarantees and most efficient transaction processing. This concentration in Orchard reflects both technical improvement and increasing sophistication among users.

The composition of shielded holdings tells an important story. Orchard pools represent 87.1% of total shielded supply at quarter-end, up from 77.8% at the beginning of the quarter. This shift matters because Orchard offers better privacy properties, lower transaction costs, and improved scalability. The migration to Orchard is a positive signal that users are not just holding ZEC privately, but are actively using the most advanced privacy technology available. Sapling pools hold 629,108 ZEC (12.4% of shielded supply), while Sprout pools hold 25,482 ZEC (0.5% of shielded supply).



ZEC Pool Holdings Relative to Circulating Supply. Source: [Blockworks](#)

Q4 2025 Shielded Pool Holding Changes			ZCASH
Pool	Start	End	Δ
Sprout	25,782 ZEC	25,482 ZEC	-300 ZEC
Sapling	822,166 ZEC	629,108 ZEC	-193,058 ZEC
Orchard	2,966,388 ZEC	4,412,942 ZEC	+1,446,554 ZEC
Total	3,814,336 ZEC	5,067,532 ZEC	+1,253,196 ZEC

Data as of December, 2025 | Source: Blockworks Advisory

Table of Pool Changes. Source: [Blockworks](#)

During Q4 2025, Zcash’s shielded pool balances increased materially, driven almost entirely by growth in the Orchard pool. Total shielded holdings rose from 3.81M ZEC to 5.07M ZEC, a net increase of 1.25M ZEC over the quarter. Orchard holdings expanded by **1.45M ZEC**, more than offsetting declines in both legacy pools, as Sapling balances fell by 193k ZEC and Sprout declined marginally by 300 ZEC. This pattern strongly suggests continued migration toward Orchard as the dominant shielded pool, reflecting user preference for newer protocol features and improved efficiency, while older pools steadily wind down in relative importance.

A plausible explanation for this shift is that new shielded inflows are increasingly landing in Orchard by default, rather than users actively moving balances out of older pools.

Modern Zcash wallets now generate addresses that automatically support the newest shielded pool, meaning new deposits, transaction change, and wallet-created outputs are preferentially assigned to Orchard.

**Monetary Implications**

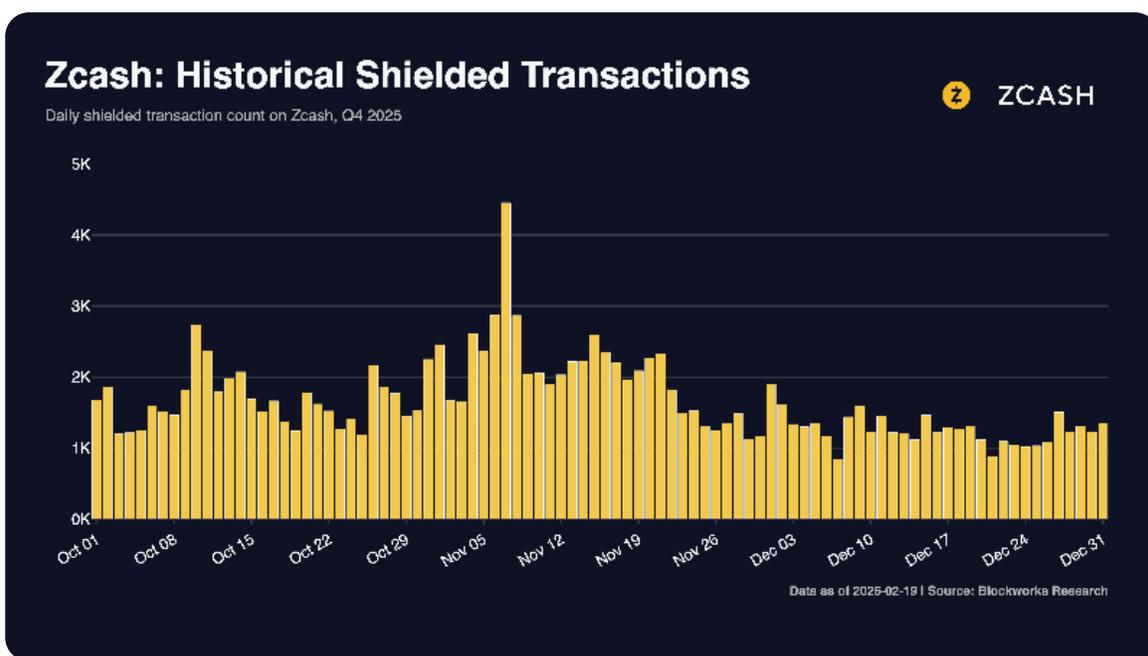
Shielded pool size is the most important metric for understanding Zcash’s monetary premium. Unlike Bitcoin or most other networks, where all transactions are transparent and holdings can be analyzed, Zcash’s shielded pools create a true “supply not for sale” dynamic. This supply cannot be easily tracked, cannot be targeted by regulators, and represents holders who have made a deliberate choice to preserve privacy.

The growth in shielded pool size, particularly in Orchard, indicates that Zcash is attracting and retaining

holders who value privacy as a core monetary property. This is not speculative activity, it is long-term conviction. As shielded pool size grows, the available transparent supply shrinks, creating natural scarcity dynamics that support price appreciation.

## Shielded Transaction Growth

Transaction volume is often a misleading metric in crypto, as it can be inflated by wash trading, speculative activity, and protocol manipulation. Shielded transactions are different. Moving funds into and out of shielded pools requires deliberate action and incurs transaction costs, disincentivizing spam. This makes shielded transaction volume a more reliable indicator of real-world usage and adoption.



