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.

Q2 2026

Blockworks Advisory

Table of Contents

SECTION 01

Executive Summary

Q2 2026 tested Zcash's foundations and, on the evidence that matters most to holders, the network held.

26.3%	124.1M	$110K	314,186 ZEC
SHIELDED SHARE OF SUPPLY	ANONYMITY SET (NOTES)	NETWORK REV	CYPHERPUNK TREASURY
from 31.0%	new high	+72% QoQ	+19,400 QoQ

Q2 2026 tested Zcash’s foundations and, on the evidence that matters most to holders, the network held. The defining event of the quarter was the disclosure of a soundness flaw in the Orchard shielded pool: a circuit-level bug that, unaddressed, could have permitted forged proofs. Surfaced through an AI-assisted external security review, it was quietly patched and disclosed under coordination, and the ecosystem converged on a measured recovery upgrade, Ironwood, scheduled for activation in late July. The central reassurance is one of supply integrity: Zcash’s long-standing turnstile mechanism bounds the ZEC that can exit any shielded pool to the amount that legitimately entered it, and early signals (steady pool growth after disclosure and the bug’s complexity) point to no exploitation. No counterfeit supply circulated.

That security event reshaped the quarter’s onchain story without derailing the underlying adoption trend. Shielded balances contracted: the total ZEC held across shielded pools fell from roughly 5.16 million at the end of Q1 to 4.42 million (-14%), and the shielded share of supply eased from 31.0% to 26.3%, as deshielding outpaced new shielding through the period. Yet the activity picture diverged from the balance picture in a way worth underlining. Shielded transaction counts actually rose 11% quarter-over-quarter to roughly 132,000, and the anonymity set, the cumulative measure of Zcash’s privacy guarantee, continued to expand to a new high of 124.1 million notes. Holders moved value out of the Orchard pool while continuing to transact privately at a higher cadence.

Economics and security both firmed off the Q1 trough. Network REV recovered 72% to roughly $110,000 as fees normalized higher, and network difficulty, the

closest available proxy for hashrate, set an all-time high in mid-June and closed the quarter 30% above where it began, reflecting the arrival of institutional-grade mining capacity. Institutional conviction deepened in parallel: Cypherpunk Technologies, the Nasdaq-listed public company with a ZEC treasury vehicle pursuing 5% of network supply, grew its ZEC holdings to 314,186, while the engineering lab ZODL operated on the back of a $25 million-plus raise. The throughline for the quarter is security-response maturity layered on compounding structural fundamentals.

SECTION 02

The Orchard Soundness Flaw

The defining event of the quarter was a soundness flaw in the Orchard shielded pool, the pool that has held roughly 85% of Zcash's shielded value since it launched in May 2022 alongside the Halo 2 proving system. It is worth treating in full rather than in passing: a bug that strikes at the integrity of shielded value is the most serious thing that can happen to a privacy chain, and the network's handling of it is the quarter's most revealing signal.

The bug: what broke, and how it was caught

An independent security researcher auditing the protocol surfaced the flaw on May 29, using an AI-assisted review of the Orchard circuit. The bug lived in the variable-base scalar-multiplication step of the Halo 2 circuit, the part that is supposed to prove a spender's key was derived from the protocol's own base point. The circuit wrote the base-point coordinates into the proof without binding them to that protocol-specified value, a single missing equality constraint. With the base point left unbound, a prover could substitute an arbitrary one and still produce a proof the network would accept. The bug had been latent since Orchard first activated in 2022. The response was fast and staged: the researcher disclosed privately to core engineers the same evening, and within days the network shipped an emergency upgrade that first paused Orchard transactions and then, on June 3, re-enabled the pool with the corrected circuit. That patch closed the live exposure, and Ironwood, targeted for late July, is the durable recovery that follows it rather than the first line of defense. This is the second time Zcash has caught a forge-proofs soundness bug before it was used: the original Sprout pool carried a comparable flaw, disclosed in 2019, that could also have counterfeited unlimited ZEC, and it too was closed with no evidence of exploitation.

Counterfeiting, not theft, and not inflation

The capability the flaw granted is narrower than the worst-case reading. The exploit path was double-spending inside the Orchard pool: because the substituted base point let an attacker derive several valid-looking nullifiers for a

single note, that note could be spent more than once, and the network, which only checks whether a given nullifier has appeared before, would not catch the repeat. That is counterfeiting of ZEC within the pool. It is not theft of other users' funds, and, critically, it could not inflate the total ZEC supply. The reason is the turnstile.

The turnstile, and what it does and does not guarantee

Zcash treats every shielded pool as a single publicly visible balance. The holdings inside a pool are private, but the net total the pool contains is not: it rises as ZEC is shielded in and falls as ZEC is deshielded out. That public per-pool balance is the turnstile, and it is not specific to any one pool. Sprout, Sapling, and Orchard are all governed by it, so Orchard is not an exception. Its guarantee is an aggregate one: the total value that can ever leave a pool cannot exceed the total that verifiably entered it. That is why an internal counterfeiting bug could not become new network-wide supply. An attacker could forge spends inside Orchard, but the moment they tried to carry counterfeit value out it would draw down a public balance, and consensus rejects any outflow that would push cumulative withdrawals past cumulative deposits. The limits of that assurance are worth stating plainly. The turnstile bounds the total in a pool; it does not verify individual notes or ownership, and it acts only at the pool's edges, not on transfers that stay inside. The circuit, not the turnstile, is what polices spends within a pool, which is exactly why a circuit flaw was the failure mode. So the turnstile is a backstop that caps the blast radius of such a flaw rather than a mechanism that prevents it. As for confidence that the flaw was not exploited when the pool is private: monitoring found no evidence of exploitation and no unauthorized value, the working exploit never left a local test environment, and any counterfeiting large enough to matter would have had to breach the public pool balance to leave the pool at all. Runtime monitoring cannot inspect individual private notes, but formal verification can close that gap: a machine-checked proof that the corrected circuit is sound rules out the entire class of bug, so assurance extends from total supply down to the individual shielded spend, and it is high.

