GSR Research

Weekly Update

April 6th, 2026

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

Highlights

Quantum Computing Leaps Forward

Last week, two organizations independently published research significantly reducing the estimated resources required for quantum computing to break the elliptic curve cryptography (ECC) that underpins virtually every major blockchain. A team from Google Quantum AI, which included Ethereum researcher Justin Drake and Stanford cryptographer Dan Boneh, proposed a lower-overhead implementation of Shor's algorithm that could theoretically crack a private key using fewer than 500,000 physical qubits, a 20-fold reduction from previous estimates. A separate group from Caltech and UC Berkeley showed that as few as 26,000 neutral-atom qubits could achieve the same result, though over a longer timeframe. Neither result means a quantum attack on crypto is imminent, but together they meaningfully compress the timeline on which the industry needs to prepare.

Most blockchains use elliptic curve digital signature algorithms to authenticate transactions. The security of these signatures relies on the computational difficulty of deriving a private key from its corresponding public key. Classical computers are unable to solve this problem in any practical timeframe. A sufficiently powerful quantum computer running Shor's algorithm, however, could. Bitcoin, Ethereum, and many other major chains rely on elliptic-curve public-key cryptography, meaning the risk to cryptocurrencies is systemic.

Last week's research is significant because of the scale of improvement. Resource estimates for attacking ECC have been declining at an accelerating rate, with last week marking an order-of-magnitude reduction in physical qubit requirements. A year ago, the best estimates required millions of physical qubits to break elliptic curve cryptography. Google’s research brings that number to sub-500,000 for superconducting architectures, while Caltech’s lowers it further for neutral atoms, below 26,000. Both figures now fall within the published roadmaps of several leading quantum labs for the late 2020s and early 2030s.

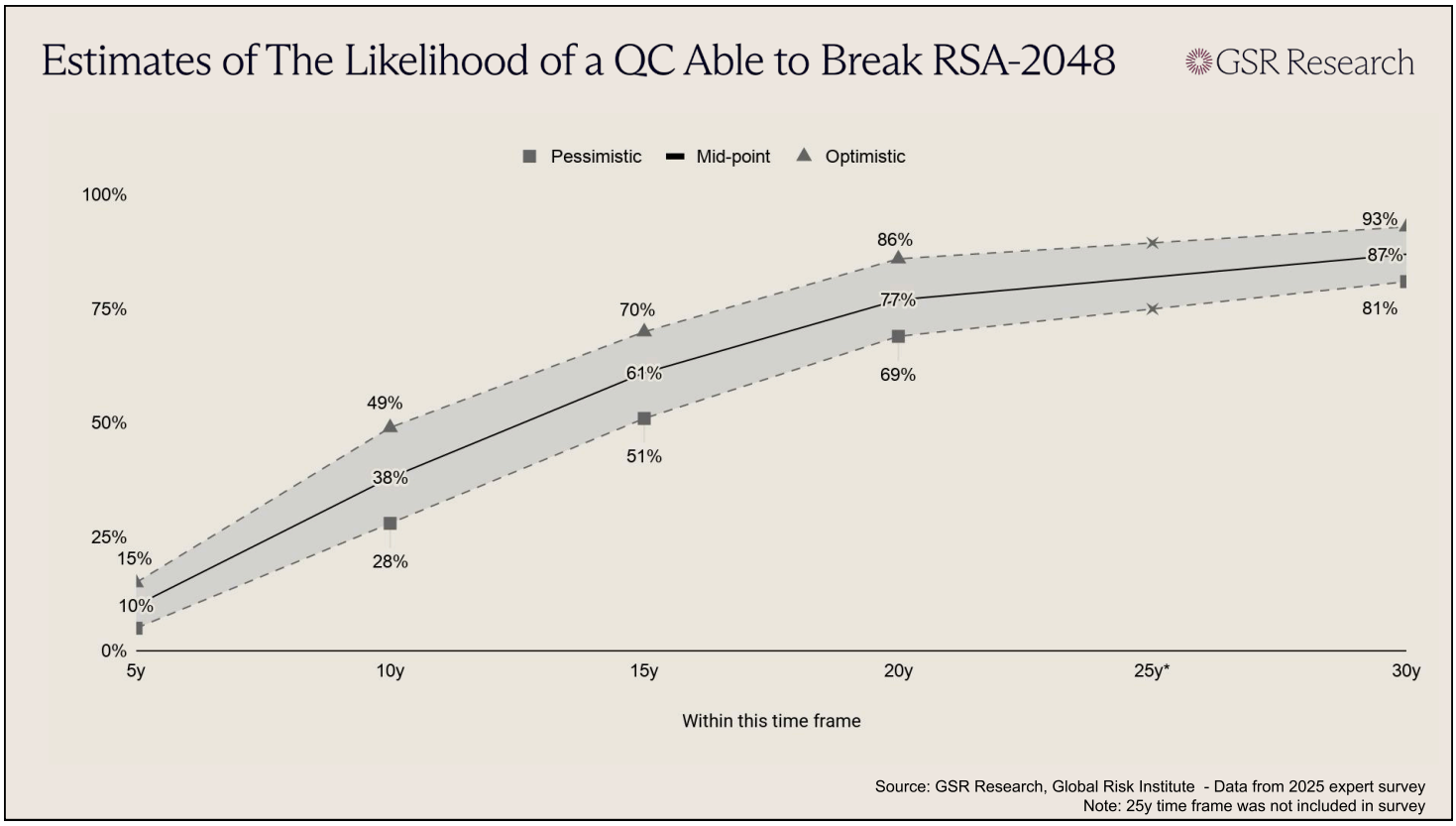
It’s worth pointing out that there is still a substantial gap between theoretical resource estimates and actual hardware capabilities. No quantum computer has reliably factored anything beyond trivially small numbers using Shor's algorithm. The Global Risk Institute's latest survey of 26 quantum computing experts places the