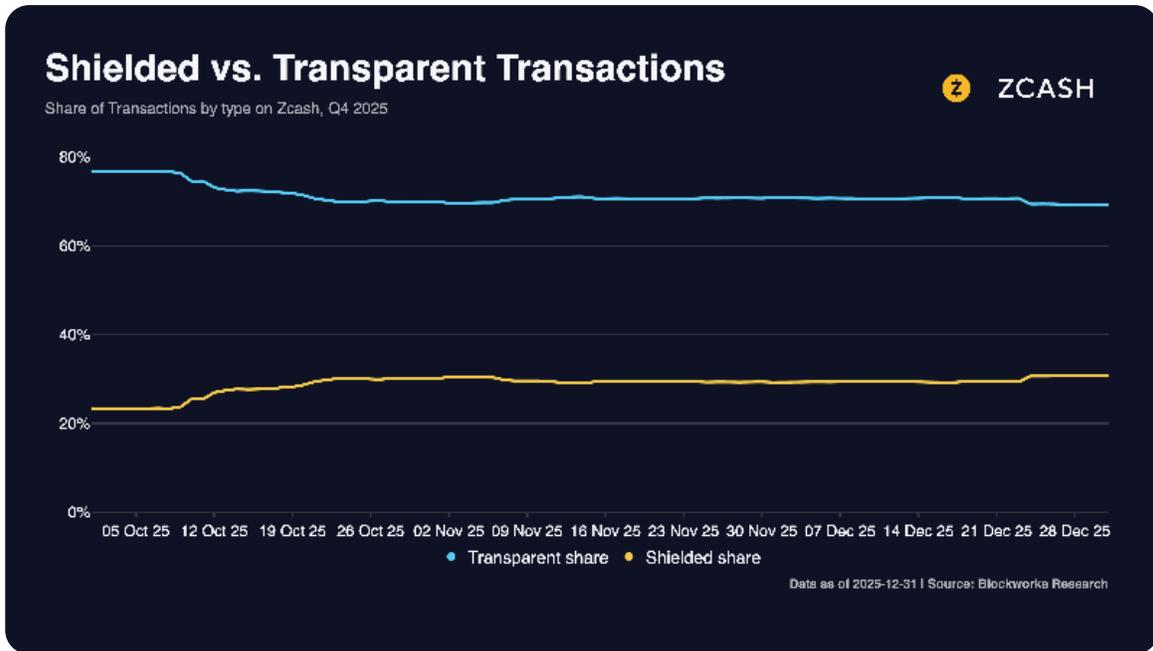
Daily shielded transaction count on Zcash, Q4 2025. Source: [Blockworks](#)

As such, shielded transactions represent real usage. The growth in shielded transactions indicates that Zcash is being used for its intended purpose: private, censorship-resistant money.

Q4 2025 saw 156,161 total shielded transactions, representing a 224.1% increase from Q3 2025. This growth occurred across all shielded pools, with Orchard transactions representing the majority of activity. The substantial increase in shielded transactions throughout the quarter indicates both a growing shielded user base and higher per-user activity, with users engaging in shielded transfers more frequently.

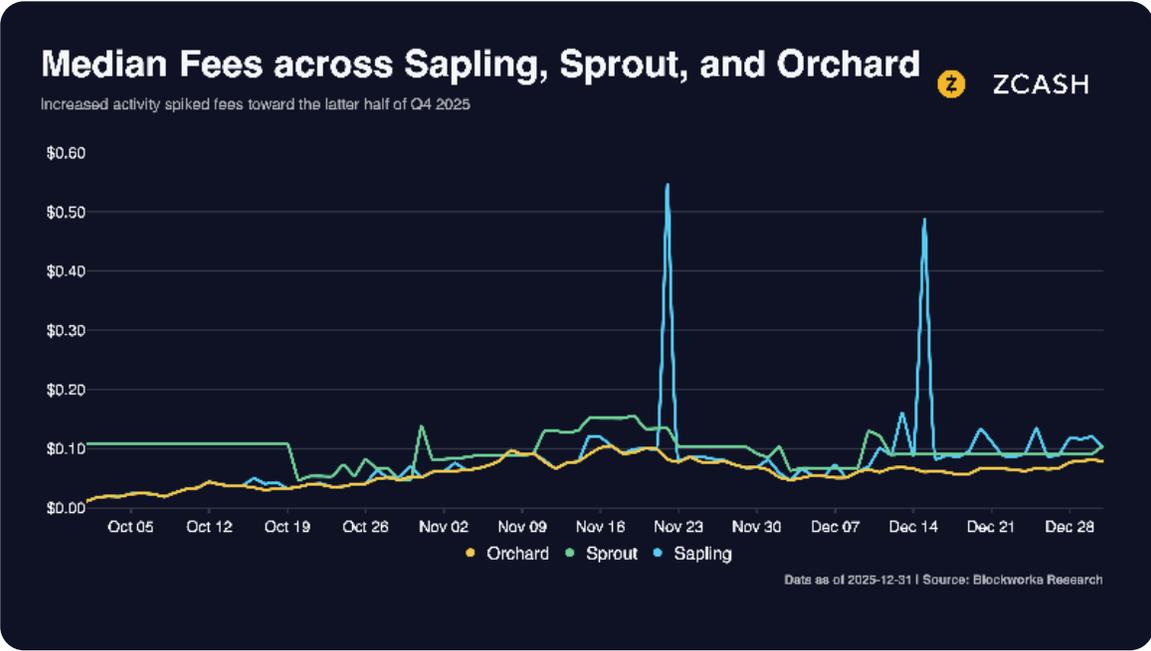
## Privacy Usage and Adoption

The ratio of shielded to transparent transactions provides insight into how users are choosing to interact with Zcash. As this ratio shifts toward shielded transactions, it indicates that privacy is becoming the default, not the exception. This is a critical signal for understanding Zcash's adoption trajectory and long-term value proposition.