Ironwood: the durable recovery, and what remains

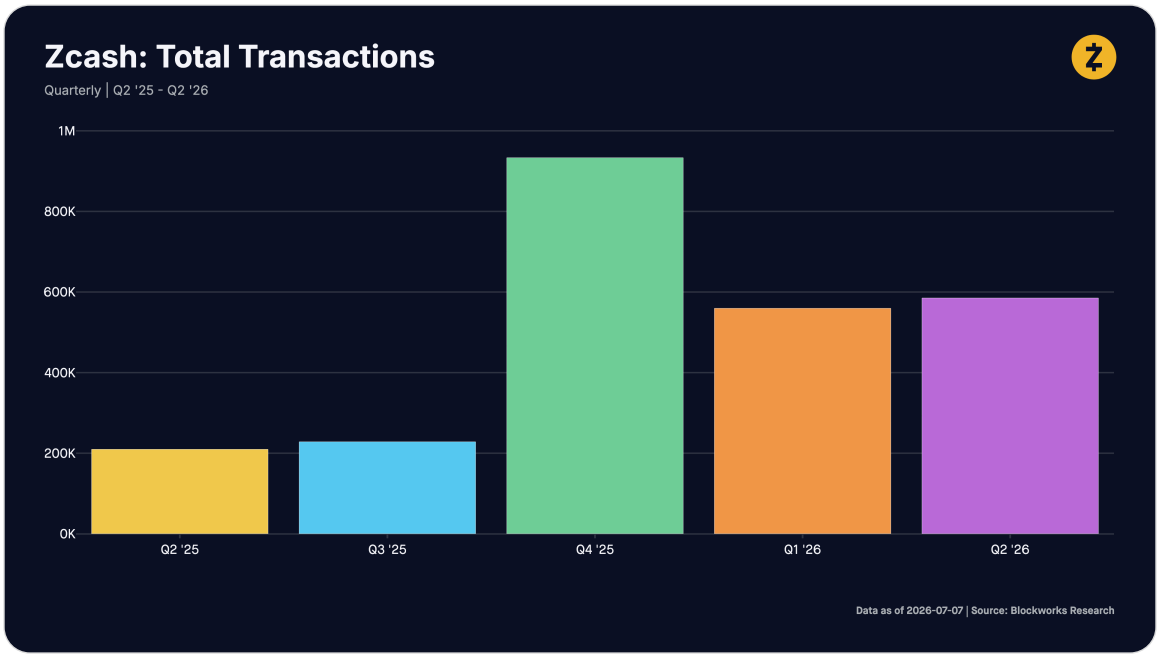
Ironwood, formally network upgrade NU6.3, makes the turnstile the instrument of recovery, and it does more than repair the bug: it introduces two innovations that leave the shielded pool materially stronger than before the disclosure. The upgrade stands up a replacement shielded pool built on the corrected circuit, permanently seals the legacy Orchard pool to new incoming payments, and routes all new Orchard-addressed activity to the replacement. Every ZEC leaving the old pool must pass through the turnstile to enter the new one, so the amount that can migrate is capped at the amount that legitimately existed. As Sean Bowe framed it, the combination bounds the circulating supply of ZEC to no more than the amount that is supposed to exist. The first innovation is formal verification: machine-checked mathematical proofs that rule out literally all implementation bugs rather

than patching them one at a time, backed by independent third-party audits, materially more assurance than a single-team hotfix. The second is quantum recoverability, which ships with Ironwood: it establishes recovery pathways for funds whose keys could be exposed by future quantum hardware, making Zcash the first crypto network engineered so that holders could recover their funds even if a large-scale quantum attack arrived tomorrow. Existing addresses carry over, so holders are not forced through key rotation, and wallet providers are expected to offer one-click migration. The recovery is credible and broadly owned: it was proposed jointly by ZODL, Project Tachyon, the Valar Group, the Zcash Foundation, and Shielded Labs. It is not yet finished. Testnet trials, ecosystem coordination, and final audits remain outstanding ahead of the late-July activation, which coincides with the retirement of the legacy zcashd software. Holders should treat a clean activation as the event that closes the matter.

SECTION 03

Network Performance

Network activity stabilized in Q2 after the sharp normalization that defined Q1. Total transactions rose 4.6% quarter-over-quarter to roughly 585,000, a modest recovery that nonetheless sits well below the elevated 933,000 logged in Q4 2025. The right reading is normalization rather than weakness: Q4's spike reflected a period of unusual throughput, and the subsequent two quarters have settled the network onto a more representative baseline. Block production was essentially flat at roughly 104,000 blocks for the quarter, with average block intervals holding near their 75-second target. The chain produced blocks on schedule throughout, including across the period surrounding the Orchard disclosure.

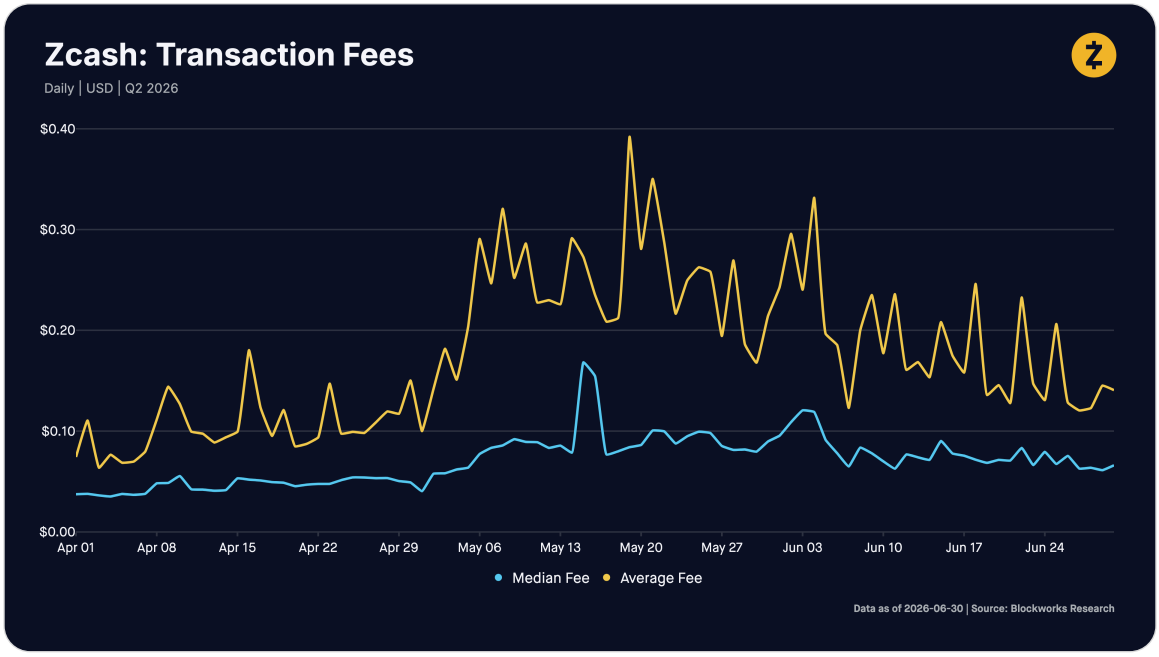


Zcash: Total Transactions. Quarterly | Q2 '25 - Q2 '26. Source: Blockworks

The composition of that activity is where the more interesting movement sits. Transparent transaction counts grew 3.4% to roughly 349,000, while Orchard

transaction counts grew faster at 13.2% to roughly 112,000. Shielded usage, in other words, gained share of total activity even as transparent transactions remained the larger absolute category, a continuation of the multi-quarter trend toward private transfers as the default behavior for a growing slice of users.

