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.

Q1 2026

Blockworks Advisory

Table of Contents

Executive Summary

Zcash's Q1 2026 performance reflected continued strengthening in its core privacy fundamentals, even as overall network activity normalized from elevated Q4 levels. Shielded pool holdings increased to 5.16M ZEC, representing 31.0% of circulating supply (+20bps QoQ), while Orchard's share rose to 87.6%, indicating continued consolidation into the network's primary shielded pool. The anonymity set expanded by 301K notes to 123.76M, sustaining growth in Zcash's underlying privacy guarantees.

Network activity moderated during the quarter, though privacy-preserving usage remained relatively resilient. Shielded transactions declined 24.1% QoQ to 118,484, while total transactions fell more sharply to 559,640 (-40.0% QoQ). As a result, shielded transactions increased as a share of activity to 21.2% (vs. 16.7% in Q4). While transaction-level flows skewed toward deshielding (46.7K shielding vs. 69.7K deshielding), shielded balances continued to grow, suggesting sustained demand for private holdings.

Economic activity tracked lower alongside usage. Network REV declined 79.1% QoQ to $64.2K, and median transaction fees fell 52.2% to $0.0445, reinforcing Zcash's positioning as a low-cost network for private value transfer.

Q1 also marked a significant organizational transition. The departure of the Electric Coin Company development team led to the formation of ZODL and a $25M+ fundraise, while the SEC closed its investigation into the Zcash Foundation without enforcement action. Network fundamentals strengthened further, with hashrate reaching an all-time high of 16.54 GS/s and shielded supply setting a new peak.

Overall, Zcash exited Q1 with stronger privacy fundamentals and improving institutional positioning, despite a normalization in activity and fee generation.

Network & Privacy Performance

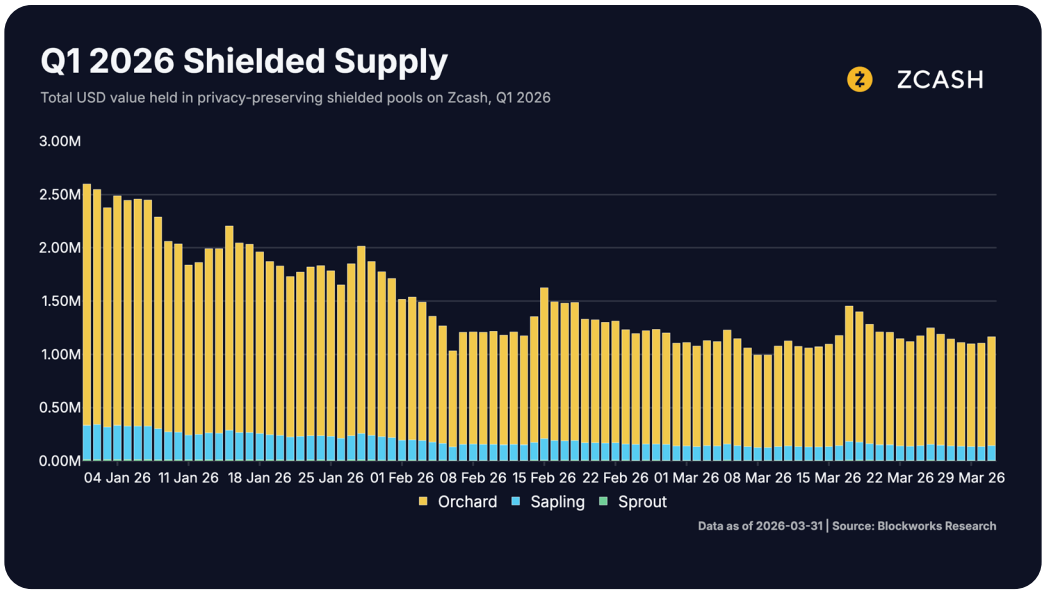
Zcash Value Proposition

Zcash is a proof-of-work blockchain launched in 2016 whose sole purpose is to function as encrypted digital money. Unlike Bitcoin, where every transaction is publicly visible on a transparent ledger, Zcash uses zero-knowledge proofs (zk-SNARKs) to allow users to send and receive value without revealing the sender, recipient, or amount to anyone observing the blockchain. Zcash is not a smart contract platform, a DeFi protocol, or an application layer. It is a monetary network designed to do one thing: move value privately. Its native currency, ZEC, has a fixed supply of 21 million coins (the same as Bitcoin) and is mined through PoW consensus.

Privacy remains Zcash's core differentiator and primary source of long-term defensibility. Unlike transparent blockchains, where balances and flows are publicly observable, Zcash's shielded pools allow users to hold and transfer value without exposing transaction details onchain. As a result, the most important indicators of network health are not raw throughput or fee generation, but rather the size of shielded balances, the level of shielded usage, and the continued growth of the anonymity set.

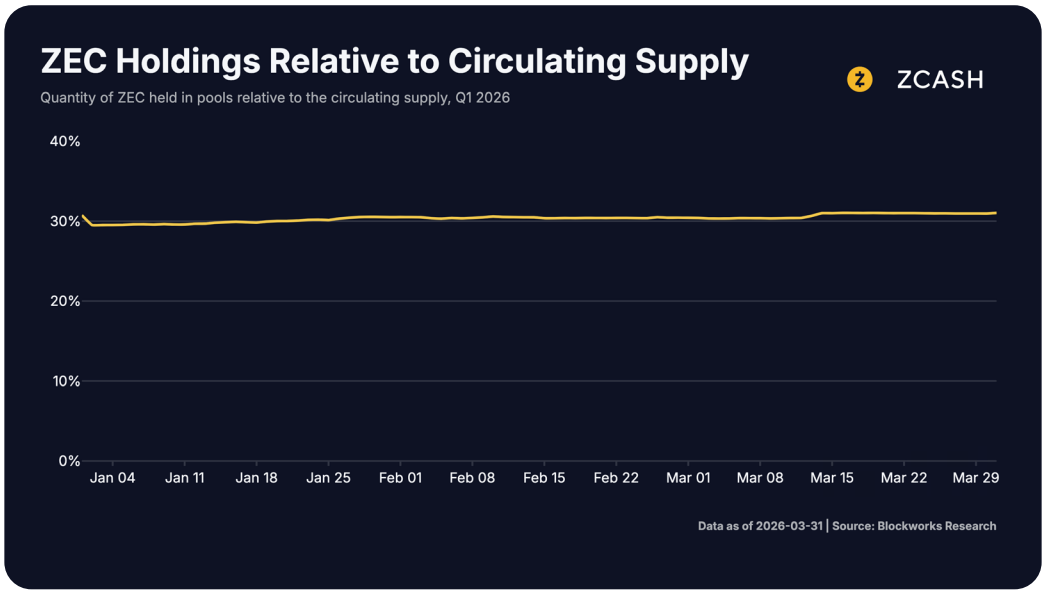
Shielded Pool Size

Shielded pool balances continued to expand in Q1, even as broader network activity cooled from Q4's stronger base. By quarter-end, 5.16 million ZEC were held in shielded pools, up 1.9% QoQ from 5.07 million ZEC in Q4. Shielded balances also increased as a share of total onchain supply, rising to 31.0% from 30.8% in the prior quarter. This continued increase is significant because shielded pool holdings represent the clearest stock measure of committed privacy usage. Funds held in shielded pools are more likely to reflect deliberate privacy preference and longer-duration conviction than transparent balances, which are easier to monitor and quicker to reposition.



Q1 2026 Shielded Supply (USD) Total USD value held in privacy-preserving shielded pools on Zcash, Q1 2026. Stacked by pool (Orchard, Sapling, Sprout). Source: Blockworks

Composition within shielded supply also continued to improve. Orchard accounted for 87.6% of shielded balances at the end of Q1, up from 87.1% in Q4, while Sapling and Sprout continued to decline as a share of private holdings. This ongoing consolidation into Orchard strengthens Zcash's privacy architecture by reducing fragmentation across shielded pools and concentrating more activity into the network's dominant modern privacy set.