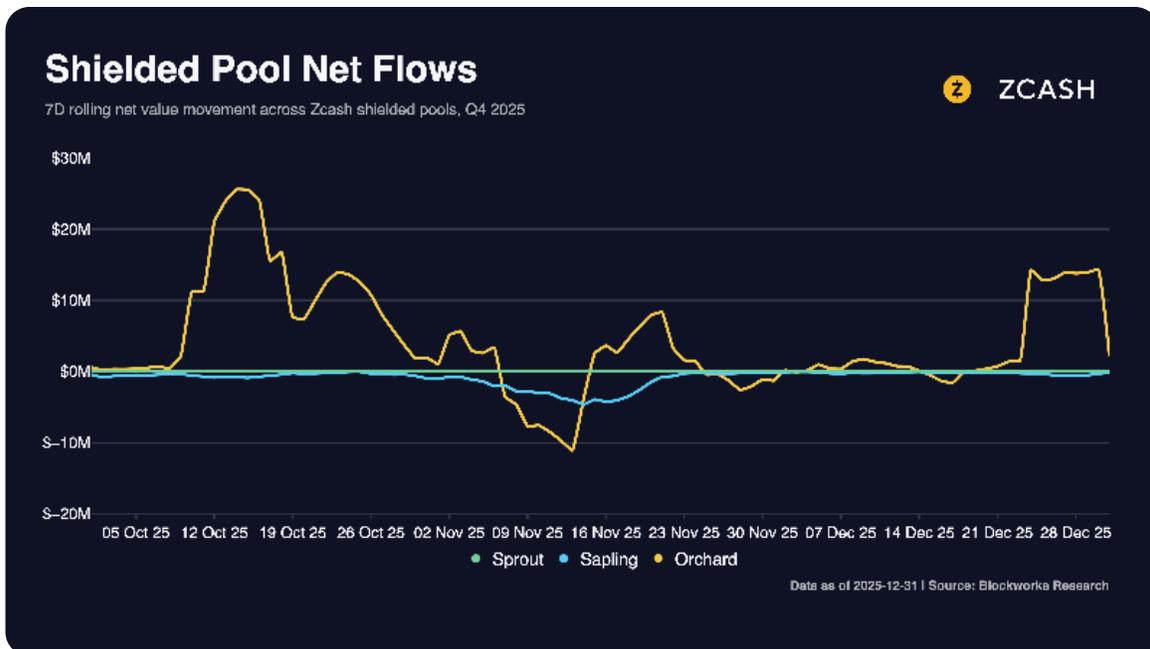
Share of transactions by type on Zcash, Q4 2025. Source: [Blockworks](#)

During Q4 2025, shielded transactions represented 18.9% of total transactions, down from 39.2% in Q3 2025. This decline in share reflects a substantial increase in transparent transaction volume during the quarter, which outpaced the growth in shielded transactions. However, the absolute number of shielded transactions increased significantly (224.1% quarter-over-quarter), indicating continued adoption of Zcash's privacy features even as overall network activity expanded. The decline in share should be interpreted in context: while the relative share decreased, absolute shielded transaction volume grew substantially, suggesting that privacy adoption is continuing even as transparent usage also increased.



Median Fees across Sapling, Sprout, and Orchard, Q4 2025. Source: [Blockworks](#)

For tokenholders, the substantial absolute growth in shielded transactions validates Zcash's core value proposition. Privacy is no longer just a theoretical benefit, it is being adopted in practice by an increasing number of users, even as overall network activity expands. This usage creates network effects: as more users adopt shielded transactions, the anonymity set grows, making privacy stronger for everyone.

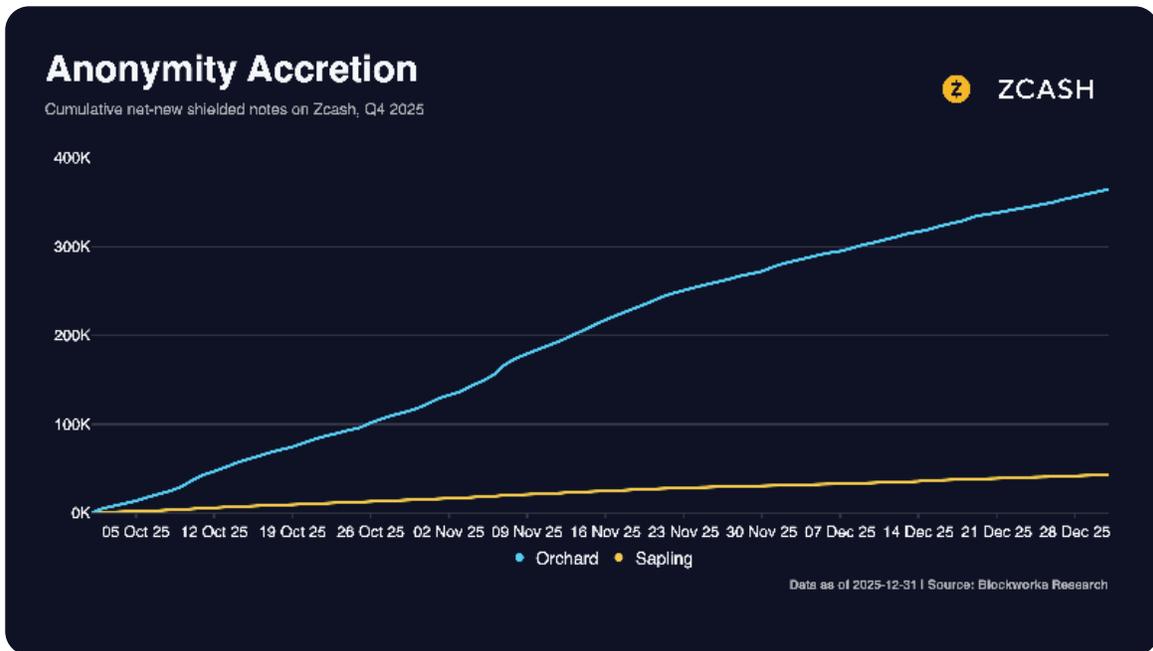


Shielded Pool Net Flows, Q4 2025. Source: [Blockworks](#)

## Anonymity Set Growth: Compounding Privacy

The anonymity set is Zcash's most defensible competitive advantage. Zcash's anonymity set refers to the total collection of shielded transactions within a given shielded pool from which any individual transaction cannot be distinguished. When a transaction is conducted using Zcash's shielded functionality, its sender, recipient, and value are cryptographically hidden and rendered indistinguishable from all other shielded activity in the same pool. The size and activity level of this pool directly determine the strength of privacy guarantees, as a larger anonymity set increases uncertainty for any external observer attempting transaction linkage. Consequently, growth in shielded usage strengthens privacy for all participants by expanding the effective anonymity set.

Unlike other privacy metrics, which can fluctuate with usage patterns, the anonymity set grows monotonically with every shielded transaction through the creation of shielded notes. This creates a compounding privacy benefit that becomes stronger over time and is impossible for competitors to replicate without starting from zero.

