GSR Research

Weekly Update

June 8th, 2026

WRITTEN BY
CARLOS GUZMAN, RESEARCH ANALYST
SLATER SANTER, RESEARCH ANALYST

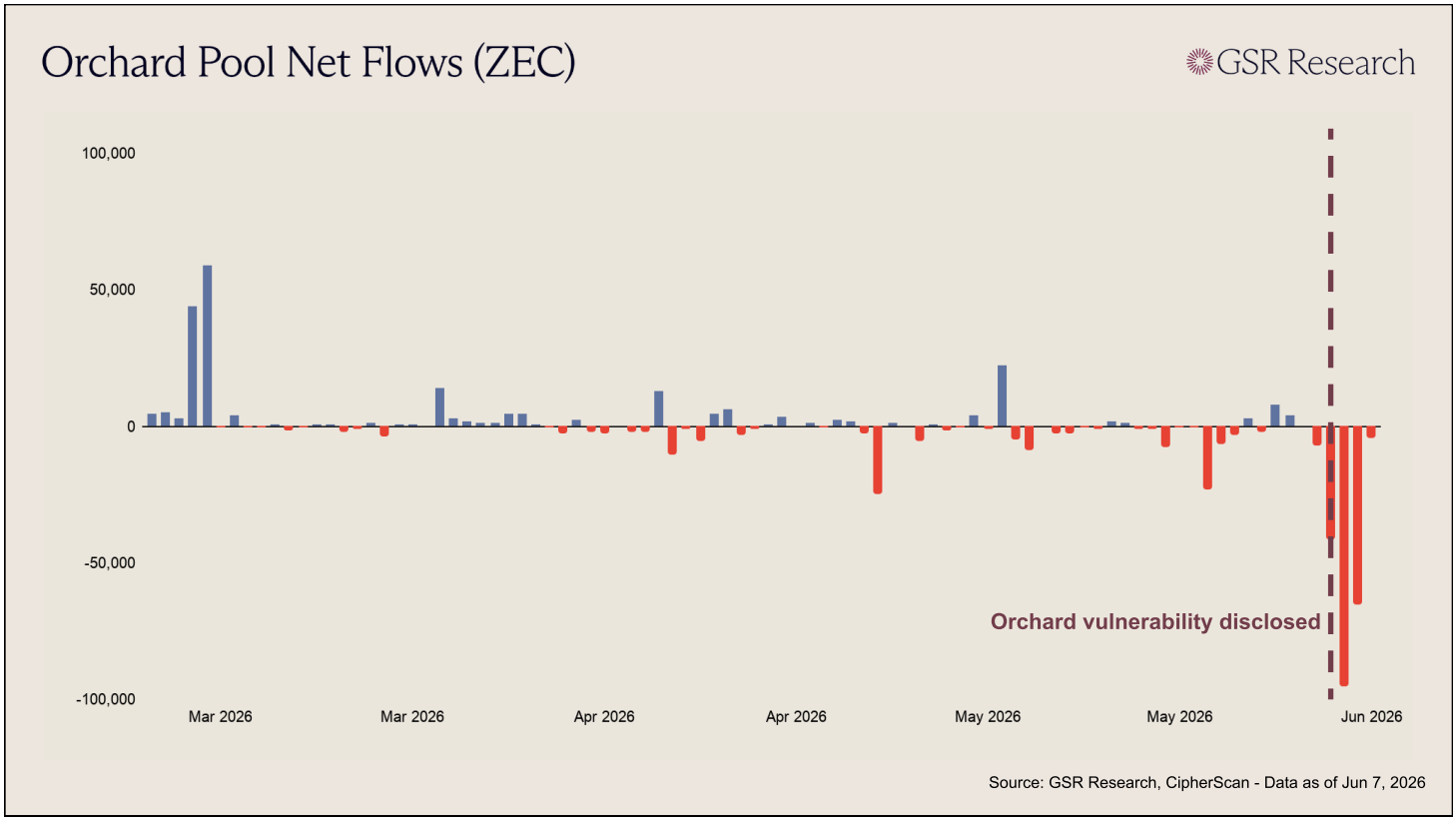
Highlights

Zcash's Infinite Mint Bug

Zcash's ZEC token crashed roughly 40% last week after the protocol's developers disclosed a critical counterfeiting vulnerability in its Orchard shielded pool, a flaw that had been present for four years and was only caught with the help of Anthropic's latest AI model. The bug could have allowed an attacker to mint unlimited, undetectable counterfeit ZEC within Orchard. Beyond the immediate fallout for Zcash, the episode highlights the unique challenges of auditing privacy-preserving cryptographic systems, and the increasingly consequential role AI plays in both finding and potentially exploiting their vulnerabilities.

Infinite ZEC

Zcash enables private transactions using zero-knowledge proofs. Users transact within shielded pools where amounts, senders, and recipients are hidden from public view, with a cryptographic circuit enforcing protocol rules without revealing private information. The Orchard vulnerability was in a circuit constraint that enforces those rules, it had been written loosely enough that it would accept false inputs into an elliptic curve operation and still pass validity checks. An attacker could have exploited this to fabricate spendable shielded notes and thus mint ZEC from nothing, without a visible trace. The flaw survived multiple security audits over four years before security researcher Taylor Hornby discovered it on May 29 using Anthropic's Opus 4.8.



Proposed Solutions & Their Limitations

The Zcash team responded quickly, they deployed an emergency soft fork on June 2 and a hard fork on June 3 to patch the circuit. To address the existential question of supply integrity, Shielded Labs has proposed "Ironwood," which would create a new shielded pool using the corrected circuit while freezing the old pool and routing all outflows through