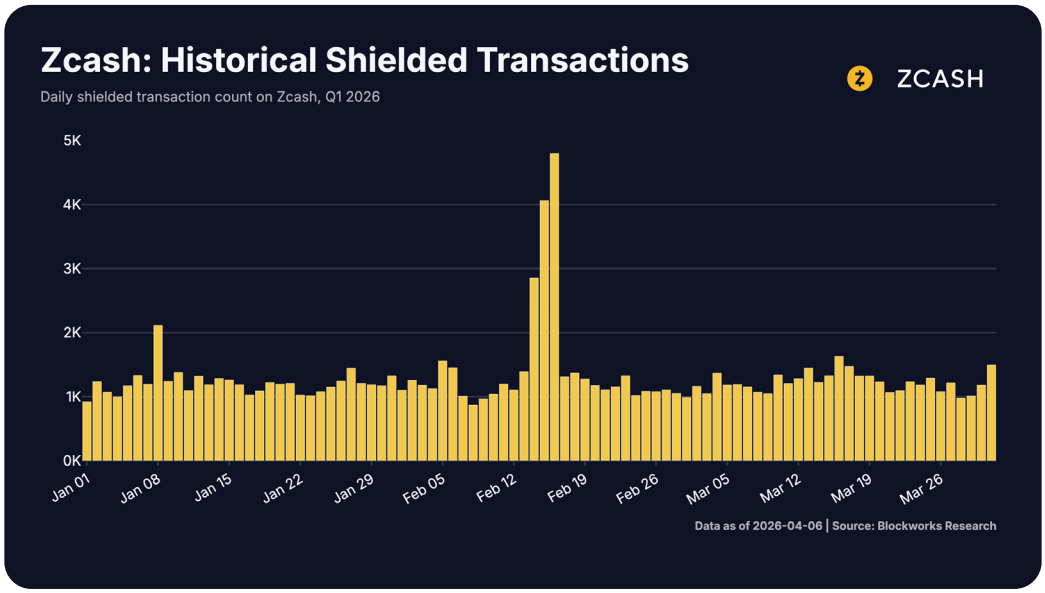


ZEC Holdings Relative to Circulating Supply Percentage of ZEC held in shielded pools relative to the circulating supply, Q1 2026. Source: Blockworks

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 and represents holders who have made a deliberate choice to preserve privacy.

Shielded Transaction Growth

Transaction activity moderated in Q1 following the unusually strong Q4. Zcash processed 118,484 shielded transactions during the quarter, down 24.1% QoQ from 156,161 in Q4. Total transactions fell more sharply, declining 40.0% QoQ to 559,640. On the surface, this looks like a weaker quarter for activity overall, but the relative performance of shielded transactions tells a more constructive story.

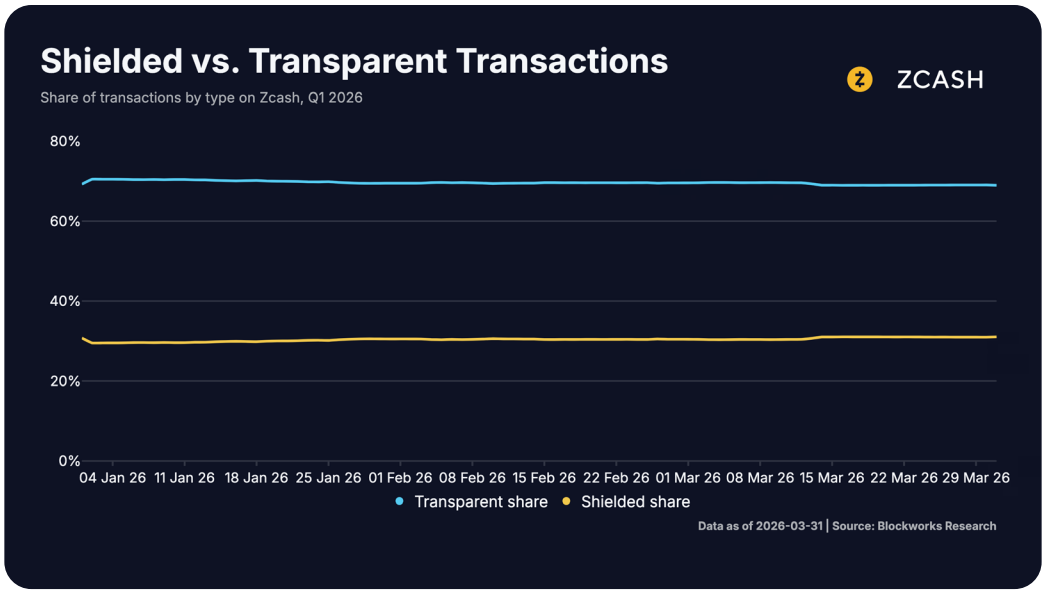


Historical Shielded Transactions Daily shielded transaction count on Zcash, Q1 2026. Source: Blockworks

Because shielded activity contracted materially less than total activity, privacy-preserving usage proved more resilient than the network as a whole. This suggests that while speculative or incidental transaction volume cooled in Q1, users who rely on Zcash for its privacy properties remained more consistent. Raw transaction volume can be noisy and influenced by temporary conditions. Still, shielded transactions are generally a stronger signal of intentional use because entering or exiting privacy requires explicit user action. In that sense, Q1's decline in shielded transaction count should be read as normalization from an elevated prior quarter rather than as a reversal in privacy adoption.

Privacy Usage and Adoption

The relationship between shielded and transparent usage improved in Q1. Using non-coinbase transactions, shielded transactions represented 21.2% of total activity in Q1, up from 18.9% in Q4. This increase occurred despite the absolute decline in shielded transactions because transparent and other non-shielded activity fell even faster. In other words, privacy usage gained share during the quarter.



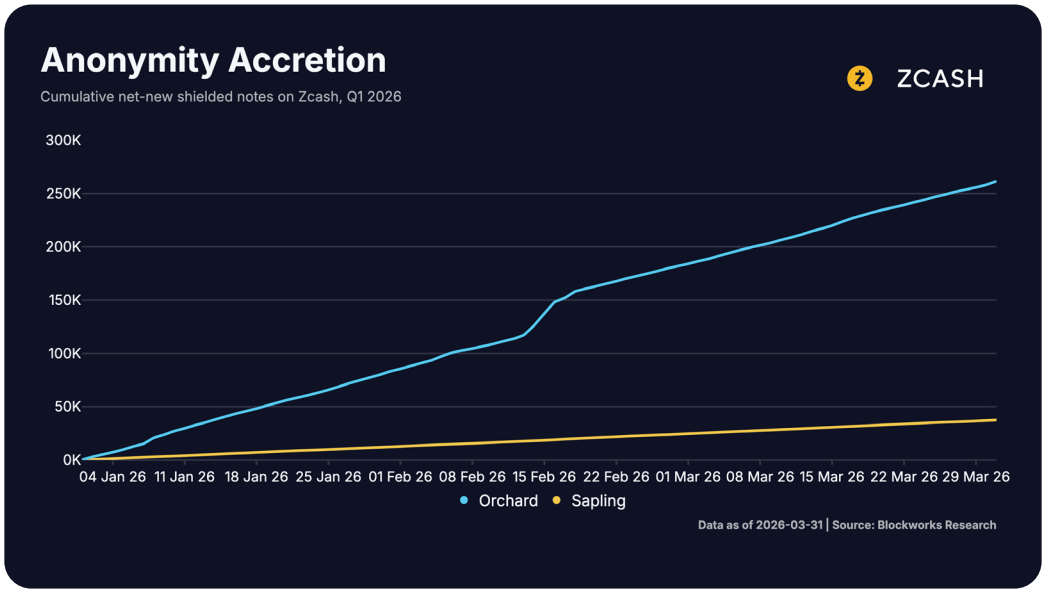
Shielded vs. Transparent Transactions Share of transactions by type on Zcash, Q1 2026. Source: Blockworks

This is an important signal for understanding how users are choosing to interact with the network. In Q4, the main takeaway was that privacy usage was growing quickly in absolute terms, even as transparent activity expanded even faster. In Q1, the dynamic shifted: absolute activity cooled, but privacy-preserving transactions held up better than the rest of the network.