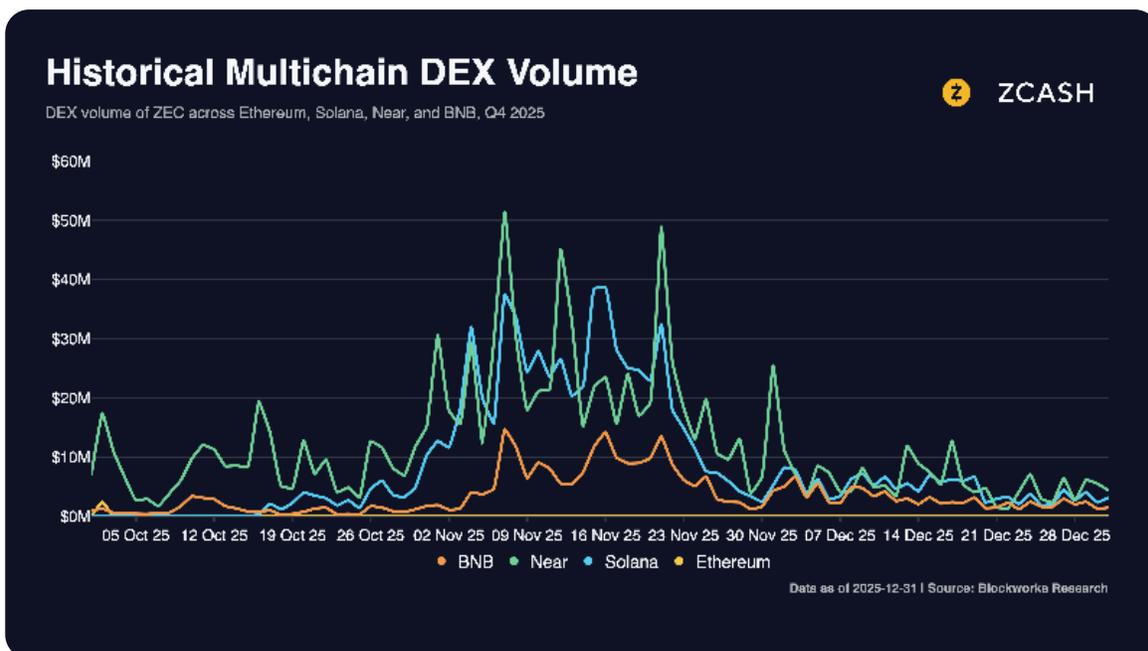


Cumulative net-new shielded notes on Zcash, Q4 2025. Source: [Blockworks](#)

Notes are the private units of value inside Zcash’s shielded pools, analogous to UTXOs in Bitcoin but fully encrypted. Each shielded transaction consumes existing notes and creates new ones, expanding the pool of indistinguishable value objects that underpin Zcash’s privacy guarantees. The total number of notes is therefore a meaningful metric to track, as a larger note set directly strengthens the anonymity and privacy of all shielded users. Importantly, notes are distinct from transactions: growth in notes reflects the expansion of Zcash’s privacy set rather than an increase in transaction volume, meaning note growth improves network-wide privacy even when transaction counts remain stable.

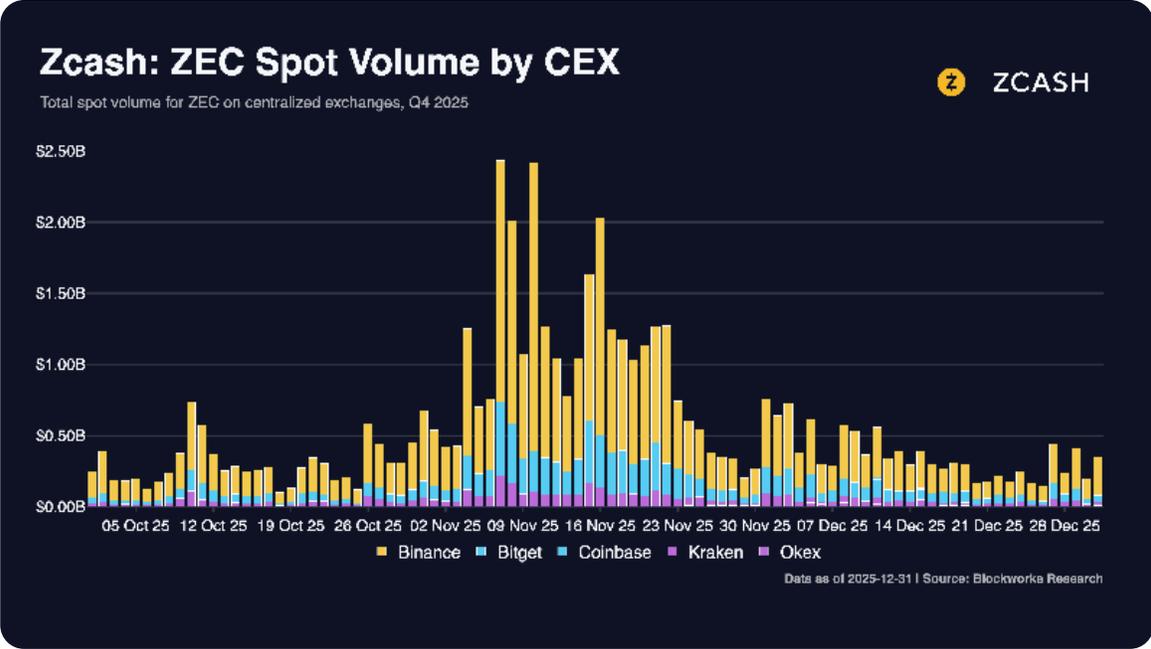
Q4 2025 saw the anonymity set grow by 407,686 notes, bringing the total to 123,454,995 notes. This growth occurred across all shielded pools, with Orchard notes representing the majority of new additions. The monotonic growth pattern demonstrates that Zcash’s privacy benefits compound over time. The anonymity set is perhaps the most important metric for understanding Zcash’s long-term value proposition. Unlike transaction volume or price, which can fluctuate, the anonymity set represents a permanent improvement to the protocol’s privacy guarantees. While market activity changes, the steady expansion of Zcash’s anonymity set represents a permanent, compounding improvement to the protocol’s privacy foundations.