average estimated likelihood of a cryptographically relevant quantum computer at 28% to 49% within 10 years and 51% to 70% within 15 years. However, the 2025 survey was conducted before last week's research was published, and already marked a notable acceleration from prior years. Even conservatively, these are probabilities the crypto industry cannot ignore.

The gap in preparedness across major protocols is significant. Ethereum has been working on post-quantum cryptography (PQC) for several years and is a leader in the area among major blockchains. The Ethereum Foundation (EF) published a formal PQC roadmap in February, launched a dedicated resource hub in March, and has around 10 client teams running weekly PQC interoperability devnets.

The EF has a plan for upgrades across different layers of the protocol, including quantum-resistant signatures through account abstraction on the execution layer, hash-based validator signatures aggregated on the consensus layer, and PQC-secured data availability on the data layer. The Foundation is targeting 2029 for quantum resistance, a timeline that now aligns with Google's own internal deadline for migrating its authentication services to PQC.

Bitcoin faces a structurally harder challenge. The protocol has no coordinated PQC roadmap, no equivalent of the Ethereum Foundation to fund and direct a multi-year engineering effort, and a governance model that makes large-scale changes slow and politically difficult.



BIP-360 proposes quantum-resistant address formats, but it remains a proposal. Chaincode Labs has estimated that an emergency PQC migration would take at least two years, with a more realistic timeline closer to seven. Meanwhile, roughly 6.9 million BTC (worth ~$480B at current prices) sit in addresses where public keys have already been exposed on chain, representing a significant pool of assets that would be directly vulnerable to a quantum attack.

Although the existence of a cryptographically relevant quantum computer is likely still years away, the industry needs to start taking preparations seriously now. Upgrading decentralized protocols is a multi-year coordination problem that needs to begin well before the threat materializes, and the margin of safety for planning mitigations and upgrading is narrowing quickly.

Aave V4 Launches on Ethereum Mainnet

On March 30th Aave Labs launched Aave V4, a ground-up rewrite of how the protocol structures liquidity, risk, and market expansion. The rollout has prioritized security, with formal verification, multiple audit rounds, invariant testing, fuzzing, and a large Sherlock contest preceding mainnet. Rather than immediately forcing a migration, Aave chose to deploy V4 alongside V3, a decision that reflects the large scale of change between the two iterations. DeFi lending is still constrained by fragmented liquidity, blunt risk pricing, and growing governance overhead as protocols expand into additional assets and market types. Where V3's challenge was bootstrapping deposits, V4 tries to shift the bottleneck toward creating safe, new demand by unifying liquidity into shared hubs while allowing specialized markets to plug in as modular spokes, enabling new collateral types and strategies to access deep capital from day one without fragmenting the balance sheet or compromising risk isolation.

V4 is designed to turn Aave's deep protocol liquidity into reusable infrastructure. On V4's new Aave Pro a market is effectively defined by a Spoke plus a Hub. The simplest way to conceptualize the upgrade is that Hubs represent the balance sheets while Spokes act as the rulebooks. Liquidity sits in a Hub, while users interact through Spokes that determine accepted collateral, borrowable assets, and liquidation logic. As a result, new markets no longer need to bootstrap their own deposit base from scratch as they did in V3, as lending markets will now have the ability to plug into shared liquidity from day one.