Fee levels recovered off Q1 lows without straining the network's low-cost positioning. The median transaction fee roughly doubled from approximately $0.04 to $0.07, and the average fee rose to roughly $0.18, increases that reflect higher demand for blockspace rather than any change in fee policy. In absolute terms these remain negligible costs for value transfer, preserving Zcash's standing as a low-cost settlement layer.



Zcash: Transaction Fees. Daily | USD | Q2 2026. Source: Blockworks

The quarter's throughput also unfolded against an active protocol-engineering backdrop. The NU7 testnet went live during the period, exercising upgrades that target materially faster shielded transactions and shorter block times ahead of any mainnet activation. The network also showed resilience under stress: continuous block production, on-schedule intervals, and a recovering fee market through a security disclosure and the coordination of an emergency response. That is itself a performance signal, and one consistent with a chain whose tooling and node software are maturing.

SECTION 04

Supply, Flows, and Usage

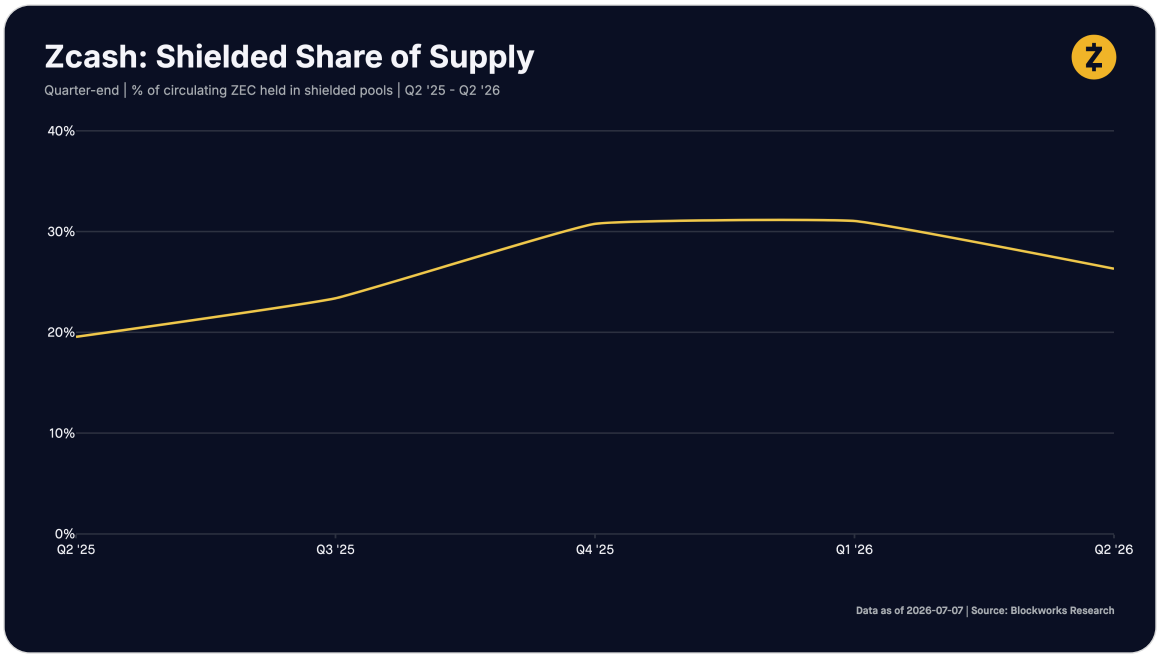
This is the quarter's central story, and it requires holding two facts in view at once: shielded *balances* drew down, while shielded *usage* and the privacy guarantee both grew.

Shielded supply and composition

Total ZEC held across the shielded pools fell from roughly 5.16 million at the end of Q1 to 4.42 million at the end of Q2, a 14% contraction. The Orchard pool absorbed essentially all of the movement: its balance fell from roughly 4.53 million to 3.77 million ZEC (-17%), while the older Sapling pool held roughly flat near 621,000 and Sprout remained negligible.

Zcash: Shielded Supply by Pool. Quarter-end ZEC in shielded pools | Q2 '25 - Q2 '26. Source: Blockworks

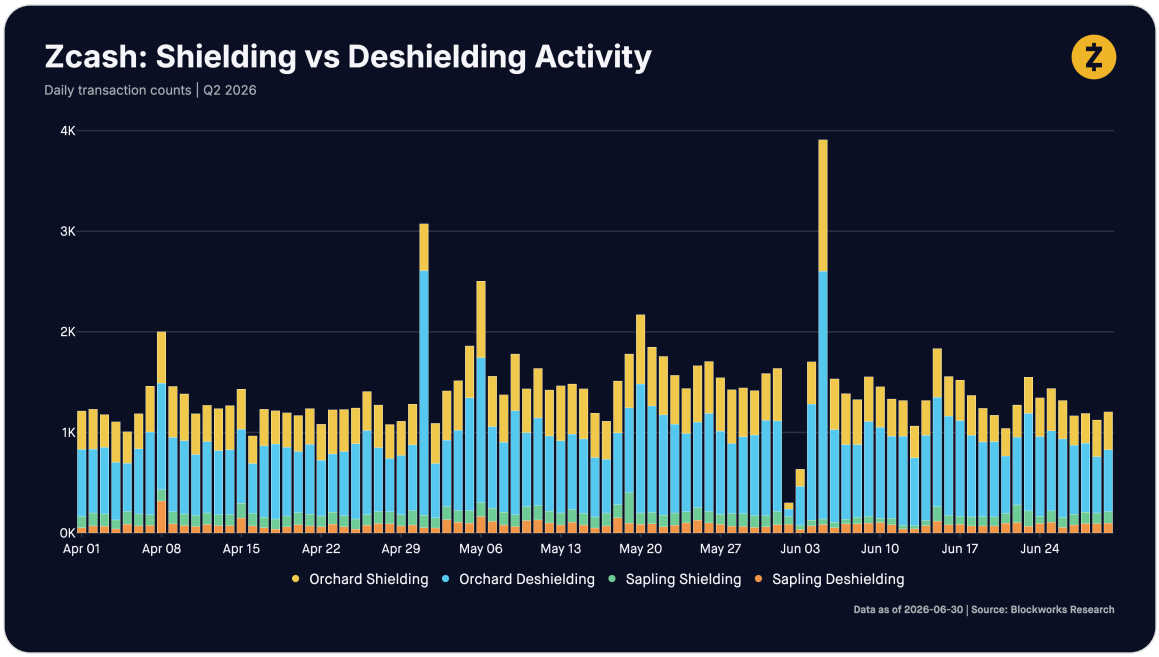
The shielded share of circulating supply eased in step, from 31.0% to 26.3%, with the decline concentrated late in the quarter: the ratio opened Q2 near 31% and closed at 26.3%. Orchard still anchors the shielded set at roughly 85% of shielded value, down only modestly from 88% a quarter earlier; its dominance as the network's primary shielded pool is intact, even as the absolute balance receded.