## Cross-Chain Volumes and Activity

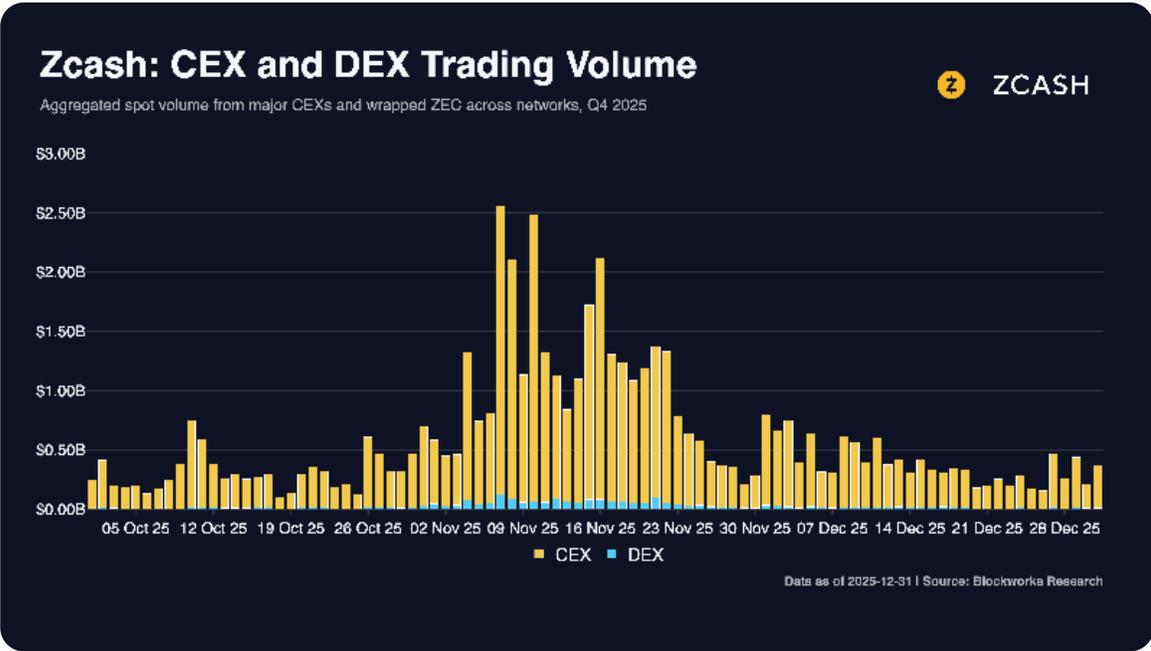


Historical Multichain DEX Volume, Q4 2025. Source: [Blockworks](#)

Against this backdrop of strengthening privacy infrastructure, Zcash also experienced episodic surges in cross-chain liquidity. Cross-chain DEX activity linked to Zcash rose sharply in early to mid-November before declining into a lower, more stable range by December. The increase was visible across multiple ecosystems, including Solana, NEAR, and Ethereum, indicating growth in all multichain sectors. This period coincided with heightened attention around Zcash's privacy stack and improvements in shielded usability, which may have catalyzed rapid capital movement and cross-chain rebalancing. Interestingly, NEAR received a high portion of this volume particularly because of its NEAR intents integration allowing for an improvement in UX for traders while being partnered with the Zcash app, Zodi.



Zcash: ZEC Spot Volume by CEX, Q4 2025. Source: [Blockworks](#)



Historical Multichain DEX Volume, Q4 2025. Source: [Blockworks](#)

ZEC spot trading activity was highly episodic during Q4 2025, with volume peaking sharply in early to mid-November before normalizing into December. The majority of activity occurred on centralized exchanges, particularly Binance, suggesting that price discovery and liquidity remained primarily CEX-driven during periods of heightened interest. Decentralized and cross-chain venues contributed a smaller but visible share of total volume, indicating growing, but still secondary, onchain participation.

# Institutional & Governance Maturity

Zcash's governance model is designed to preserve agility in deploying cryptographic breakthroughs, as demonstrated by the network's iterative evolution of privacy pools. Protocol changes are proposed through Zcash Improvement Proposals (ZIPs), which are implemented through an off-chain execution model involving three core actors: the Zcash Open Development Lab (ZODL), which serves as the primary protocol engineering team and implements most consensus-level ZIPs; the Zcash Foundation, an independent nonprofit steward that operates node infrastructure and funds development; and miners, who ultimately enforce consensus rules through software adoption.

In Q4 2025, Zcash introduced tokenholder voting to formalize community decision-making and align protocol direction with stakeholder preferences. Rather than replacing existing executors, token voting codified what had previously been informal social consensus, resolving coordination frictions between ZODL, the Zcash Foundation, and the broader community. This shift marked a transition toward more explicit, transparent governance while preserving Zcash's execution-driven model, positioning the protocol for greater long-term sustainability.

Additionally, in November, token holders used this system to vote on retroactive projects to receive funding from the Lockbox. Participation required moving ZEC into the shielded pools. 9 retroactive projects were presented and 5 passed:

- FPF: Admin for the Coinholder-Director Retroactive Grant Program
- Bitcoin VN
- Zcash Open Development Lab
- ZcashCommunity.com Hosting
- Unstoppable Wallet

## Entities and Goals

- Zcash Open Development Lab (ZODL): This team is the original engineering team that developed Zcash and serves as the primary service provider for developing Zcash as a product. Their main goal is to develop Zcash's mobile stack with the Zodi wallet and third party SDKs for alternative wallets. They also serve as the primary marketing and communication arm.