Zcash's turnstile accounting mechanism. Turnstiles track how much ZEC has entered and exited each pool and reject any withdrawal attempt exceeding legitimate inflows, giving users a way to verify total supply upon activation. This system-wide guarantee, however, doesn't resolve every concern. If the bug was exploited before being patched, counterfeit ZEC could be sitting in the old pool. The turnstile would prevent it from escaping, but the pool itself could be insolvent.

That is, if a counterfeiter has already withdrawn, legitimate users who migrate later could find themselves unable to exit. Furthermore, because it's likely that not every coin will migrate out of Orchard (e.g., some keys may have been lost), the question of whether exploitation actually occurred may never be definitively answered.

Invisible Bugs

The episode highlights a fundamental tension in zero-knowledge systems. The features that make these systems useful for privacy also makes them much more difficult to audit. Unlike bugs in transparent blockchain systems, which can be publicly identified as soon as they are exploited, bug exploits in privacy-preserving systems may leave no trace. This makes thorough system integrity from the get-go essential.

Formal verification offers a potential path forward. Instead of relying on humans to find errors in complex hand-written circuits, it enables the use of mathematical proofs to show that code conforms exactly to a specification. Shielded Labs has committed to formally verifying both the Orchard circuit and its next-generation Tachyon protocol. The idea is compelling: instead of trying to find and eliminate all the bugs, you can prove that there are none. It’s not a complete silver bullet, however, since formal verification can only guarantee code matches its specification, and the specification itself could be wrong. It helps reduce reliance on painstaking human auditing work, but still relies on human judgment to correctly specify the system in question.