Flow-level data adds another layer of nuance. Q1 recorded 46,693 shielding transactions and 69,676 deshielding transactions, with only 61 internal shielded transfers identified across Sapling and Orchard. On a transaction-count basis, this indicates more exits from shielded pools than entries during the quarter. However, this should not be overinterpreted as a collapse in privacy demand, because shielded balances still increased over the same period.

Anonymity Set Growth

The anonymity set continued to grow in Q1, reinforcing Zcash's strongest structural advantage. Total shielded notes increased by 301,324 during the quarter, bringing the total anonymity set to 123.76 million notes by quarter-end. This was slower than the 407,686-note increase recorded in Q4, but still represents meaningful continued compounding of Zcash's privacy guarantees.



Anonymity Accretion Cumulative net-new shielded notes on Zcash, Q1 2026. Source: Blockworks

Zcash's anonymity set refers to the total collection of shielded notes—encrypted units of value, analogous to UTXOs in Bitcoin—within its shielded pools. Each shielded transaction consumes existing notes and creates new ones, expanding the pool of indistinguishable value objects that underpin the network's privacy guarantees.

This metric remains one of the most important in the network. Unlike many crypto metrics, anonymity set growth is difficult to manufacture and directly tied to the usefulness of the protocol's privacy system. It also grows monotonically, the anonymity set can only expand, creating a compounding privacy benefit that strengthens over time and is impossible for competitors to replicate without starting from zero.

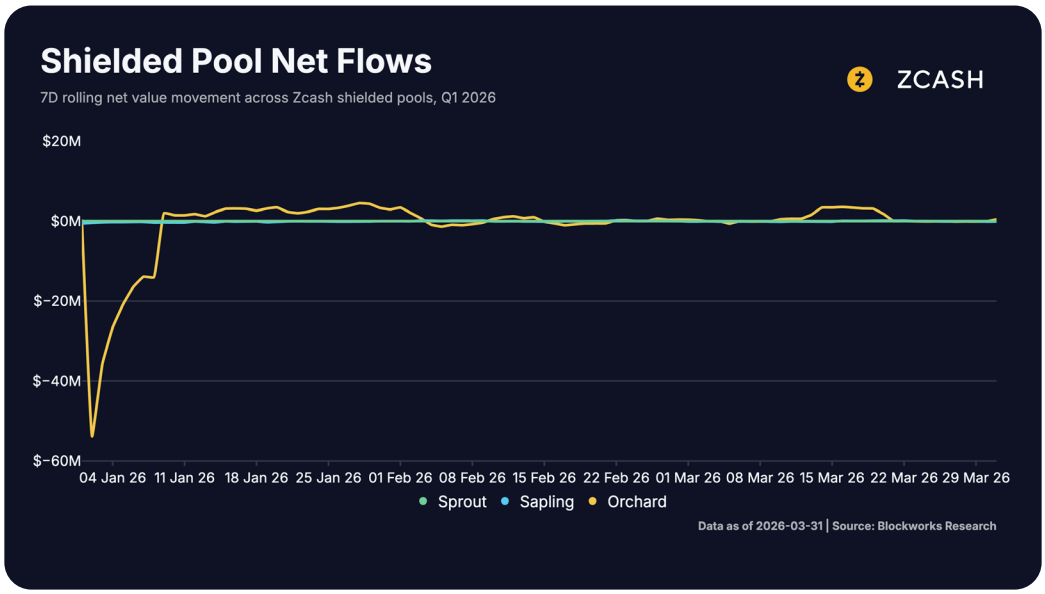
Taken together, Q1 presented a mixed but ultimately constructive picture for privacy adoption. Shielded transactions declined from Q4's elevated level, but shielded balances grew, privacy usage gained share of total activity, and the anonymity set continued to expand. The result is a network whose most important privacy fundamentals remain intact and, in several respects, continue to strengthen.

Supply, Flows, and Usage

While shielded balances and transaction counts provide a high-level view of privacy adoption, flow-level data offers a more granular perspective on how users are actually interacting with Zcash's privacy system. In particular, flows between transparent and shielded pools—and within shielded pools themselves—help distinguish between one-time usage, persistent adoption, and transactional behavior within privacy.

Shielding and Deshielding Activity

Flow activity in Q1 was characterized by a higher number of exits from shielded pools than entries on a transaction basis. Over the quarter, Zcash recorded 46,693 shielding transactions compared to 69,676 deshielding transactions, indicating that more transactions involved funds leaving privacy than entering it.



Shielded Pool Net Flows 7-day rolling net value movement across Zcash shielded pools, Q1 2026. Source: Blockworks

At face value, this could suggest weakening privacy usage. However, this interpretation is incomplete without considering balance-level dynamics. Despite higher deshielding activity, total shielded supply increased over the same period. This divergence indicates that shielding transactions in Q1 were likely larger on average or associated with longer-duration holdings, while deshielding activity may have been more frequent but smaller in size. In other words, transaction count alone understates the persistence of capital within shielded pools.

This distinction is important. A system where funds enter privacy in fewer but larger increments, and remain there, can still reflect strong privacy demand even if exit transactions are more numerous. Q1's data suggests that shielded usage may be shifting away from high-frequency entry and exit toward more stable balance retention.

Intra-Shielded Activity

Internal activity within shielded pools remained limited in Q1. The privacy-flows dataset recorded 61 internal shielded transactions across Sapling and Orchard, indicating that most shielded interactions involved movement into or out of privacy rather than transactions fully contained within shielded pools.

This has two implications: (1) it suggests that shielded pools are still used primarily as endpoints for value storage or transfer rather than as fully self-contained transactional environments; (2), it highlights a potential area of growth for Zcash: increasing intra-shielded economic activity would further strengthen privacy guarantees by reducing the need for funds to exit into transparent pools for usage.

At the same time, it is important to recognize that intra-shielded activity is more difficult to measure than entry and exit flows, and transaction-level counts may not fully capture economic activity occurring within privacy.

Transfer Volume and External Activity

Total onchain transfer volume was $25.1B in Q1, normalizing from $58.6B in Q4's unusually active period. The composition remained weighted toward transparent activity (90.1% of volume), with Orchard contributing a growing 8.3% share and Sapling at 1.6%. Importantly, the moderation in volume did not correspond to a decline in shielded balances, reinforcing the view that privacy usage remained stable even as the market cooled.