As of writing, the protocol has released three Ethereum Liquidity Hubs (Core, Prime, and Plus), plus tight initial caps that the DAO can raise over time as behavior is observed in production. Core is the default liquidity venue, Prime is intended to offer a more controlled collateral posture, and Plus

is designed for more strategy-heavy stablecoin activity. V4 also connects Hubs through governance-controlled credit lines, allowing specialized markets to draw on Core's liquidity without collapsing all assets into a single pool. Aave is intentionally aiming to keep the shared core as simple as possible. The Hub contracts are designed to be immutable by default, with new functionality expected to come from adding Spokes rather than constantly rewriting the core. This underscores the broader V4 philosophy: keep the balance sheet compact and auditable while pushing specialization to the edges.

The initial Spoke mix illustrates what Aave aims to accomplish with V4. Rather than launching a single, generalized Ethereum market, V4 segments use cases into tightly scoped venues. That includes narrow, protocol-specific LST and LRT leverage environments like Lido, EtherFi, Kelp, and Lombard BTC, alongside more unusual categories such as gold and forex-style markets. The modularity is purposeful, as it expands the range of assets and strategies Aave can support without forcing all of them into the same assumptions or fragmenting liquidity across a growing list of siloed pools.

V4 also introduces an innovative Risk Premiums upgrade. In V3, two users borrowing the same asset face similar rates even if one posts a much safer collateral than the other. V4 adds a collateral-dependent surcharge on top of a Hub's base borrow rate, so stronger collateral (stablecoins and majors) can receive better terms, while riskier positions pay more. This removes some of the hidden cross-subsidies in V3 and gives Aave more room to support non-standard collateral, structured credit, and other specialized markets without distorting pricing for the rest of the system.

Collateral and Borrow Assets by Spoke

GSR Research

Spoke	Collateral	Borrow
Main Spoke	wETH, wstETH, wBTC, cbBTC, USDT, USDC, LINK, AAVE	wBTC, cbBTC, wETH, USDT, USDC, USDG, RLUSD, frxUSD, GHO, EURC
Lido (e-Mode)	wstETH	wETH
EtherFi (e-Mode)	weETH	wETH
Kelp (e-Mode)	rsETH	wETH
Lombard BTC (e-Mode)	LBTC	wBTC, cbBTC
Gold Spoke	XAUt	USDT, USDC, EURC