Promises & Perils of Improving AI Capabilities

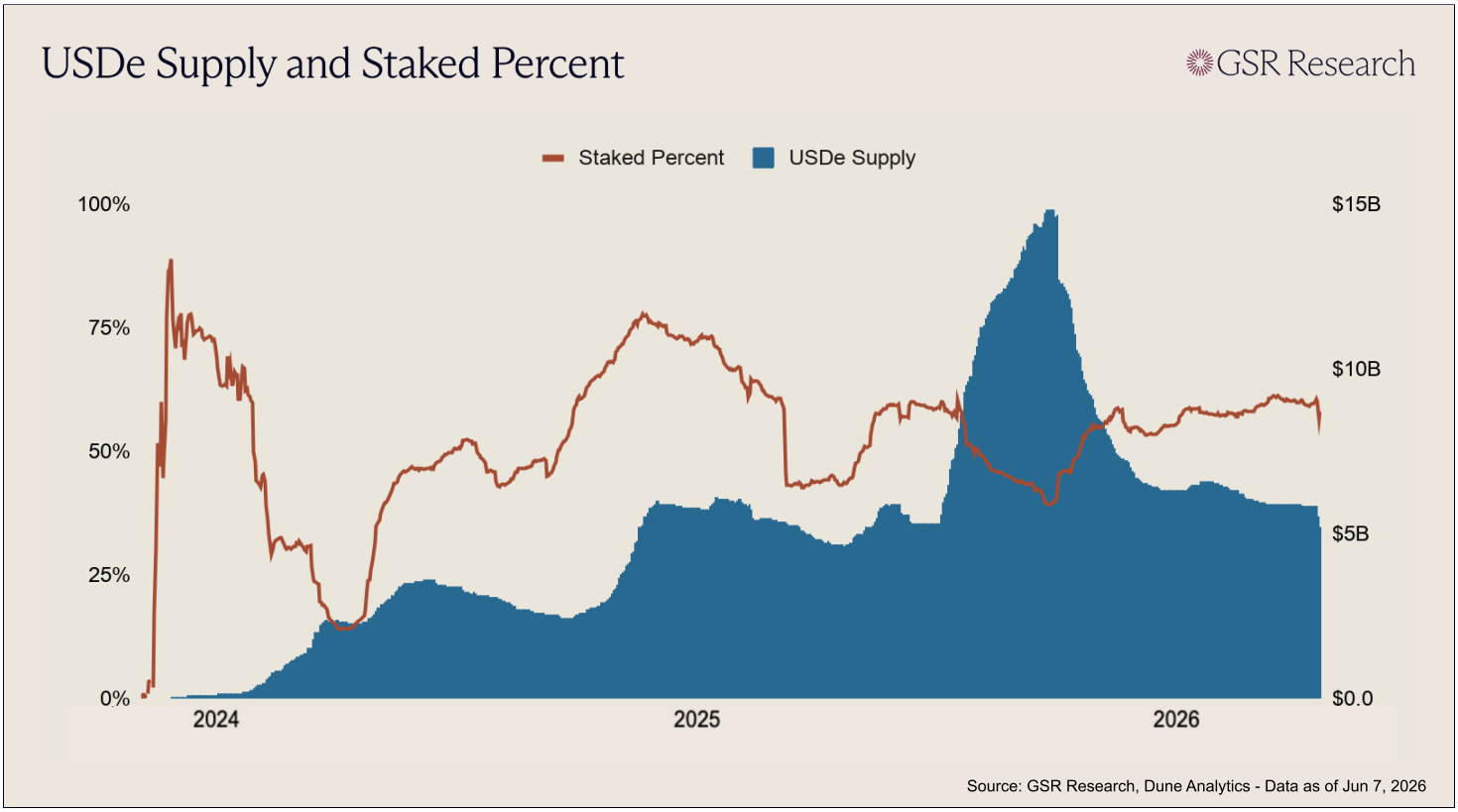
Hornby found the vulnerability with Opus 4.8 shortly after the model's release, succeeding where earlier AI systems and years of human review had not. This is the best-case scenario for AI in crypto security, a defender catching a critical flaw before an attacker can exploit it. Had a malicious actor gotten there first, the same capabilities would have enabled silent, limitless counterfeiting.

AI is also what's making formal verification newly feasible. As Vitalik Buterin has pointed out, AI agents can now write formal proofs at a pace humans never could, compressing what used to be years of labor into weeks. What was once an extremely grueling exercise, rarely undertaken in anything but the most security critical software systems, is increasingly becoming a practical tool for the defense of live crypto systems.

The race between attackers and defenders is nothing new in security, but AI is accelerating both sides simultaneously. More powerful models make tools like formal verification and AI-assisted auditing feasible at scale while also lowering the barrier to discovering and exploiting flaws. Privacy protocols thus face a particularly steep challenge in the short-term, but there’s light at the end of the tunnel.