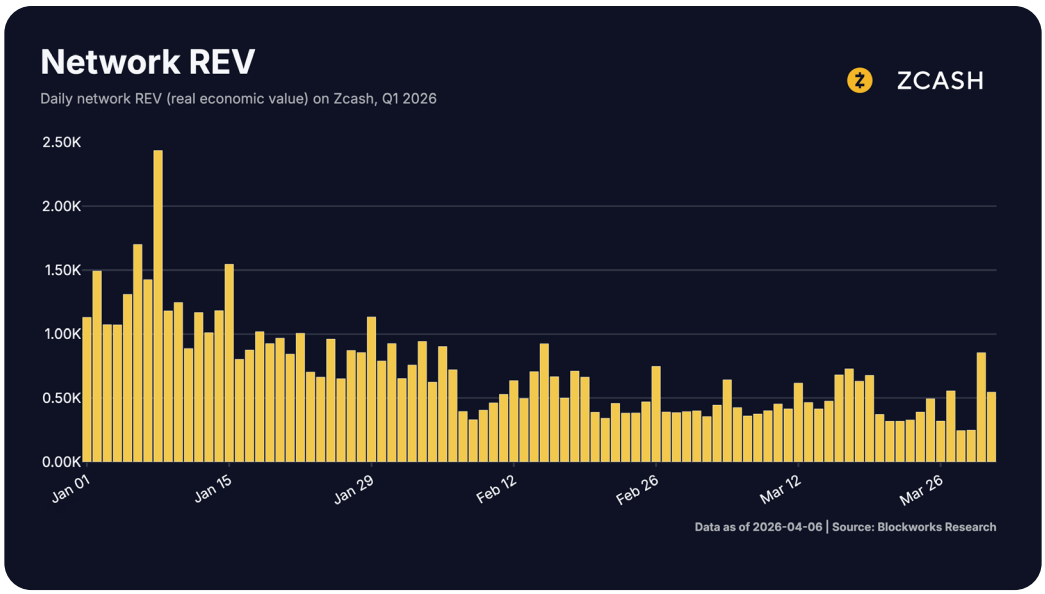
Across external venues, combined CEX and DEX trading volume was $13.9B, while wrapped ZEC supply on other chains totaled 219,881 ZEC (~$50.9M) at quarter-end—up 8.2% in ZEC terms from Q4, though still representing approximately 1.3% of circulating supply. The continued growth in wrapped supply suggests expanding multichain reach, while the concentration of value on the native chain reflects Zcash's core positioning as a self-contained private monetary network.

Market Structure & Economic Activity

While privacy metrics define Zcash's long-term value proposition, market structure and economic activity provide important context for how the asset is used and valued across both onchain and offchain environments. In contrast to high-throughput smart contract platforms, Zcash's economic model is not centered on fee maximization or application-layer revenue. Instead, its activity is better understood through transaction costs, miner-captured value, and trading dynamics across centralized and decentralized venues.

Network Revenue (Real Economic Value)

Network revenue declined materially in Q1 following the elevated activity observed in Q4. Zcash generated approximately $64.2K in Real Economic Value (REV) during the quarter, down 79.1% QoQ from $307.0K in Q4.



Network REV Daily network REV (real economic value) on Zcash, Q1 2026. Source: Blockworks

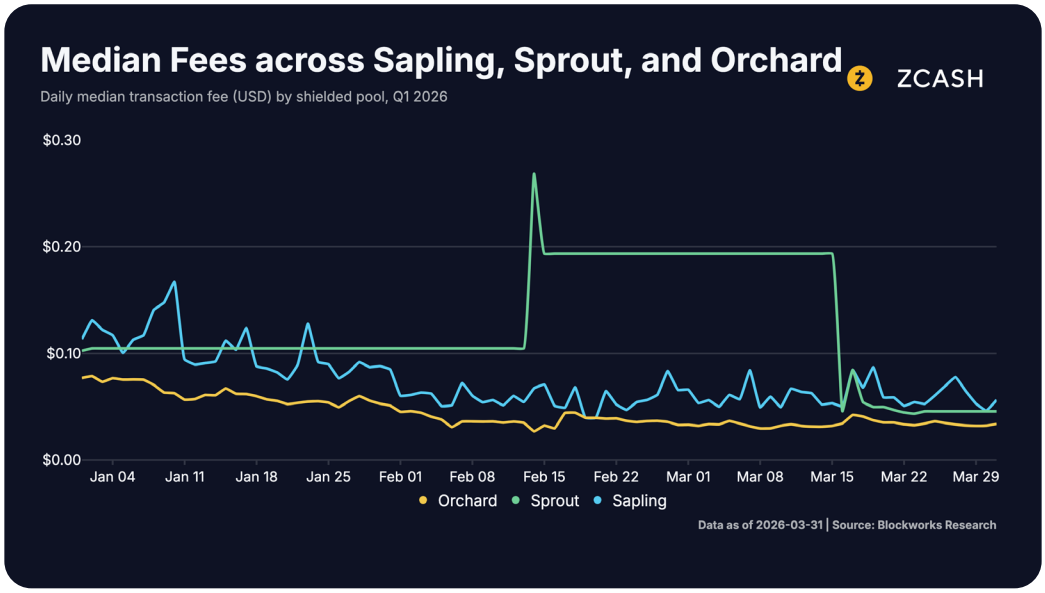
This decline was primarily driven by lower transaction activity rather than any structural change in fee dynamics. Because Zcash's fee model is linear and does not rely on congestion-based pricing or MEV extraction, network revenue scales directly with usage rather than with demand for blockspace. As activity cooled in Q1, REV followed proportionally.

Importantly, this reduction in revenue should not be interpreted as a weakening of the network's economic model. Unlike fee-maximizing chains, Zcash is designed

to minimize user costs, not extract value from them. As a result, lower REV in a period of reduced activity is consistent with its intended design rather than indicative of declining utility.

Transaction Fees

Transaction fees declined alongside overall network activity, reinforcing Zcash's low-cost execution environment. Median transaction fees averaged approximately $0.0445 in Q1, down 52.2% QoQ from $0.0931 in Q4.



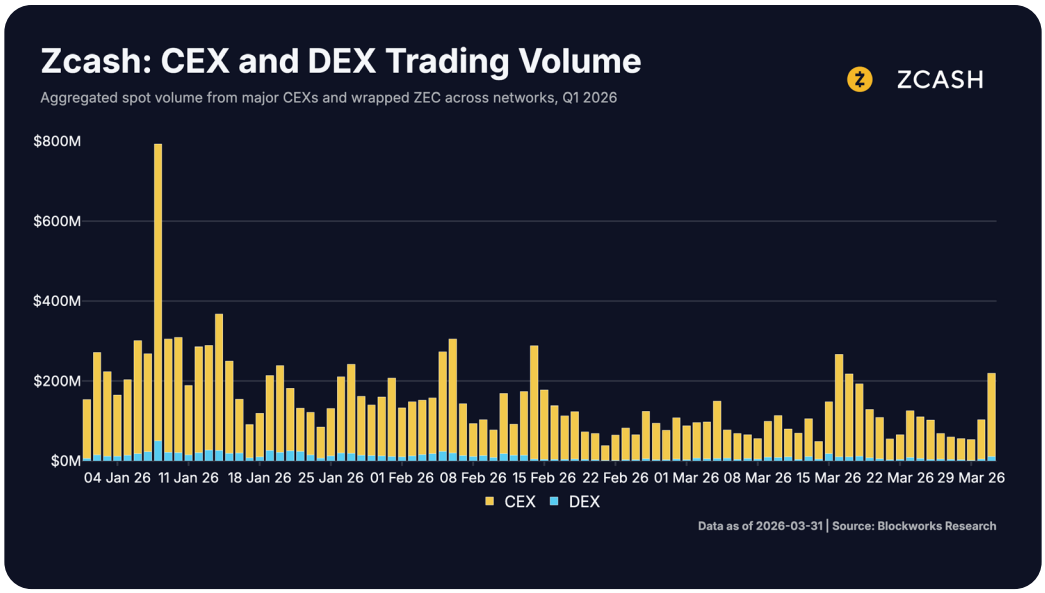
Median Fees across Sapling, Sprout, and Orchard Daily median transaction fee (USD) by shielded pool, Q1 2026. Source: Blockworks

At these levels, transaction costs remain economically negligible for most use cases, including private transfers, savings, and frequent movement of funds. The persistence of low fees is a defining feature of the network. Rather than competing on throughput or fee generation, Zcash enables users to transact privately without incurring meaningful economic friction.