Zcash: Shielded Share of Supply. Quarter-end | % of circulating ZEC held in shielded pools | Q2 '25 - Q2 '26. Source: Blockworks

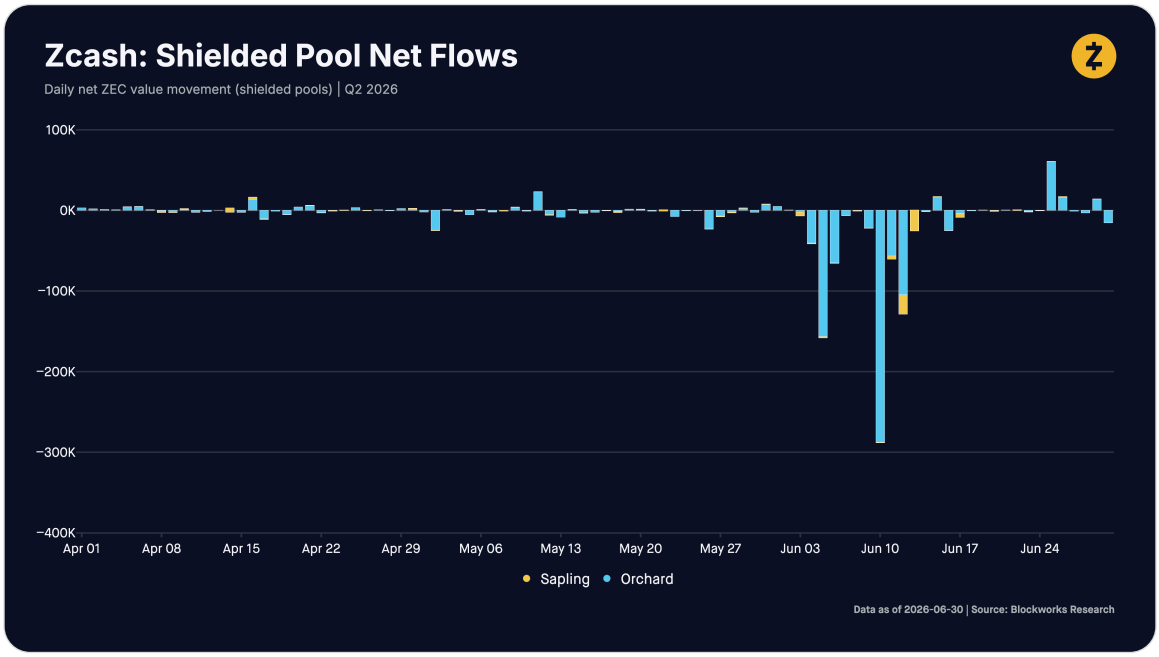
Flows: deshielding outpaced shielding

The contraction was a flow story, not a usage story. Deshielding transactions (value moving out of shielded pools) rose 15% quarter-over-quarter to roughly 80,200, while shielding transactions rose a slower 6% to roughly 49,300. The persistent skew toward deshielding that the prior quarter flagged not only continued but widened, and it is the direct mechanism behind the lower shielded balance.



Zcash: Shielding vs Deshielding Activity. Daily transaction counts | Q2 2026. Source: Blockworks

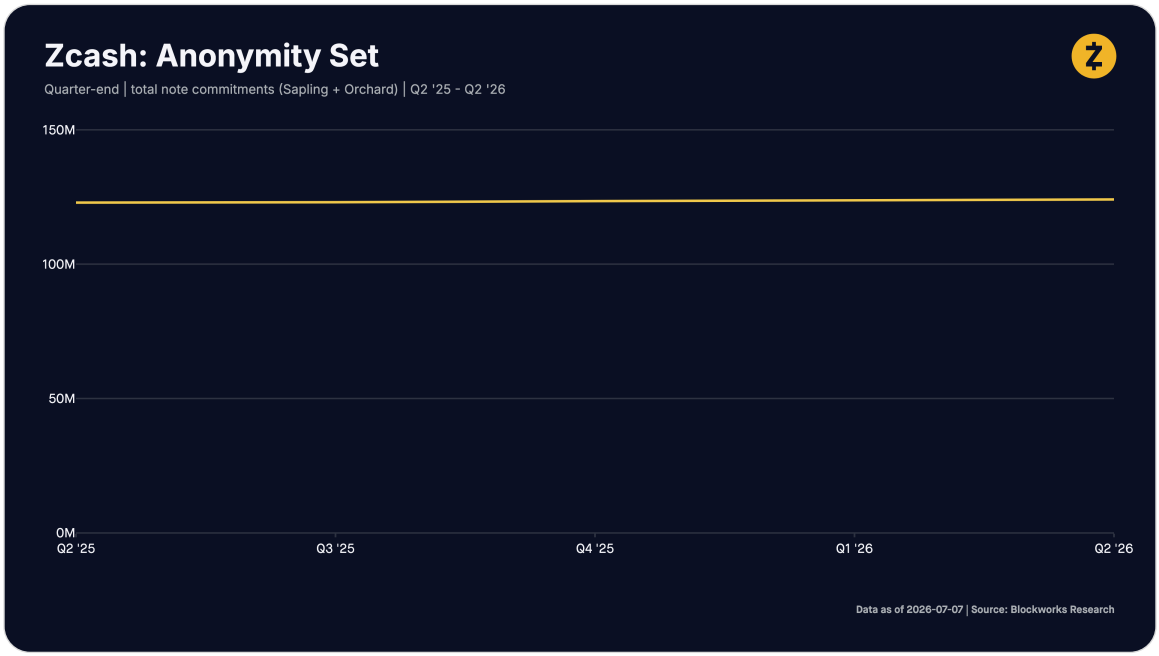
The timing coincided with the Orchard disclosure, a coherent pattern: holders responded to news of a circuit bug by moving value, even as the turnstile guaranteed that no illegitimate supply could accompany it.