Coinbase Partners with Ethena

Last week Coinbase and Ethena announced a partnership that will bring Ethena's onchain savings products to Coinbase's 100M+ users, while Coinbase Ventures simultaneously announced that they had made a strategic ENA investment through an open market purchase. The first initiative is expected to launch next week, with USDe and its yield-bearing form sUSDe distributed through Base and the broader Coinbase ecosystem. Additionally, Coinbase is now Ethena's primary custodian, wallet provider, and perpetuals venue, illustrating how embedded the exchange has become across Ethena's infrastructure and making the partnership deeper than a simple listing or venture investment.



Distribution, Not Just Yield

The partnership solves Ethena's biggest near-term problem: distribution. USDe was one of the fastest-growing stablecoins last fall, with supply peaking at nearly $15B before falling back toward the $5B to $6B range as funding rates and general demand cooled.

Despite the staked share of USDe remaining elevated, the protocol has lost users due to lower funding rates and subsequent compressed yields. While the protocol has maintained a smaller userbase of yield-seeking users during the bear market, it has lacked new channels for capital inflow beyond DeFi-native loops.

This makes Coinbase, an exchange with one of the largest captive dollar user bases in crypto, an ideal distribution partner for Ethena. If sUSDe yields clear baseline USDC rates, Coinbase can offer a more competitive dollar savings product, while Ethena gets access to deeper and cheaper funding than it could source from native DeFi alone. For Ethena, the partnership gives the protocol a cleaner path to growth at a time when USDe supply has already shown the cyclical nature of DeFi-native demand.

Beyond Perp Funding

The partnership coincides with Ethena's desire to reduce its reliance on perpetuals funding and diversify into a broader set of yield sources. USDe was originally presented as a synthetic dollar backed by opposing delta-neutral spot and futures positions, with sUSDe yields derived from staking rewards and funding rates. While that model works extremely well during bull markets, it compresses as the broader market softens and funding rates fall. Ethena furthermore recognized it would need other sources of yield beyond bull-market perp funding if it wanted to scale further through a regulated distribution channel like Coinbase. Consequently, Ethena has moved away from being a pure crypto basis trade, with perpetual futures now representing only a small share of USDe backing and the rest allocated across stablecoin reserves and active DeFi lending positions on Morpho and Aave.

The next phase is to diversify that backing even further through overcollateralized institutional lending of stablecoins through Anchorage Digital, RWAs beyond T-bills (AAA-rated CLOs to start), equity and commodity basis trades, and prime lending to trading firms.

The next version is no longer reliant on a single funding trade, but a generalized platform that combines perp, equity, and commodity basis trades, stablecoin reserve rewards, diverse RWA exposure, active DeFi participation, prime lending, and institutional credit into a broader stack of onchain yield. This targeted diversification makes the Coinbase partnership more credible as a broader yield stack reduces the risk that sUSDe becomes less competitive as perp funding rates collapse.

Why Not Just USDC?

While the benefits for Ethena are clear, the more interesting question is what advantage the partnership poses for Coinbase, which already has an extremely valuable stablecoin business through its relationship with Circle. Because Coinbase receives 50% of the residual revenue generated from USDC reserves, it seems logical that keeping balances in USDC would be the simple, regulated, and profitable approach. However, while USDC reserve income is a great business for Coinbase, it is not necessarily a great savings product for its users.