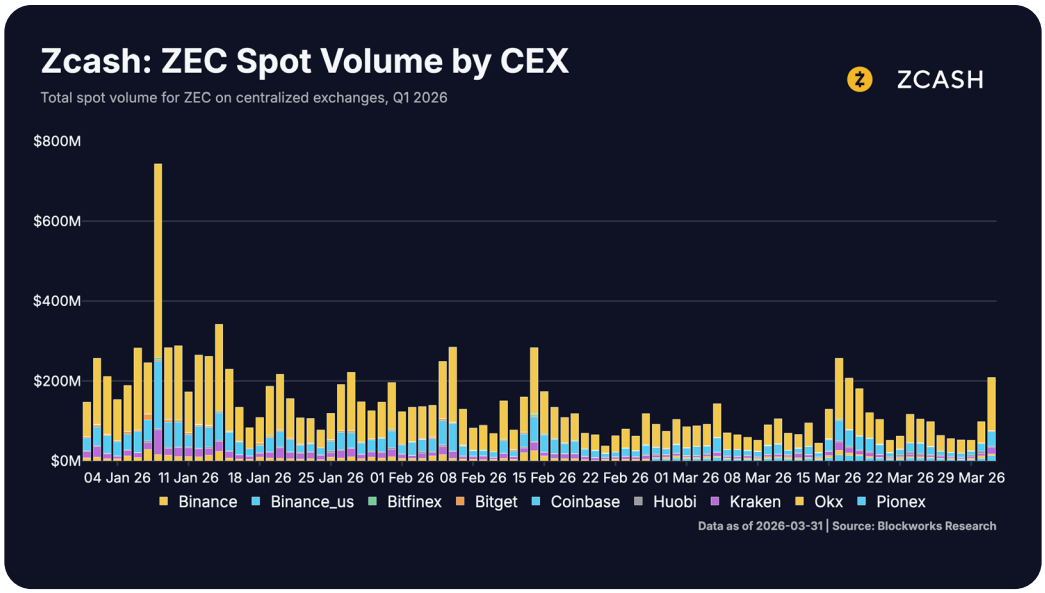
The combination of declining fees and declining REV reflects reduced activity rather than increasing costs. In contrast to networks where higher fees can signal congestion or demand pressure, Zcash's fee structure ensures that cost remains low regardless of activity levels. This makes it particularly well-suited for use cases where predictability and affordability are more important than blockspace competition.

Trading Activity (CEX and DEX)

Combined CEX and DEX trading volume for ZEC totaled $13.9B in Q1, moderating from Q4's elevated $54.0B base. CEX venues accounted for $12.9B (92.7% of total), led by Binance (61.5% share), Coinbase (20.7%), and Kraken (7.8%). DEX volume contributed $1.01B, and notably, DEX's share of total trading increased from 4.6% in Q4 to 7.3% in Q1, suggesting that decentralized venues are gaining relative adoption even as overall volumes normalize.



CEX and DEX Trading Volume Aggregated spot volume from major CEXs and wrapped ZEC across networks, Q1 2026. Source: Blockworks

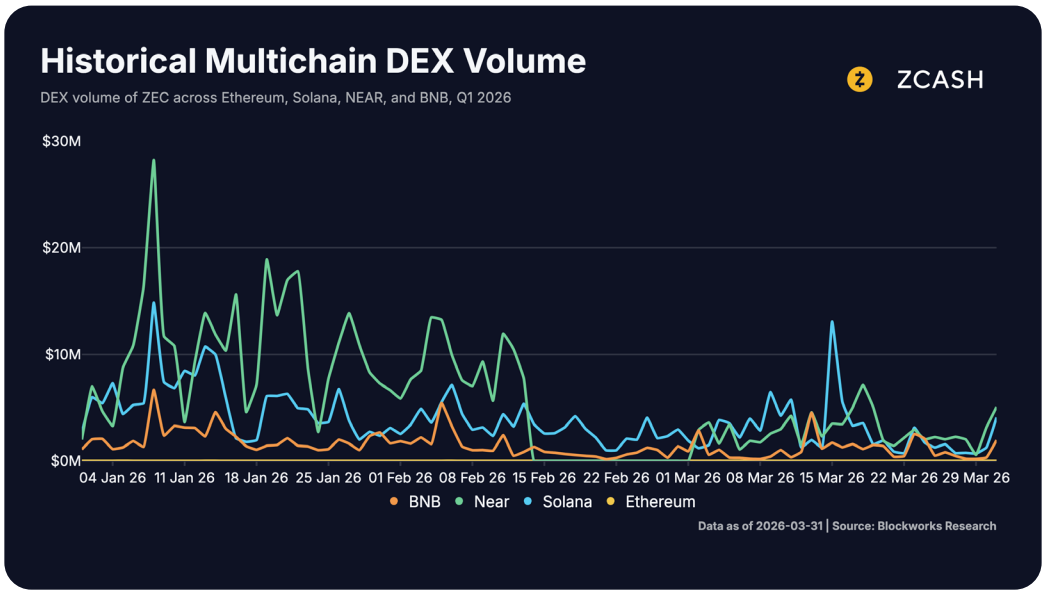


ZEC Spot Volume by CEX Total spot volume for ZEC on centralized exchanges, Q1 2026. Source: Blockworks

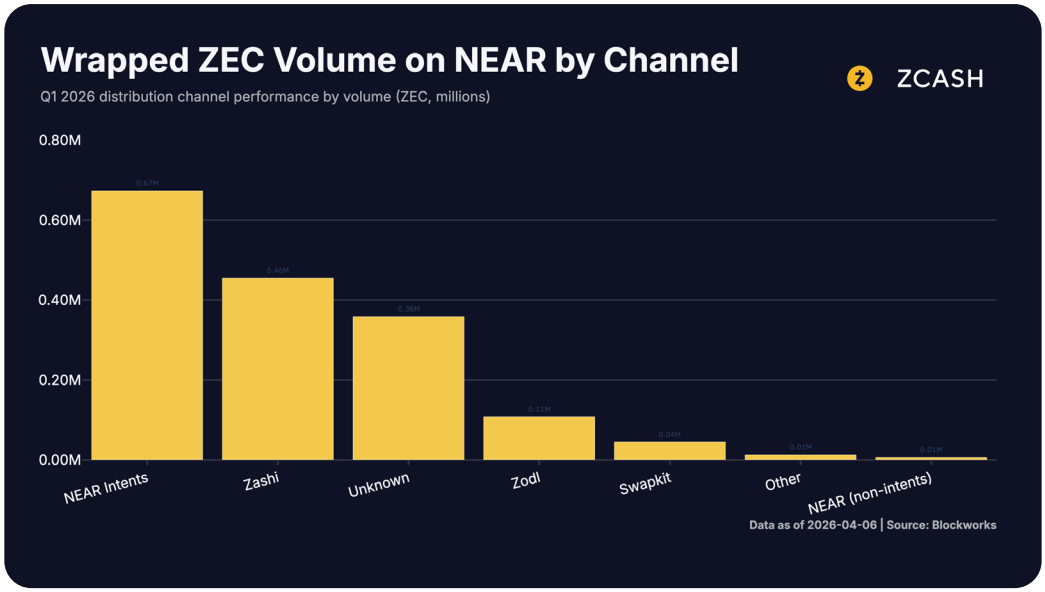
This distribution reflects Zcash's current market structure. Unlike many smart contract ecosystems, Zcash does not natively support complex DeFi applications, and as a result, most trading occurs on centralized platforms where liquidity is deeper and execution is more efficient. While multichain DEX volume for ZEC exists, it remains fragmented across ecosystems and does not yet represent a primary venue for price discovery. The persistence of CEX-dominated volume suggests that ZEC continues to function primarily as a monetary asset rather than as a composable DeFi primitive. This aligns with the network's broader positioning as encrypted digital money rather than as a generalized financial execution layer.

Cross-Chain DEX Activity and Wrapped ZEC

Cross-chain DEX volume totaled $1.01B in Q1, with activity distributed across multiple ecosystems. NEAR led all chains at $529M (52.3% of multichain DEX volume), reflecting the continued traction of the NEAR Intents integration with the Zodl wallet—the top referral channel accounted for 37.4% of NEAR volume, followed by Zashi/Zodl users at 27.4%. Solana contributed $350M (34.6%) and BNB Chain added $133M (13.2%), while Ethereum-based ZEC activity remained minimal at $107K, consistent with the broader migration of ZEC trading toward faster, lower-cost chains.