Zcash: Shielded Pool Net Flows. Daily net ZEC value movement (shielded pools) | Q2 2026. Source: Blockworks

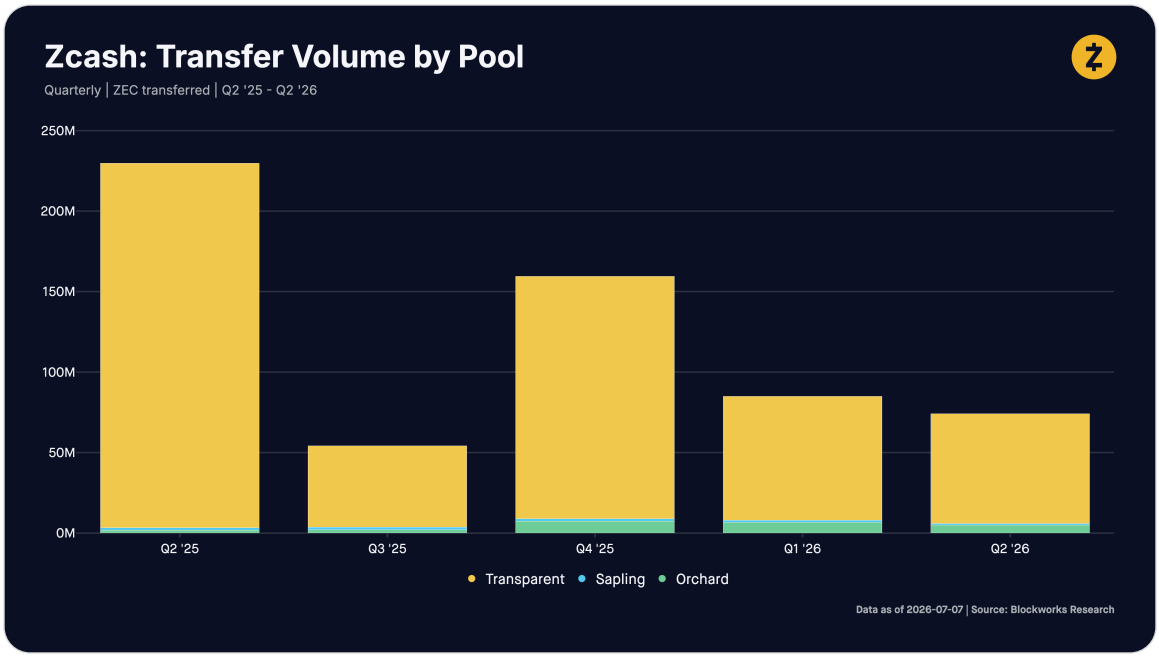
Usage and the anonymity set kept growing

Critically, the appetite for private transacting did not retreat. Shielded transaction counts rose 11% quarter-over-quarter to roughly 132,000, and the anonymity set, the cumulative count of shielded note commitments and the truest measure of the privacy Zcash offers, grew to a new high of 124.1 million notes. Because note commitments are append-only, this figure ratchets upward with every shielded transaction and cannot be eroded by deshielding; the privacy guarantee compounded through the quarter regardless of the balance contraction.



Zcash: Anonymity Set. Quarter-end | total note commitments (Sapling + Orchard) | Q2 '25 - Q2 '26. Source: Blockworks

Total ZEC transferred across all pools declined 13% to roughly 74.2 million, tracking the broader normalization in value settled. The honest synthesis: Q2 saw a balance-side response to a security event, set against continued and intensifying engagement with optional privacy as a default behavior.

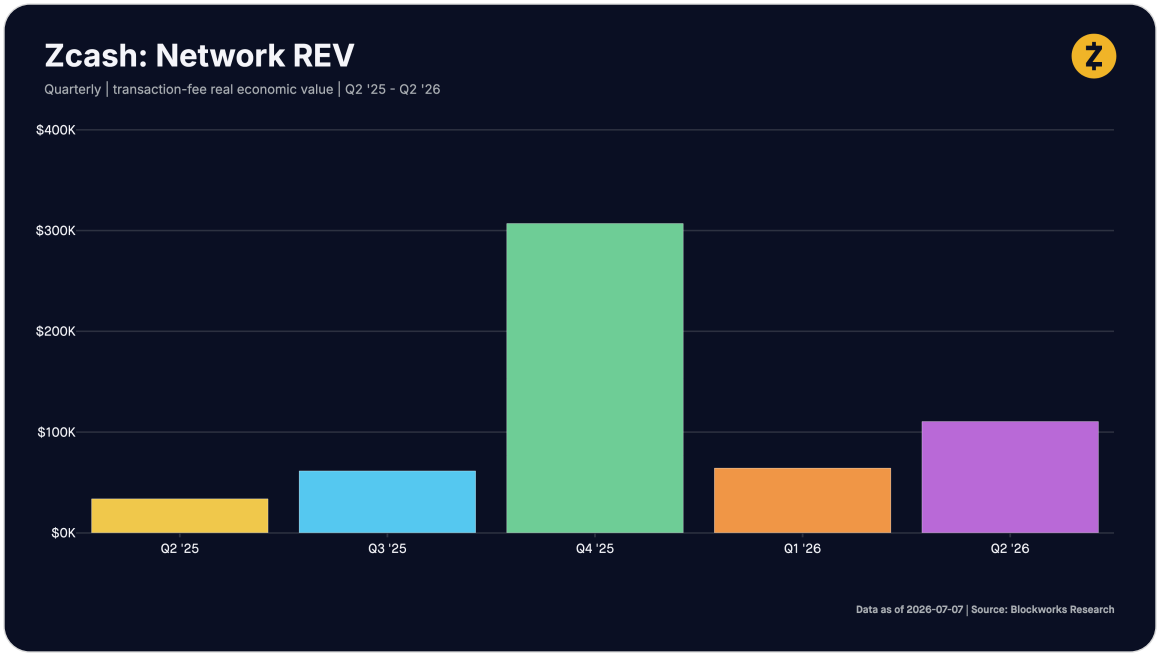


Zcash: Transfer Volume by Pool. Quarterly | ZEC transferred | Q2 '25 - Q2 '26. Source: Blockworks