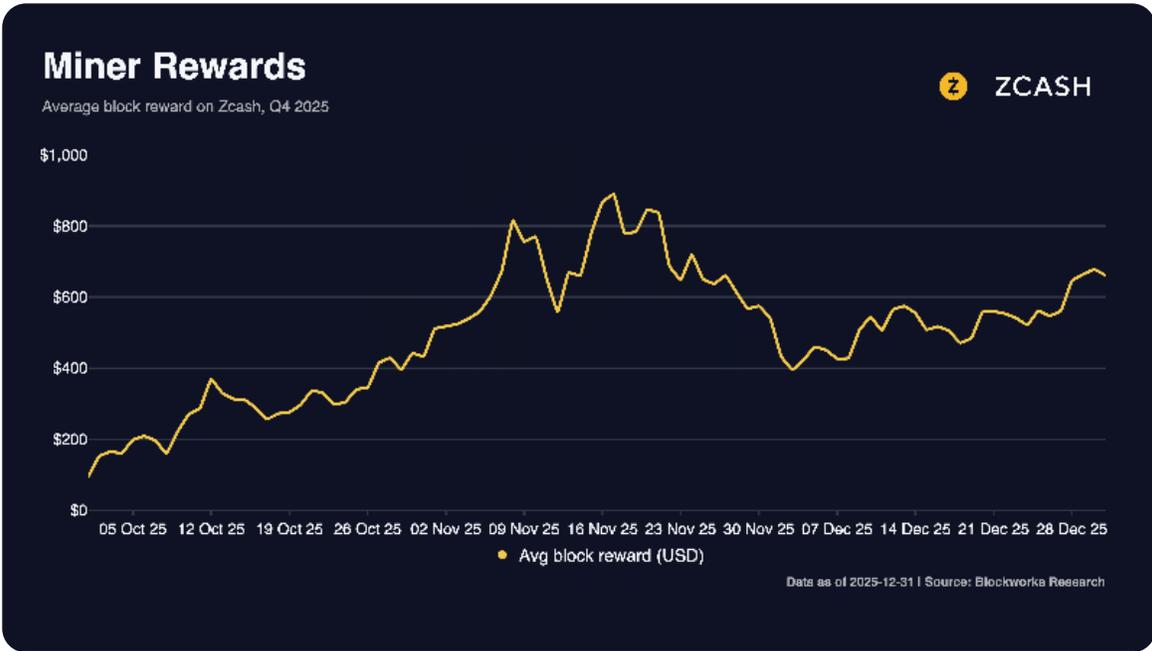
- Zcash Foundation (ZF): The Zcash foundation is a charity focused on privacy for public good. The ZF maintains the node implementation, Zebra, to enhance network client diversity. They also organize community events, like network upgrade community calls and the Zcon conference.
- Tachyon: Tachyon is a specialized engineering project and team committed to scaling Zcash. Their specific goal is to implement an ambitious architectural change that would enable scaling through recursive ZK proofs, a cryptographic technique for scaling and privacy.
- Shielded Labs: This team acts as a third party service provider research team. Their current goal is to propose and implement Crosslink, a hybrid system between Proof of Work and Proof of Stake.

### Why This Matters for Holders

The governance transition is fundamentally positive for Zcash tokenholders. First, it creates a more sustainable governance structure that can adapt to changing conditions without centralized control. The ZIP editors serve as funnels to keep the community directionally focused with their expertise on cryptography and Zcash's original message. Second, it aligns developer incentives with tokenholder interests, ensuring that protocol development serves the community. Third, it resolves prior governance tensions that created uncertainty and risk.

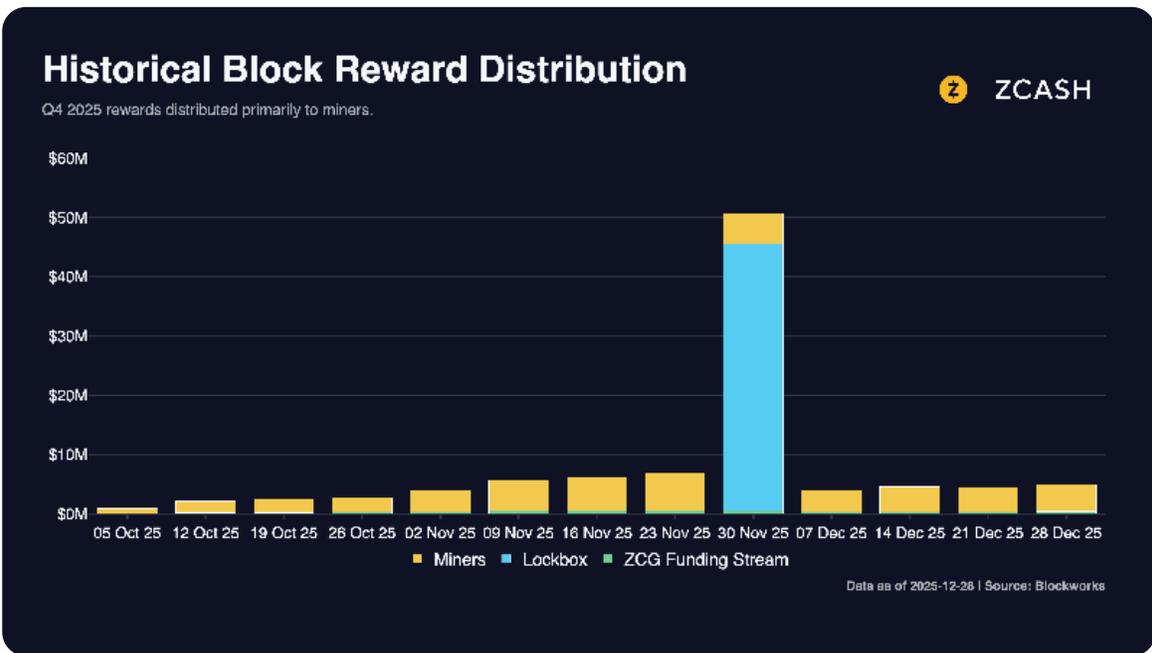
### Mining Rewards and Distribution

Overall, Zcash miner rewards increased materially over Q4 2025, reflecting both rising ZEC prices and steady block production. Average block rewards climbed from roughly the low-\$100 range in early October to peaks above \$800 in mid-November, before declining into early December and stabilizing in the \$500–\$650 range by quarter-end. In aggregate terms, block reward distribution during Q4 2025 was overwhelmingly directed to miners, who captured the vast majority of issuance across the quarter. A notable exception occurred in late November, during the introduction of NU 6.1, when a large, discrete Lockbox disbursement temporarily dominated weekly distributions, dwarfing routine miner rewards for that period. Outside of this event, Lockbox and ZCG Funding Stream allocations remained comparatively small and consistent, underscoring that Zcash's Q4 2025 issuance economics continued to be primarily miner-driven, with governance and ecosystem funding representing a secondary share of total block rewards.



Miner Rewards, Q4 2025. Source: [Blockworks](#)

The Lockbox disbursement observed in late Q4 2025 reflects Zcash’s post-NU6 funding architecture, in which a fixed share of block rewards is sequestered into a deferred funding pool rather than paid directly to predefined recipients. Unlike miner rewards or ongoing ZCG allocations, Lockbox funds accumulate over time and are only released following governance-driven activation or protocol-level transfer events. As a result, Lockbox activity appears as infrequent but large, discrete disbursements rather than steady weekly flows.