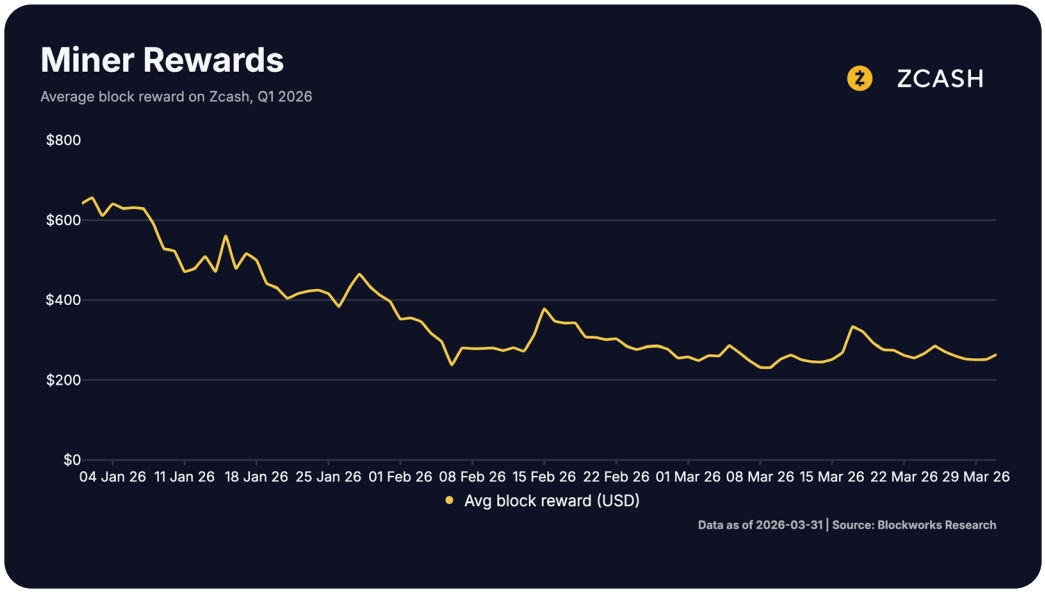
Historical Multichain DEX Volume DEX volume of ZEC across Ethereum, Solana, NEAR, and BNB, Q1 2026. Source: Blockworks



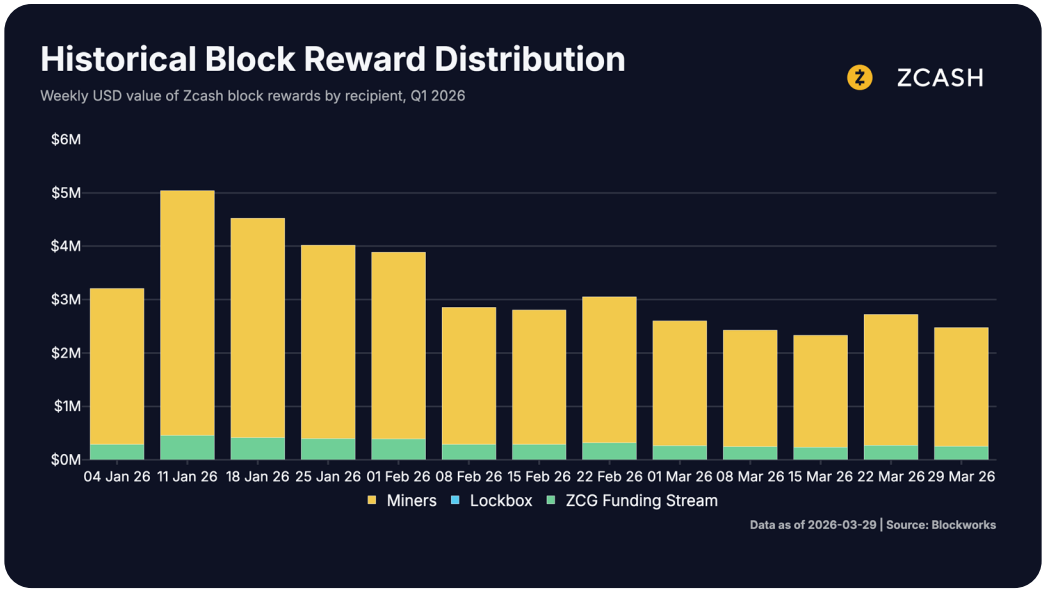
Wrapped ZEC Volume on NEAR by Channel Q1 2026 distribution channel performance by volume. Source: Blockworks

Wrapped ZEC supply on external chains grew to 219,881 ZEC (~$50.9M) at quarter-end, up from 203,240 ZEC in Q4. BNB Chain held the largest share at 120K ZEC ($27.1M), followed by Solana at 65.4K ZEC ($16.0M) and NEAR at 33.5K ZEC ($7.6M). At 1.3% of circulating supply, wrapped ZEC remains a modest fraction of total holdings, indicating that native-chain usage continues to anchor the network. The steady growth in wrapped supply nonetheless signals expanding cross-chain accessibility for ZEC as an asset.

Mining & Block Reward Distribution



Miner Rewards Average block reward on Zcash, Q1 2026. Source: Blockworks

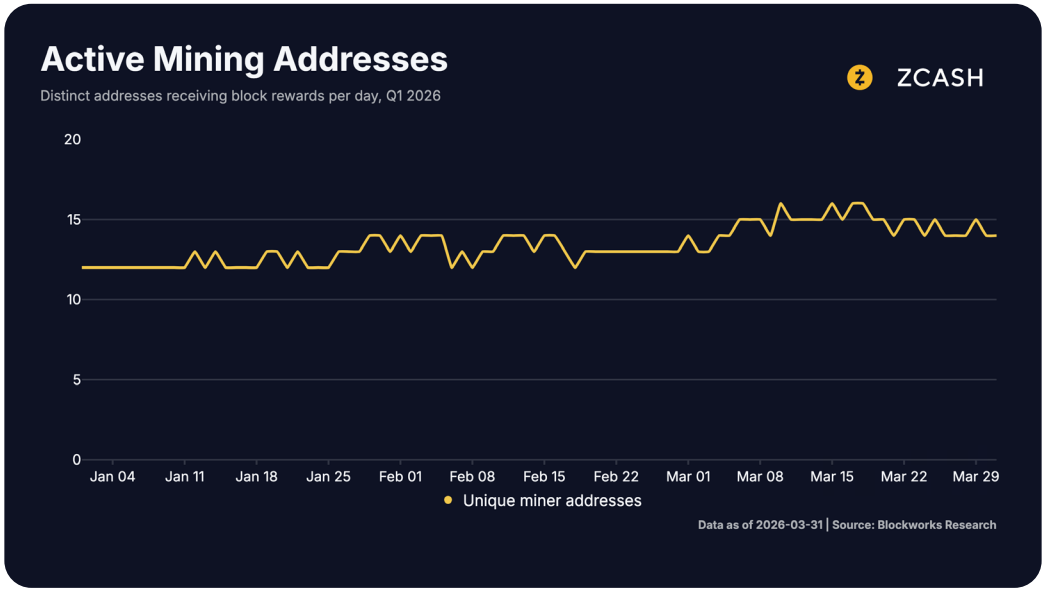


Historical Block Reward Distribution Weekly USD value of Zcash block rewards by recipient (Miners, Lockbox, ZCG Funding Stream), Q1 2026. Source: Blockworks

Mining remains central to Zcash's security model, and block reward distribution provides visibility into how newly created supply flows across the ecosystem's key stakeholders. Total block reward distribution in Q1 amounted to $42.7M,

with miners receiving $38.5M (90.2%) and the ZCG funding stream receiving $4.2M (9.8%). Average block rewards were $357.55, reflecting lower ZEC prices rather than any change to the issuance structure. On the supply side, a constructive signal emerged in miner participation: the average number of unique mining addresses increased 41.9% QoQ to 13.4 per day, suggesting improving decentralization in the mining landscape heading into the Foundry pool launch.