SECTION 05

Market Structure & Economics

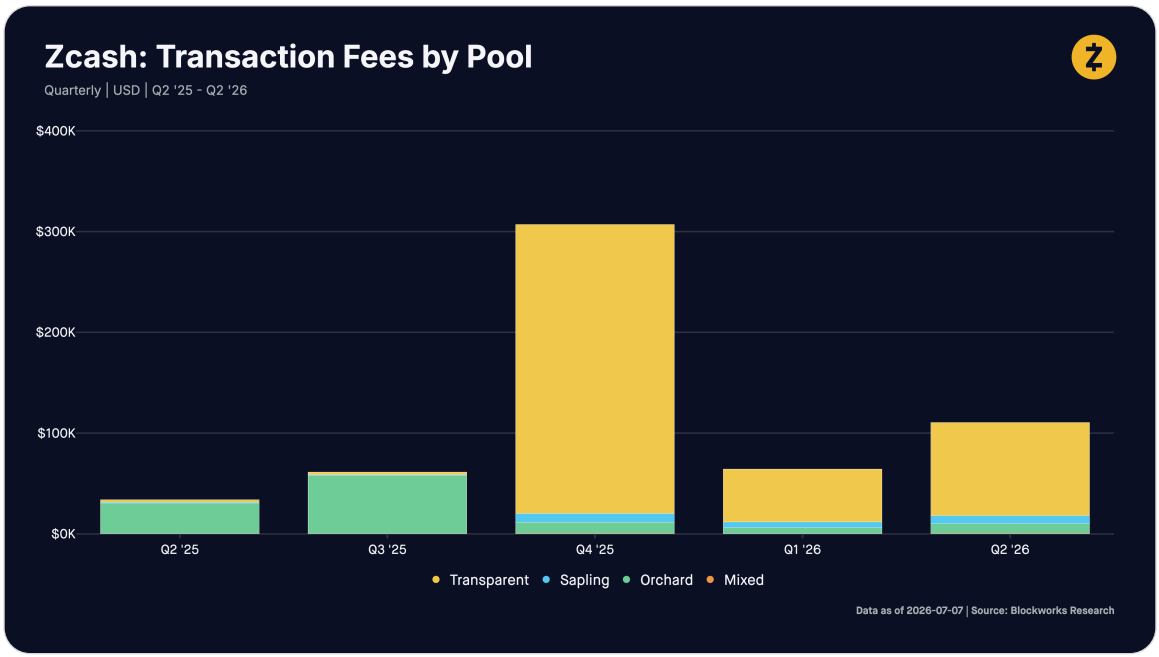
Network economics recovered meaningfully from the Q1 trough. Network REV, the real economic value accruing to the protocol through transaction fees, rose 72% quarter-over-quarter to roughly $110,000, recovering a portion of the ground lost in Q1's $64,000 reading while remaining below the $307,000 generated in Q4 2025. The recovery was fee-driven, consistent with the higher median and average fees discussed earlier, rather than a function of transaction-count growth alone.



Zcash: Network REV. Quarterly | transaction-fee real economic value | Q2 '25 - Q2 '26. Source: Blockworks

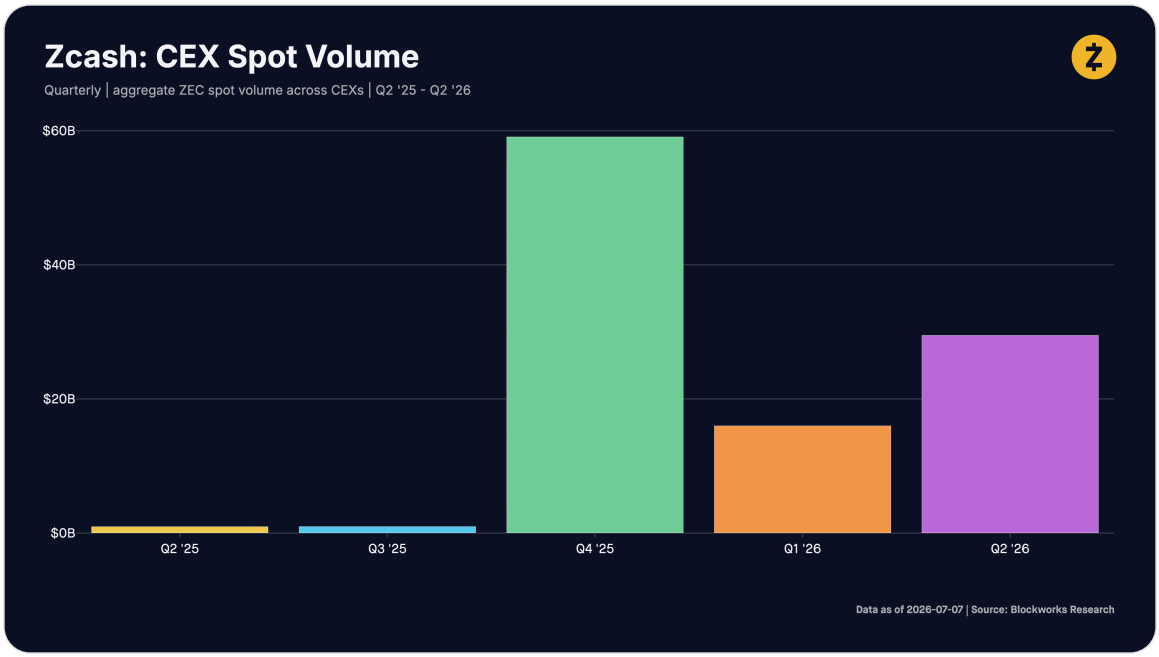
Fee composition by pool reinforces the network's structure. Transparent transactions generated the large majority of fee revenue at roughly $92,000, with Orchard contributing roughly $10,000 and Sapling roughly $8,000. That transparent activity carries most of the fee load is expected for a network where transparent transfers remain the higher-count category; it does not diminish the

shielded adoption thesis, which is a supply-and-usage story rather than a fee-share one. Notably, fee revenue grew across every pool quarter-over-quarter, indicating broad-based demand recovery rather than a single-pool artifact.