Historical Block Reward Distribution, Q4 2025. Source: [Blockworks](#)

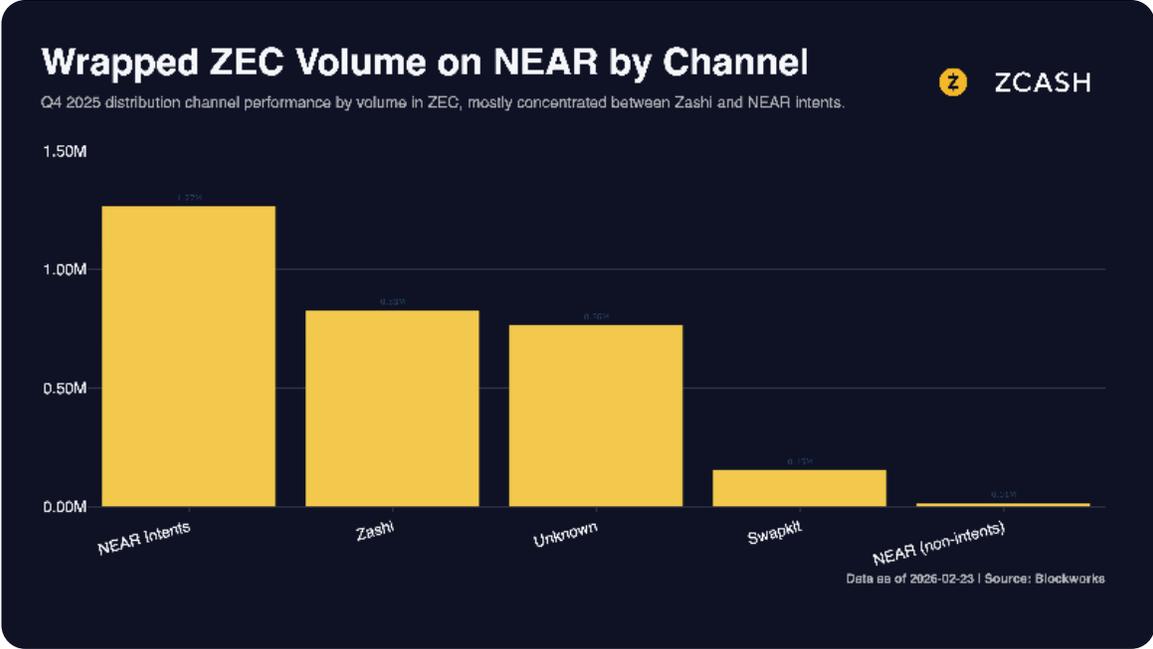
# Zodl Wallet Adoption

Q4 2025 saw significant progress in making Zcash more user accessible, with increased adoption from the wallet app Zodl and integration partnerships allowing Zodl to have a decentralized offramp solution, offer decentralized swaps in app, and make private crosschain payments.

Zodl Wallet is a mobile, self-custody wallet for Zcash, launched in 2024, focused specifically on shielded transactions. As such, all funds held and spent in Zodl are encrypted onchain and can be protected from public view at the user's will. It's built and maintained by Zcash Open Development Lab (ZODL), the original developers of Zcash, and is intended to dramatically lower the usability barriers that hindered adoption.

Zodl represents an improvement in Zcash's UX, making shielded transactions more accessible to mainstream users. The wallet interface simplifies the process of creating and managing shielded addresses, reducing the friction that previously limited adoption. Zodl has integrations like Zodl Swaps and CrossPay using intent-based systems (NEAR Intents) which have contributed millions of dollars in transaction volume tied to private swap and payment activity.

During Q4 2025, Zcash routinely processed hundreds of millions to over \$1B in daily transfer volume across transparent and shielded pools at the network level. The chart below focuses specifically on wrapped ZEC transfer activity on NEAR, examining the subset of volume that can be attributed to identifiable NEAR-side distribution channels, such as wallets and intent-based routing surfaces, rather than total Zcash protocol throughput. Within this attributed NEAR volume, NEAR Intents emerged as the largest distribution channel, contributing approximately \$501M in notional transfer volume, followed by Zodl at \$327M. Transfers categorized as Unknown totaled roughly \$300M, underscoring that a meaningful share of crosschain user activity remains unattributed to a specific interface. By comparison, Swapkit contributed \$59M, while non-intent NEAR flows were immaterial. Taken together, the data suggests that while overall Zcash transfer volume is broad and diffuse at the base-layer level, crosschain user-facing distribution on NEAR is increasingly concentrated in purpose-built wallets and intent-based routing layers.



Zodl’s mobile app has also gained tens of thousands of downloads on both iOS and Android, with over 25,000 users installed. Its ratings are strong (~4.9★) and suggest that it is in a healthy early user engagement phase. The adoption of Zodl is important because it demonstrates that Zcash can achieve mainstream usability while maintaining privacy guarantees. Previous wallet interfaces were too complex for average users, limiting adoption to technical users who understood the protocol’s intricacies.

# Scaling & Tachyon

Tachyon is Zcash's long-term scaling initiative, designed to enable billions of private transactions without compromising Zcash's core privacy guarantee: ledger indistinguishability. Its key insight is that today's scalability limits come not from zero-knowledge proofs themselves, but from how wallets and validators must continuously synchronize shared shielded state. Tachyon addresses this by redesigning how wallets interact with the blockchain, allowing Zcash to scale transaction throughput while keeping blocks small and verification efficient.

At a high level, Tachyon introduces oblivious synchronization, where wallets maintain cryptographic proofs that their state is valid up to a recent point in the chain. Transactions then carry succinct proof-carrying data showing correctness, rather than forcing validators and other wallets to reprocess historical state. This allows validators to prune old data, aggregate shielded transactions efficiently, and dramatically reduce state contention. The result is a credible path for Zcash to offer Bitcoin-like monetary properties with strong privacy at mainstream scale, rather than forcing users to trade privacy for usability.