Block rewards in Q1 were distributed across three primary recipients: miners (who secure the network), the Lockbox (a protocol-level fund directed by coinholder governance), and the Zcash Community Grants (ZCG) funding stream. The continued operation of these funding mechanisms reflects the network's transition toward a self-sustaining economic model where protocol-level revenue supports both security and development.



Active Mining Addresses Distinct addresses receiving block rewards per day, Q1 2026. Source: Blockworks

Organizational & Technical Progress

Q1 2026 was the most consequential quarter for Zcash's organizational structure since the network's launch. A governance dispute culminated in a mass departure from the Electric Coin Company, a new development entity raised significant venture capital, the SEC closed a years-long investigation, and a critical security vulnerability was discovered and resolved. Despite the disruption, protocol development continued across all major workstreams, and the network's hashrate reached an all-time high.

ECC Governance Dispute and ZODL Formation

On January 7–8, the entire Electric Coin Company (ECC) development team—including CEO Josh Swihart—resigned following a governance clash with Bootstrap, the 501(c)(3) nonprofit that oversees ECC. The core dispute centered on the future of the Zashi wallet: ECC leadership sought to privatize Zashi to attract external capital, while Bootstrap's board argued this would violate nonprofit law and fiduciary duty. ZEC fell approximately 14% on the news. By February 16, the team had formally established the Zcash Open Development Lab (ZODL) and rebranded the wallet to Zodl—the update was automatic, requiring no new download or recovery phrase changes.

On March 9, ZODL closed a seed round exceeding $25 million, with participation from Paradigm, a16z crypto, Winklevoss Capital, Coinbase Ventures, Cypherpunk Technologies, Chapter One, and Balaji Srinivasan among other angel investors. This represents one of the largest privacy-focused fundraises in recent years and signals significant institutional confidence in Zcash's development trajectory.

The net result is a shift from a historically centralized contributor model (ECC under Bootstrap) to a broader, independently funded development ecosystem. While this transition introduces near-term coordination complexity, it also reduces single-entity dependency and aligns with the network's long-term goal of decentralized governance.

SEC Investigation Closure

In mid-January, the SEC officially closed its investigation into the Zcash Foundation (case "In the Matter of Certain Crypto Asset Offerings SF-04569," active since August 2023) without recommending enforcement action. ZEC surged over 12% on the announcement, which removed a significant regulatory overhang that had been a persistent concern for institutional holders.

Separately, Grayscale's Zcash Spot ETF filing (submitted November 2025 to convert the $137M Zcash Trust into a spot ETF on NYSE Arca) remains pending. A decision is now expected in Q2 2026 or later. The SEC investigation closure strengthens the case for approval by removing the most direct regulatory question mark around the asset.

Security: Sprout Pool Vulnerability

In late March, security researcher Alex "Scalar" Sol discovered that zcashd versions 3.1.0 through 6.11.x had been silently skipping Sprout proof verification during block connection for approximately six years. The flaw theoretically exposed 25,424 ZEC ($6.5M) in the legacy Sprout pool to potential draining. A fix (zcashd v6.12.0) was released and deployed by major mining pools (Luxor, F2Pool, ViaBTC, AntPool) by March 26. The bug was never exploited, and the turnstile mechanism would have limited damage had it been. Sol received a 200 ZEC bounty (~$51,000), split equally among Shielded Labs, ZODL, ZF, and Bootstrap. A dedicated bug bounty platform, bountyzcash.org, also launched during Q1.

Governance and Funding Coordination

Beyond the ECC/ZODL transition, coinholder-directed governance mechanisms continued to mature. The Zcash Community Grants (ZCG) program and Lockbox-based funding structures remained the primary channels for allocating ecosystem resources. The Q1 round of the coinholder-directed retroactive grants program opened for proposals, with review closing March 17 and polling to follow. Proposals included Zchat (a shielded messenger), NEAR Intents integration, and Maya Protocol advanced shielded ZEC support.

The Lockbox (receiving 12% of block rewards since NU6 in November 2024) continues accumulating ZEC, though no disbursement mechanism has been finalized. FROST development (especially DKG and ZIP-312) is a prerequisite for the eventual multi-party disbursement process.

Protocol changes continue to be proposed through Zcash Improvement Proposals (ZIPs), implemented through an off-chain execution model involving four core entities:

Zcash Open Development Lab (ZODL): The original Zcash engineering team, now independently funded. Primary focus: Zodl wallet, third-party SDKs, protocol development, and ecosystem communications.

Zcash Foundation (ZF): Independent nonprofit focused on privacy for the public good. Maintains the Zebra node implementation, organizes Zcon and community events. The ZF positioned itself as a stabilizing force following the ECC departure.

Tachyon: Led by cryptographer Sean Bowe (creator of Halo and Sapling), focused on scaling Zcash through recursive ZK proofs using Proof-Carrying Data—enabling wallet synchronization in seconds instead of hours and targeting thousands of shielded TPS.

Shielded Labs: Research and development team. Zooko Wilcox serves as CPO. Received a second donation from Vitalik Buterin on February 6 and announced incentivized feature nets beginning April 15, where participants can earn real ZEC.

Technical Progress

Despite the organizational disruption, technical development continued across all major workstreams:

Zebra & Z3 Stack. Every blockchain needs node software—the program that miners and validators run to process transactions and enforce the network's rules. For most of Zcash's history, this was zcashd, a single codebase originally derived from Bitcoin. Running a single node implementation is a known risk: a bug in zcashd would affect the entire network. Zebra is a ground-up rewrite of Zcash's node software, built in Rust by the Zcash Foundation, designed to be faster, more secure, and independently maintained. After the next network upgrade (NU7), Zebra becomes the sole consensus node, and zcashd will be retired.

The broader Z3 stack (Zebra + Zaino + Zallet) wraps Zebra with a lightweight indexer (Zaino) and wallet toolkit (Zallet), creating a complete replacement for the legacy infrastructure. Notably, the Z3 stack includes built-in Tor support, meaning node operators can route all network traffic through Tor by default—adding network-level anonymity on top of Zcash's transaction-level privacy.

FROST (Flexible Round-Optimized Schnorr Threshold Signatures). FROST is a cryptographic protocol that allows a group of participants to jointly control a wallet without any single person holding the full private key. Think of it as a privacy-

preserving multi-signature scheme: for example, 3 out of 5 keyholders must agree to authorize a transaction, but the resulting signature looks identical to a normal single-signer transaction onchain—preserving privacy even for multi-party operations.

This matters for Zcash because the Lockbox (which accumulates 12% of all block rewards) currently has no disbursement mechanism. FROST is the technology that will eventually enable Lockbox funds to be released through a decentralized, multi-party signing process rather than relying on a single trusted entity. Version 3.0.0-rc.0 was released in Q1 with cheater detection enabled by default, and ZIP-312 finalization (the formal protocol specification) and Distributed Key Generation (DKG) implementation are 2026 priorities.

Zodl Wallet. For most of Zcash's history, using shielded transactions required technical sophistication—command-line tools, long sync times, and confusing address management. Zodl (formerly Zashi) is a mobile, self-custody wallet that makes shielded transactions the default experience. When a user opens Zodl, all funds are automatically held in the Orchard shielded pool, and all sends are private by default. No configuration, no toggle, no technical knowledge required.

Beyond basic send/receive, Zodl has integrated two features that generate meaningful onchain activity: Zodl Swaps (powered by SwapKit SDK and Maya Protocol, enabling decentralized token swaps from within the wallet) and CrossPay (private cross-chain payments via NEAR Intents). These integrations have produced real traction: cumulative NEAR Intents ZEC volume exceeded $1.5B by end of March, while Zodl Swaps processed nearly $600M in ZEC swaps since October 2025. This demonstrates that improving UX can translate directly into onchain usage—and that privacy and usability are not in tension.