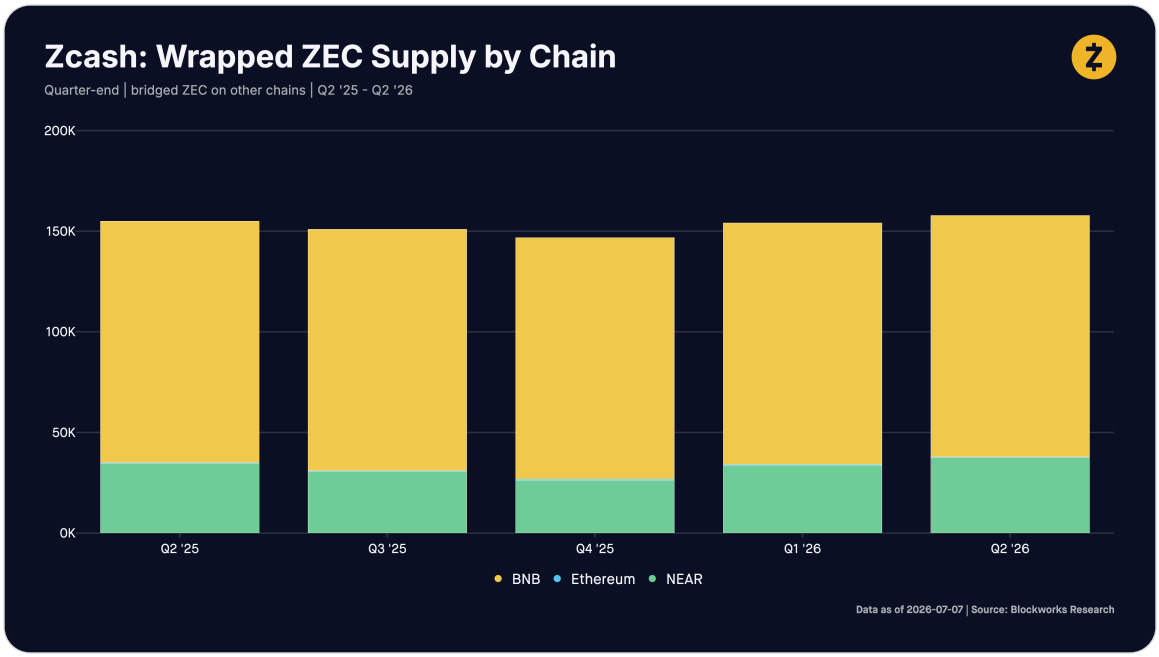
Zcash: Transaction Fees by Pool. Quarterly | USD | Q2 '25 - Q2 '26. Source: Blockworks

Exchange liquidity expanded sharply. Aggregate ZEC spot volume across centralized exchanges rose 85% quarter-over-quarter to roughly $29.5 billion, recovering from $16.0 billion in Q1 though still shy of Q4's $59.1 billion. Liquidity remains concentrated among the major venues, with Coinbase representing roughly a fifth of CEX volume; the network's optional-privacy design (transparent addresses that exchanges can support directly, with shielding available to users by choice) continues to underpin its compatibility with regulated venues in a way mandatory-privacy designs cannot match.



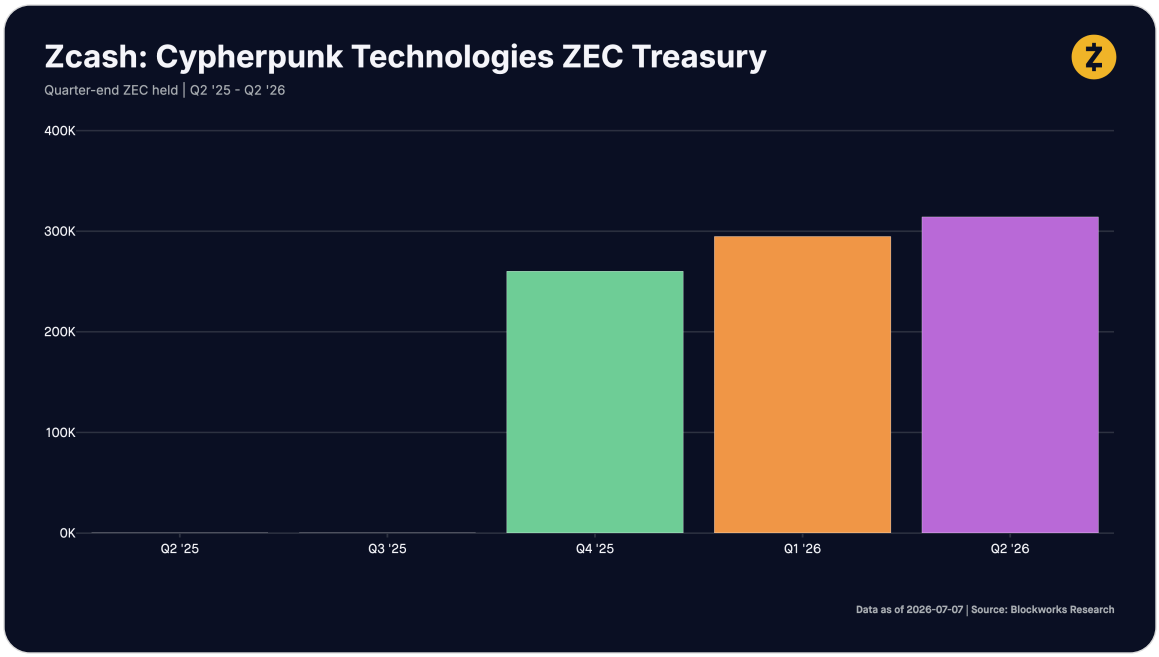
Zcash: CEX Spot Volume. Quarterly | aggregate ZEC spot volume across CEXs | Q2 '25 - Q2 '26. Source: Blockworks

ZEC's footprint beyond its own chain remains modest but is broadening at the edges: wrapped ZEC across BNB Chain, Ethereum, and NEAR totaled roughly 158,000 ZEC at quarter-end, under 1% of supply, with the NEAR-bridged balance growing 12% over the period even as the Ethereum-wrapped balance eased.



Zcash: Wrapped ZEC Supply by Chain. Quarter-end | bridged ZEC on other chains | Q2 '25 - Q2 '26. Source: Blockworks

The quarter's clearest demand signal came from the treasury layer. Cypherpunk Technologies, the Nasdaq-listed public company with a ZEC treasury vehicle, pursuing a stated goal of accumulating 5% of network supply, increased its holdings to 314,186 ZEC by quarter-end, adding roughly 19,400 ZEC over the period and bringing the net asset value of its position to approximately $128 million. The pace of accumulation moderated from Q1's larger additions, but the direction held: a regulated, balance-sheet buyer continued to absorb supply through the quarter's volatility, an institutional-grade vote of confidence in Zcash as a long-horizon holding.



Zcash: Cypherpunk Technologies ZEC Treasury. Quarter-end ZEC held | Q2 '25 - Q2 '26. Source: Blockworks

SECTION 06

Mining & Block Rewards

Zcash's proof-of-work security model strengthened materially in Q2, even as it grew more concentrated. Network difficulty, the closest available proxy for hashrate, rose 30% quarter-over-quarter on a quarter-end basis and touched an all-time high near 241 million in mid-June, having averaged roughly 143 million across the period (a 16% increase on the quarterly average). Rising difficulty signals that more computational capacity is competing to secure the chain, and the proximate driver is identifiable: Foundry Digital, operator of the largest Bitcoin mining pool, launched a SOC 1/SOC 2-compliant, institutional-grade Zcash mining pool during the quarter and grew it to roughly 30% of total network hashrate, onboarding regulated institutional miners and publishing a dedicated block explorer alongside it.