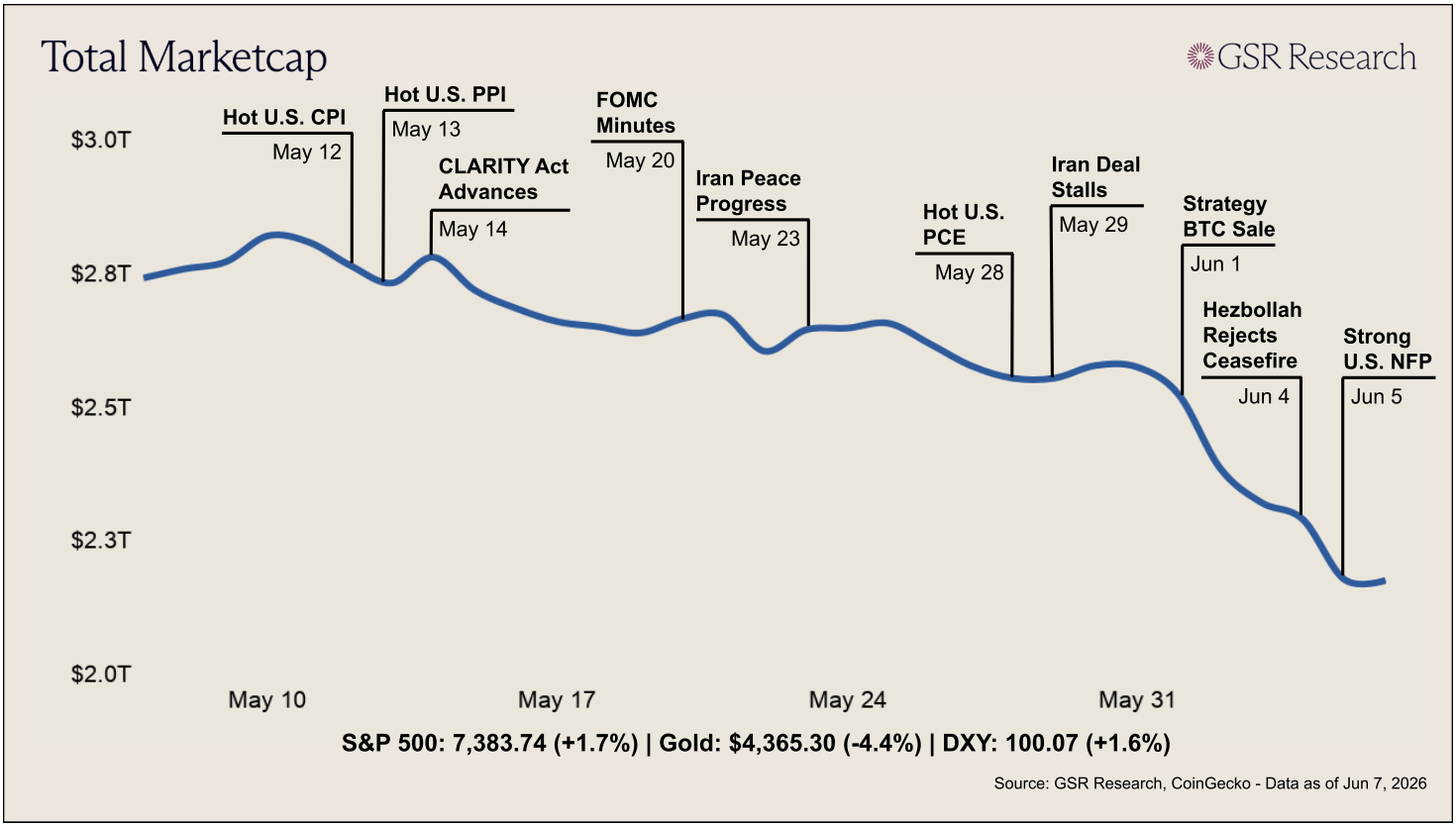
As rates fall, baseline USDC rewards become less compelling, and proposed market structure rules in The CLARITY Act have increasingly focused on restricting deposit-like stablecoin yield. Ethena gives Coinbase a more defensible route to pass through yields: an onchain savings product backed by active crypto-native and institutional yield sources rather than simply sharing reserve income.

Coinbase is not abandoning USDC, but trying to build a higher-yielding product layer around it.

If the integration functions as intended, USDC will remain the base dollar asset, with Coinbase maintaining custody, wallet, Base, and execution economics, with Ethena becoming the yield engine sitting on top. For Coinbase, the Ethena partnership is more strategically important than previous DeFi integrations, as the exchange is no longer simply routing users into onchain yield, but testing whether that yield can be packaged as a Coinbase-native dollar savings product.