Post-quantum preparedness remained a topic of active discussion. The most concrete proposal is the Quantum Recoverable Orchard scheme, which reduces security to hash functions—against which quantum computers have no known advantage. Half the problem (proving ownership of funds) is already quantum-safe due to a forward-looking design choice embedded in Orchard wallets since launch.

Mining Developments

On March 11, Foundry Digital—operator of the world's largest Bitcoin mining pool—announced plans to launch a SOC 1/SOC 2 compliant, institutional-grade Zcash mining pool in April 2026. This is significant for hashrate decentralization: Zooko Wilcox noted it would help redistribute hashpower away from its current concentration in a single pool.

Network hashrate reached an all-time high of 16.54 GS/s during Q1, reflecting growing miner confidence despite the organizational upheaval elsewhere in the ecosystem.

Despite the short-term disruption, Q1's institutional developments are potentially constructive for Zcash's long-term trajectory. The rapid formation of ZODL, the $25M fundraise from top-tier investors, the SEC investigation closure, and continued technical progress across all workstreams collectively suggest a network that is becoming more diversified, better capitalized, and less dependent on any single entity than at any prior point in its history. The key risk is coordination: with development now spread across ZODL, ZF, Tachyon, and Shielded Labs, the ecosystem must demonstrate that a decentralized contributor model can execute as effectively as the prior centralized structure. The Q1 evidence—continued Zebra and FROST development, Zodl wallet traction, and ATH hashrate—suggests that execution has not meaningfully slowed, but this bears watching in subsequent quarters.

Post-Quantum Roadmap

The Threat

In April, Google published a 20x algorithmic improvement to Shor's algorithm—the quantum computing method that can break the elliptic curve cryptography underlying virtually every blockchain and most internet security. A separate paper from Oratomic demonstrated additional speedups in a different quantum setting. These results introduced a third dimension to quantum risk beyond the two previously tracked (physical qubit scaling and error correction): the attack algorithm itself is getting faster.

Scott Aaronson, one of the field's most prominent researchers, had already signaled in 2025 that by ~2030 we would know whether quantum error correction works at the scale needed to break real cryptographic keys. If it does, breaking ECC becomes an engineering problem rather than a physics problem. The recent algorithmic gains compress that timeline further.

For blockchains specifically, the threat has two distinct components. First, soundness: a quantum computer could forge proofs or signatures, enabling counterfeiting. Second, and less discussed, retroactive privacy compromise: every transaction ever recorded under quantum-vulnerable encryption could be de-anonymized after the fact. Unlike soundness, which can be patched going forward, privacy leaks from historical data are permanent and irreversible.

Zcash's Quantum Roadmap

Zcash is one of the only blockchain projects with a phased quantum defense plan already in execution. The ordering is deliberate: privacy first (because blockchain data is permanent), soundness second (because it can be patched modularly).

Phase 1: Quantum Recoverability

Phase 1 is a wallet-only update that ensures all fund ownership claims are provable against a quantum adversary. If a quantum computer appeared tomorrow, shielded pools could be frozen and users running updated wallets could safely migrate funds to a new quantum-resistant pool. The code is substantially complete and deployment is gated on a Keystone firmware update and coinholder poll. Expected within weeks of poll completion.

Phase 2 : Post-Quantum Privacy (End of 2025, Tachyon)

This phase replaces the elliptic curve key exchange used in shielded payments

with ML-KEM, a different standard adapted to post quantum, already adopted by Signal. This will ship as part of the Tachyon shielded pool. Once phases 1 and 2 are complete, the urgency around quantum is effectively neutralized. User keys are safe, privacy is preserved, and the response to Q-Day is an orderly pool freeze and migration.

Phase 3: Post-Quantum Soundness

Upgrades the cryptography that prevents counterfeiting of ZEC to quantum-resistant alternatives. Tachyon's architecture is designed to make this swap modular, individual cryptographic components can be replaced without rebuilding the protocol from scratch, and without the performance penalties that would otherwise cut network throughput by 10–20x. One open challenge remains industry-wide: making these quantum-resistant proofs fast enough to generate on a mobile phone, which is necessary for wallets to function smoothly. This is an active area of research.

Parallel Scaling Track

The quantum roadmap is enabled by scaling work proceeding in parallel: Shielded sync elimination (PIR). Today, wallets must download and test every transaction to discover payments, a process that cannot scale beyond ~10 TPS. PIR-based payment discovery removes this entirely, enabling instant wallet opens with no sync delay. First production deployment is the new governance voting system; wallet integration follows.

Block time reduction (NU7, mid-2025). Proposed upgrade from 75-second to 25-second blocks, roughly tripling consensus throughput and doubling Orchard TPS.

Dynamic fee markets. Replaces flat fees (exploited during sandblasting attacks) with congestion-based pricing, designed to prevent fee metadata from leaking transaction identity. Enabled at negligible cost through Tachyon's recursive proofs.

Tachyon mainnet (end of 2025). Introduces recursive ZK proofs, solving the last non-constant scaling bottleneck and enabling all of the above without bandwidth penalties.

Execution Risk

Shipping Tachyon, PIR, NU7, and ML-KEM within a single year is aggressive, and the development team has acknowledged as much publicly. Key risks include: timeline compression across parallel workstreams now distributed among four independent entities (ZODL, ZF, Tachyon, Shielded Labs); PIR server infrastructure bootstrapping in production; and the unresolved performance gap in client-side post-quantum proving on mobile devices.

Against these risks, Zcash holds advantages no other blockchain currently matches: deep post-quantum cryptographic expertise on the core team, a protocol architecture designed from inception with quantum adversaries in mind, a quantum recoverability plan weeks from deployment, and a recursive proof system that makes post-quantum primitives economically viable at the protocol level.

Conclusion

Zcash's Q1 2026 performance reflected a normalization in activity following Q4's elevated levels, but a continued strengthening of the network's underlying privacy fundamentals. While total transactions declined 40.0% QoQ and network revenue (REV) fell 79.1% QoQ to $64.2K, core privacy metrics moved in the opposite direction. Shielded supply increased to 5.16M ZEC (31.0% of circulating supply), the anonymity set expanded to 123.76M notes (+301K QoQ), and shielded transactions proved more resilient than overall network activity, increasing their share of usage to 21.2%.

This divergence between activity and fundamentals is central to understanding Zcash. Unlike fee-driven networks, where growth is measured by throughput and revenue, Zcash's value accrues through the strength of its privacy system. In Q1, that system continued to deepen. More value was held in shielded pools, privacy guarantees improved through anonymity set expansion, and usage patterns suggested increasingly durable engagement with shielded balances despite short-term fluctuations in transaction flow.

Beyond onchain metrics, Q1 was defined by the most significant organizational restructuring in Zcash's history. The entire ECC development team departed and reformed as ZODL, raising $25M+ from Paradigm, a16z, Winklevoss Capital, and Coinbase Ventures. The SEC closed its investigation without charges, removing a multi-year regulatory overhang. A critical Sprout vulnerability was discovered and patched without exploitation. Foundry Digital announced an institutional mining pool, and network hashrate reached an all-time high. Despite the disruption, technical development continued across Zebra, FROST, and Zodl, and the ecosystem emerged more diversified and better capitalized than before.

Taken together, Q1 demonstrates that Zcash's core value proposition—private, low-cost, and censorship-resistant value transfer—remains intact and continues to strengthen at the protocol level. At the institutional level, the transition from a centralized contributor model to a multi-entity, venture-backed ecosystem introduces coordination risk but also reduces single-entity dependency and broadens the network's support base. Zcash remains positioned as one of the few blockchain systems where long-term value is derived not from maximizing economic extraction, but from maximizing privacy itself.