Zcash: Mining Difficulty. Quarterly average | hashrate proxy | Q2 '25 - Q2 '26. Source: Blockworks

That capacity arrived with a concentration trade-off worth naming directly. The number of distinct addresses receiving block rewards on a given day averaged only about 16 across Q2, a low figure that reflects the dominance of a handful of large pools, Foundry among them, in block production. Greater institutional hashrate raises the cost of attacking the network and signals professional conviction in Zcash mining economics; it also concentrates block production among fewer operators, a dynamic holders should track as the institutional mining footprint grows.

Zcash: Active Mining Addresses. Quarterly avg of daily distinct reward recipients | Q2 '25 - Q2 '26. Source: Blockworks

Block reward issuance itself was stable. The network distributed roughly 144,000 ZEC in block rewards over the quarter, essentially flat quarter-over-quarter. Miners received roughly 130,000 ZEC, about 90% of the distributed total, with the remaining roughly 14,000 ZEC flowing to the Zcash Community Grants funding stream. A further 12% of the full block subsidy, roughly 19,600 ZEC this quarter, accrued to the protocol-controlled lockbox rather than being paid out. This structure reflects the post-halving, NU6.1-era issuance model: the original Founders' Reward has long since ended, and development funding now flows through the Community and Coinholder model that NU6.1 activated in late 2025, which allocates 80% of each block subsidy to miners, 8% to Zcash Community Grants, and 12% to the lockbox. Issuance is predictable, the miner share dominant, and the funding model now subject to coinholder direction: a more accountable structure than the fixed allocations it replaced.

Zcash: Block Reward Distribution. Quarterly | ZEC block subsidy by recipient | Q2 '25 - Q2 '26. Source: Blockworks

SECTION 07

Organizational & Tech. Progress

Q2 demonstrated that Zcash's post-reorganization governance can coordinate under pressure. The defining structural shift entering the year was the move of the core engineering team out of the Electric Coin Company and into ZODL, an independent development lab that operates on a $25 million-plus funding round backed by Paradigm, Winklevoss Capital, Cypherpunk Technologies, Maelstrom, Chapter One, and angel investors including Balaji Srinivasan and Dragonfly's Haseeb Qureshi. ECC itself remains a subsidiary of the nonprofit Bootstrap Project, while the Zcash Foundation continues as the sole trademark steward and the maintainer of the Zebra node, the Zaino indexer, and the Zallet wallet: the "Z3" stack that is progressively replacing the legacy zcashd software now nearing end-of-support.

The clearest evidence that this multi-entity structure functions came from the Orchard response itself. Rather than a single team shipping a quiet fix, the Ironwood recovery was proposed jointly by ZODL, Project Tachyon, the Valar Group, the Zcash Foundation, and Shielded Labs, a coalition spanning every major contributor organization, and Sean Bowe confirmed agreement on the specific consensus rule changes in June. A soundness flaw of that severity producing a coordinated, cross-organization recovery rather than a single-team scramble is the governance signal that matters here.

On the protocol-engineering track, the NU7 testnet went live during the quarter, carrying an audited candidate ZIP for Zcash Shielded Assets, while the NU7 sentiment poll gauged coinholder appetite for Project Tachyon, which drew more than 90% support among ZCAP members and coinholders, a clear mandate for the team to pursue the work. FROST v3, the threshold-signature scheme now on a path to IETF standardization and recognized by industry participants, including Coinbase, advanced with cheater detection enabled by default. The cadence of audited, on-testnet work moving toward a coordinated upgrade is the signal here: development is continuous and converging, not stalled by the organizational transition.

SECTION 08

Forward Roadmap

Zcash's forward technical agenda is unusually concrete for a privacy network, though the headline items remain in research and testnet rather than on mainnet, and it is worth separating what is scheduled from what is still being scoped.

The near-term deliverable is Ironwood (NU6.3), the late-July recovery upgrade, which folds the corrected shielded pool, formal verification, and quantum recoverability into a single release. The principal forward effort beyond it is Project Tachyon. Led by cryptographer Sean Bowe, it aims to scale shielded transactions dramatically through oblivious synchronization (a method letting wallets query untrusted servers for the proofs they need without revealing what they are looking for), together with proof-carrying wallets and transaction aggregation. The design is staged rather than all-or-nothing, so each increment can deliver user-facing benefit ahead of the full vision. Tachyon is a research and development effort rather than a scheduled upgrade: it was included in the NU7 sentiment poll so the team could gauge whether coinholders wanted the work prioritized, and it drew more than 90% support, a clear mandate to pursue it. It is not shipping as part of NU7.

SECTION 09

Conclusion

Q2 2026 was a stress test, and the network's response is the quarter's most informative data point. A serious circuit-level flaw in the Orchard pool was surfaced, patched, and met with a coordinated, multi-stakeholder recovery upgrade, and through it, supply integrity held, with the turnstile guaranteeing no illegitimate ZEC could circulate and early evidence pointing to no exploitation. That is security-response maturity demonstrated under real conditions rather than asserted.

The onchain ledger tells an honest, two-sided story. Shielded balances contracted 14% as deshielding outpaced shielding, and the shielded share of supply eased to 26.3%, a real contraction that should not be glossed. Yet shielded transaction counts rose 11%, the anonymity set compounded to a new high of 124.1 million notes, network REV recovered 72%, difficulty reached an all-time high on the back of institutional mining capacity, and a regulated treasury buyer kept accumulating toward a 5%-of-supply goal. Usage of optional privacy intensified even as some value stepped out of the pool to await Ironwood.

The forward case rests on execution: Ironwood (NU6.3) activating cleanly in late July, delivering the corrected pool, formal verification, and quantum recoverability in one upgrade, and Project Tachyon, which coinholders have mandated the team to pursue, maturing from research toward a shippable design. Neither is guaranteed, and each remains in development or testnet today. But the structural fundamentals compound regardless: a growing anonymity set, deepening institutional conviction, and a development effort that coordinated effectively through its hardest quarter. They leave Zcash exiting Q2 with its privacy guarantee stronger, its security posture firmer, and its credibility as encrypted money at scale tested and intact.

APPENDIX

Disclosures

This research report has been funded by GenZcash. By providing this disclosure, we aim to ensure that the information reported in this document is produced 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 tokenholder 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.

All content was produced independently by the author(s) and does not necessarily reflect the opinions of Blockworks Advisory or the commissioning organization. Commissioning does not influence editorial decisions or content.

This document is provided for informational purposes only and does not constitute investment advice, an offer, or a solicitation to buy or sell any asset. Readers are advised to conduct their own independent research and seek the advice of a qualified financial advisor before making investment decisions. Digital assets are volatile and may lose some or all of their value.