.

Macro Landscape



Crypto had been softening for weeks even as equities pushed to new highs. This week, a run of macro and geopolitical catalysts turned that slow bleed into the sharpest selloff since February, with BTC falling from roughly $73,000 to a cycle low near $59,100 and total market cap contracting from approximately $2.5T to below $2.2T. The selling accelerated early in the week after Strategy disclosed its first net Bitcoin sale since December 2022, offloading 32 BTC for about $2.5 million to fund preferred stock distributions.

The amount was trivial against the company's $56 billion holding, but the symbolic break with its "never sell" identity deepened a slump in which spot Bitcoin ETFs had extended their outflow streak to roughly 13 consecutive days.

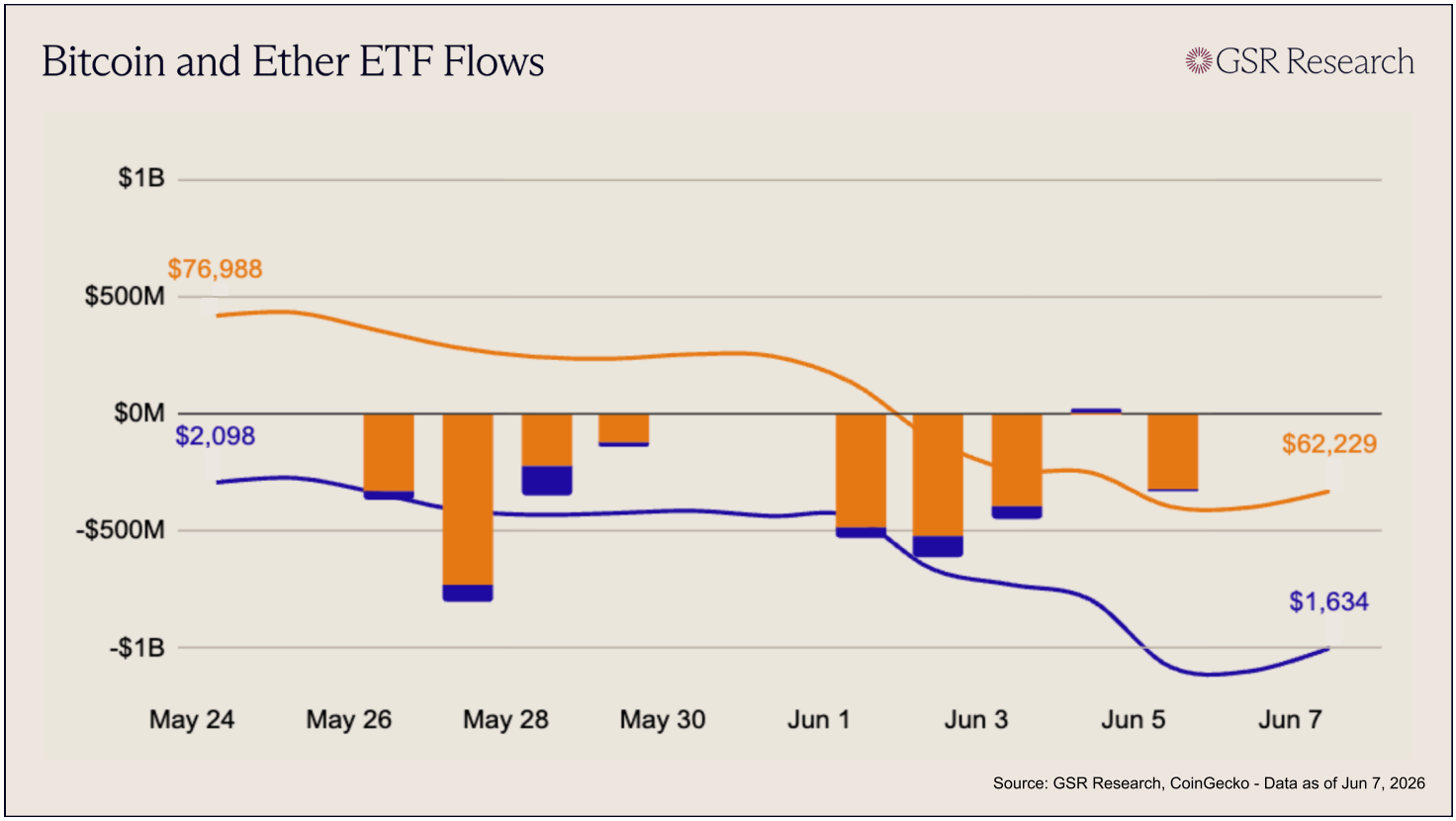
Equities also experienced losses. Broadcom beat on revenue and EPS Wednesday evening but guided Q3 AI chip sales below Street expectations, sparking a broad semiconductor selloff on Thursday that ended the S&P 500's run to new highs.