## A Note on Post-Quantum Zcash

Post-quantum cryptography is slated for discussion and possible development, with the most concrete proposal being the Quantum Recoverable Orchard scheme. The concern is straightforward: quantum computers will eventually be able to break the elliptic curve cryptography that currently secures Zcash's primary shielded pool (Orchard).

The Zcash team's proposed fix is notable for its pragmatism, rather than requiring a full protocol overhaul, the recovery mechanism reduces security down to hash functions, which quantum computers have no known advantage against. Half the problem (proving you own your funds) turns out to already be quantum-safe due to a forward-looking design choice baked into Orchard wallets since launch.

The remaining fix, securing note commitments, requires only a change to wallet-level conventions, not a consensus-breaking upgrade. When the time comes, the full migration path involves rebuilding a quantum-safe Merkle tree and verifying ownership through a post-quantum STARK proof, with users moving funds into a new quantum-resistant shielded pool. The key takeaway for stakeholders: Zcash has a credible, low-friction path to quantum resistance that doesn't require an emergency hard fork, and the groundwork is already partially in place.

# Investor Endorsements

Zcash's value proposition is increasingly recognized by institutional investors and thought leaders in the crypto space. This external validation provides credibility and supports adoption by demonstrating that privacy is a legitimate and valuable monetary property.



*“Privacy is the next frontier in crypto. It’s the point at which government and corporate overreach end and your freedom and self-sovereignty begin.”*

— **Cameron Winklevoss**



*“Zcash has completely decoupled from broader market sentiment, which is extremely rare for an asset of this size.”*

— **Simon Dedic, Moonrock Capital**



*“Bitcoin is insurance against fiat. ZCash is insurance against Bitcoin.”*

— **Naval Ravikant, Entrepreneur**

*“Bitcoin is where you store value, and Zcash is where you transact... encrypted Bitcoin.”* — **Tyler Winklevoss**

*“Privacy is normal — Zcash (\$ZEC) helps make private, on-chain transactions possible.”* — **Grayscale**

*“The choice is clear. It’s Zcash or communism.”* — **Balaji Srinivasan, Former Coinbase CTO**

# Closing Summary & Outlook

Q4 2025 represented a critical inflection point for Zcash. The quarter demonstrated that privacy-maximalist design, when combined with improved governance, infrastructure, and user experience, can achieve meaningful adoption and position the protocol for long-term success.

The quarter saw strong growth across all privacy indicators. Shielded pool holdings reached 5,067,532 ZEC (30.8% of circulating supply), with Orchard pools representing 87.1% of private holdings. Total shielded transactions increased 224.1% quarter-over-quarter, demonstrating real-world adoption beyond speculative activity. Most importantly, the anonymity set continued its monotonic growth, adding 407,686 notes in Q4 2025—the compounding privacy benefit that represents Zcash’s most defensible competitive advantage.

Furthermore, the establishment of tokenholder voting as the primary governance mechanism resolved long-standing tensions and created a more sustainable, decentralized governance structure. The re-establishment of developer funding through community grants and token-based voting has aligned incentives across developers, users, and capital providers.

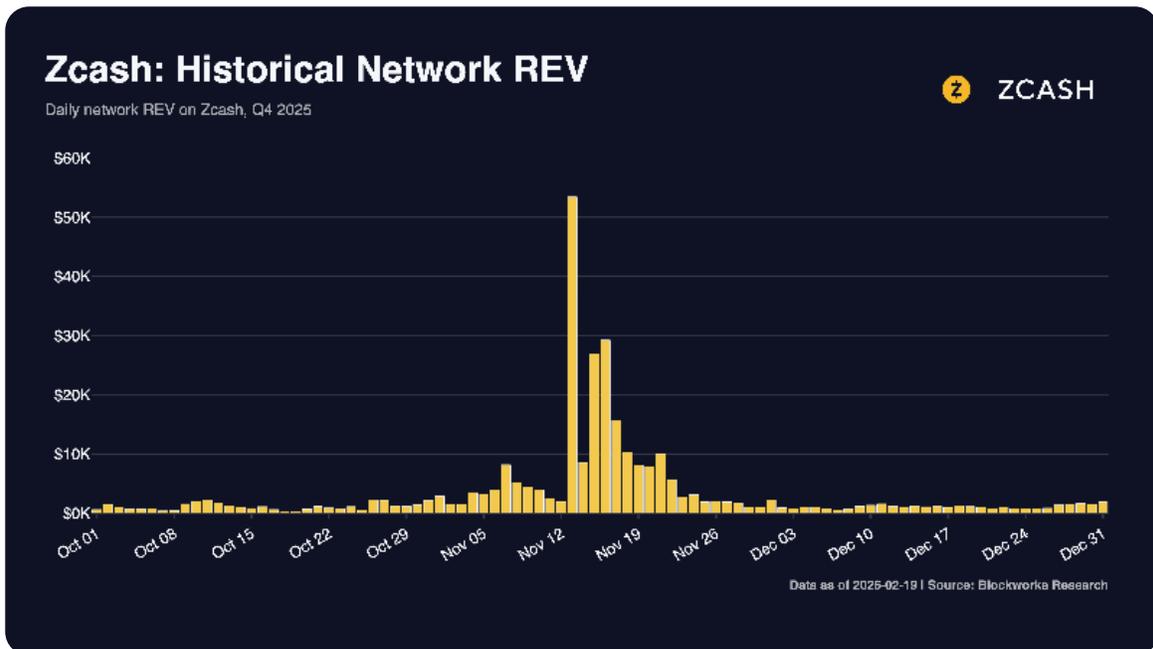
Finally, the launch of the Zodi wallet and continued development of Tachyon represent critical infrastructure investments that enable Zcash to scale to billions of users while maintaining its core privacy guarantees. These improvements make Zcash more accessible, scalable, and user-friendly while preserving its core privacy properties.

# Appendix: Financials and Secondary Metrics

The following metrics provide additional context on Zcash's network activity and economic health. These metrics are included for completeness but are not the primary focus of this report, which emphasizes privacy adoption and monetary integrity as Zcash's core value proposition.

## Network REV (Real Economic Value)

Network revenue represents the total fees paid to miners and represents the economic activity on the Zcash network. While this metric is less directly tied to Zcash's core value proposition (privacy), it provides insight into overall network activity and economic health.



Daily network REV on Zcash, Q4 2025. Source: [Blockworks](#)