A US-brokered Israel-Lebanon ceasefire agreed at the State Department on June 3 briefly lifted risk appetite, but Hezbollah's public rejection of the deal on Thursday reversed that optimism and pushed Brent back above $95.

Friday's May payrolls came in at 172,000, more than double the 80,000 consensus, with prior-month revisions adding another 93,000 jobs. The 10-year Treasury yield jumped to 4.55% as rate hike odds for 2026 climbed to roughly 70%, effectively killing any remaining case for cuts ahead of Warsh's first FOMC on June 16-17. The Nasdaq fell 4.2% in its worst session since April 2025 and the S&P 500 dropped 2.6% to snap a nine-week winning streak. BTC broke below $62,000 before touching $59,100 overnight as $1.6 billion in positions were forcibly liquidated By Sunday, BTC had recovered to the low $60,000s on thin weekend volume, with focus now shifting to May CPI on Tuesday and Warsh's inaugural FOMC the following week.

.

ETF Flows



U.S. spot Bitcoin ETFs extended the redemption cycle this week, with outflows remaining severe despite a brief midweek interruption. The week opened with three consecutive heavy negative sessions: -$484M on Jun 1, -$519M on Jun 2, and -$397M on Jun 3, driven primarily by continued withdrawals from IBIT, FBTC, ARKB, and GBTC. A marginal positive print on Jun 4 (+$3M) technically broke the record outflow streak, but the stabilization was negligible and failed to reset the broader tone. Selling resumed immediately on Jun 5 (-$326M), leaving BTC ETFs down roughly -$1.72B for the week. The current run extended the prior record to thirteen consecutive negative sessions through Jun 3 before the small Jun 4 inflow, underscoring that institutional demand remains heavily impaired despite the brief pause.

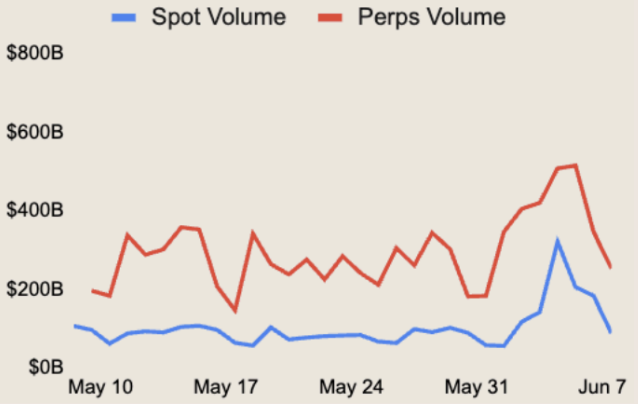
Ether ETFs followed the same broad pattern but with a smaller absolute drawdown and slightly earlier stabilization. Flows were negative to start the week, with redemptions on Jun 1 (-$45M), Jun 2 (-$90M), and Jun 3 (-$53M), extending the prior run of persistent outflows. Like BTC, ETH saw a small positive print on Jun 4 (+$19M), but this was not enough to signal a durable reversal, with flows slipping back negative on Jun 5 (-$6M). Across the week, ETH ETFs lost roughly -$174M. While the magnitude of outflows was less severe than BTC, the consistency of selling pressure continues to point to weak institutional appetite, with ETH still lacking the sustained inflows needed to mark a meaningful turn in sentiment.

Sector Performance, Top Gainers, Losers, & Volume

GSR Research

Sector	24h	7d	30d	200d	1y
Gaming	13%	32%	125%	121%	-43%
NFT	11%	15%	71%	67%	-52%
Infra	7%	-4%	7%	7%	-38%
DeFi	6%	-5%	31%	1083%	4%
Meme	7%	-5%	-18%	38%	-21%
CEX	1%	-10%	-14%	-19%	-1%
RWA	3%	-12%	-2%	-19%	-24%
AI	6%	-12%	-9%	43%	-14%
L1	5%	-12%	-13%	-19%	4%
Perps	3%	-12%	28%	37%	52%
DEX	3%	-13%	18%	20%	33%
DePIN	5%	-14%	-22%	-32%	-50%
L2	3%	-15%	-25%	-50%	-45%
Social	5%	-16%	-29%	-40%	17%
Privacy	11%	-19%	-25%	-25%	400%

Top Gainers (7D)		Top Losers (7D)	
BEAT	157.67%	ADA	-30.15%
SIREN	125.76%	APT	-27.01%
H	106.40%	ALGO	-25.84%
LAB	62.24%	BCH	-24.64%
WLD	46.79%	AVAX	-24.28%



Source: GSR Research, CoinGecko - Data as of Jun 7, 2026

Despite the selloff in the broader market, Gaming and NFT sharply outperformed this week, up 32% and 15%, respectively, with both sectors driven by Audiera's BEAT (+157.67%). SIREN (+125.76%) also surged, with the token breaking higher on a 258% jump in trading volume and a 53% rise in open interest. H (+106.40%) and WLD (+46.79%) both benefited from renewed demand for proof-of-humanity and AI identity tokens, with H supported by new staking incentives and WLD boosted by an upcoming 43% reduction in daily emissions.

Broader performance was weak, however, with most sectors down double digits on the week.

Privacy was the clear laggard, down 19%, as ZEC (-22.73%) sold off after the disclosure of a critical Orchard shielded-pool bug that could have allowed undetectable counterfeit ZEC creation. L1 weakness was broad, with ADA (-30.15%), APT (-27.01%), ALGO (-25.84%), and AVAX (-24.28%) all among the week's top losers. ADA fell to multi-year lows after Charles Hoskinson said he was taking a break and warned of a potential wave of Cardano ecosystem failures, while APT was pressured by an upcoming unlock on June 12. ALGO retraced as its post-quantum narrative faded, BCH (-24.64%) broke below multi-year support, and AVAX fell to early-2021 support amid the broader liquidation wave.

The Week Ahead: What to Watch

Monday, Jun 8	ETHConf 2026 Begins (New York)
Wednesday, Jun 10	U.S. CPI Inflation Data (May) China CPI Inflation Data (May)
Thursday, Jun11	European Central Bank Monetary Policy Decision U.S. PPI Inflation Data (May) U.S. Initial Jobless Claims
Friday, Jun 12	Michigan Consumer Sentiment Index (June)

Other Stories

Strategy buys 1,550 bitcoin for $101 million as total holdings rise to 845,256 BTC *The Block*

Bitmine files for preferred stock offering, proposing a yield of 9.5% *Bitmine*

Securitize clears SEC registration statement hurdle, sets path to NYSE listing as SECZ *The Block*

Coinbase launches Pre-IPOs, starting with SpaceX *Coinbase*

Variant raises $222 million for new fund with a thesis of AI, crypto and 'autonomy' *Fortune*

Morgan Stanley lets clients lend bitcoin and other assets for spot crypto ETF conversions *The Block*

Stripe, Visa, Mastercard said to be among backers of soon-to-debut stablecoin platform *CoinDesk*