Source: GSR Research

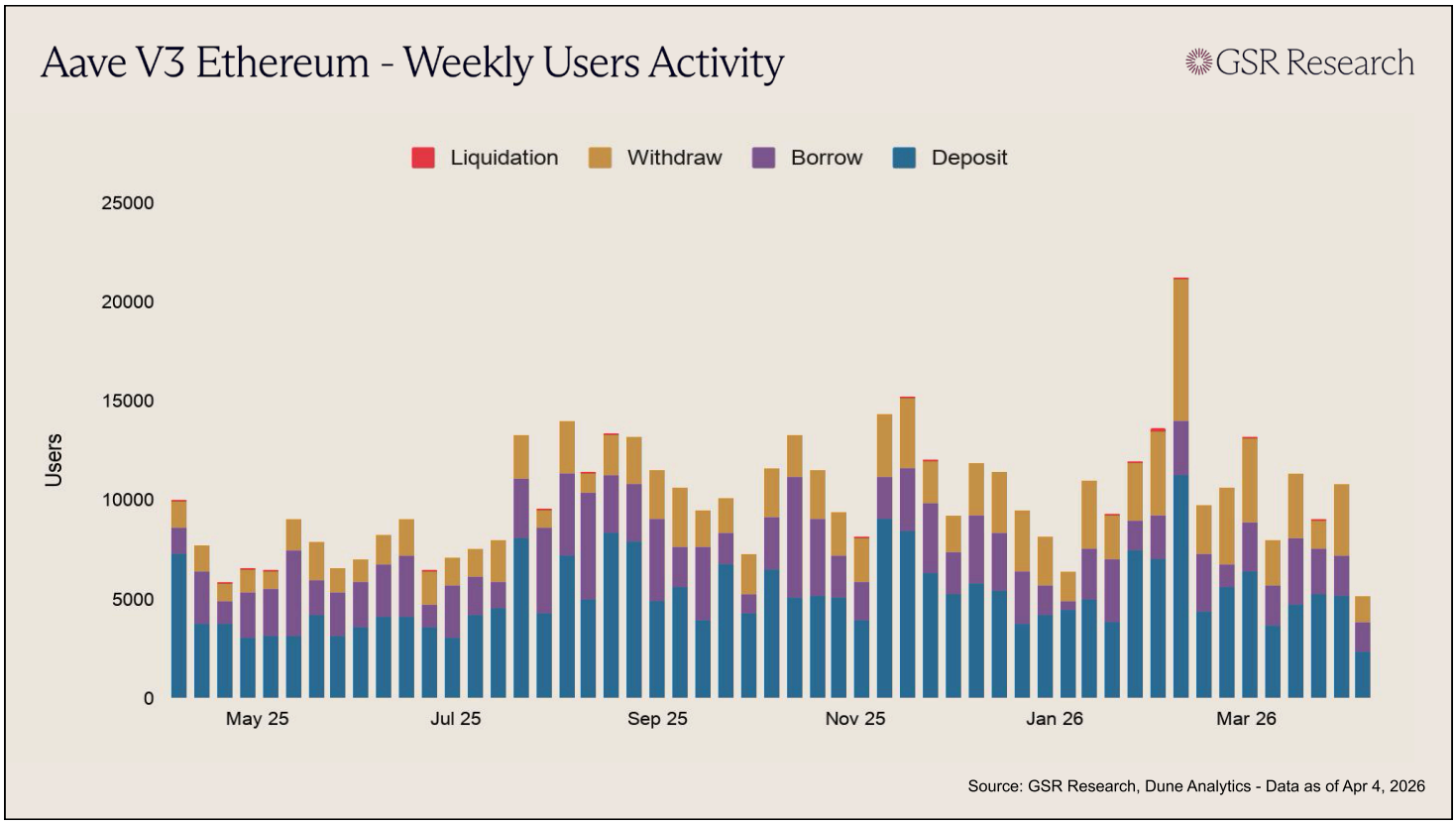
The upgrade also allows Aave's governance to become more precise. V4's Dynamic Risk Configuration system enables new risk settings to apply to new positions, while existing positions remain on the configuration they opened under unless the user takes an action that increases risk, such as borrowing more or withdrawing collateral. This reduces one of DeFi's biggest pain points, where governance updates can render old positions unsafe. V4 likewise updates how liquidations are structured. Instead of relying on fixed close factors, V4 aims to liquidate only enough debt to restore a position to a governance-defined target health factor, with bonuses that increase as a position becomes more distressed.

Additionally, Aave is adding several less-flashy features that could become increasingly important as V4 utilization increases. Position Managers create a native delegation and automation primitive, but with two layers of control: they must be approved by governance and then explicitly authorized by the user. Native multicall will make common workflows cheaper and easier to execute, while the optional reinvestment module gives governance a way to deploy a portion of idle Hub liquidity into approved strategies to improve supplier returns. Aave says it currently holds roughly $20B in stablecoin deposits with around $6B sitting available for borrowing, and has argued that reinvesting excess stablecoin liquidity at SOFR-like rates would have lifted the average stablecoin deposit APY from 4.00% to 4.93%. This means that V4 represents more than a risk-management upgrade, as it's an attempt to make Aave's deposit yields more competitive when borrow demand is soft.

The timing on the upgrade is notable, as DeFi yields have largely been compressed during the bear market as borrower demand has declined.

V4 has been in the works since Aave's 2024 roadmap, and has still made it to mainnet despite a public governance rupture in late 2025. The ongoing dispute between the DAO and key contributors is operationally relevant because on top of being more modular, V4 is more demanding to run. Multiple hubs, multiple spokes, cross-hub credit lines, and more configurable liquidations will all create more surfaces to monitor. Aave seems aware of that, which is why the rollout is slow, with many of the most important variables governance-set rather than fixed protocol constants, and V4 is expected to coexist with V3 for a long time, potentially 24 - 36 months. Early TVL will likely be determined more by migration and incentives than durable product-market fit. The more indicative signals of early adoption will be hub utilization, spoke-level borrow growth, and how heavily Prime and Plus rely on Core-sourced liquidity.

Historically, across Aave V3, depositors have made up about 51% of the weekly activity mix, borrowers around 26%, withdrawers about 23%, and liquidated users just 0.3%. However, the mix clearly turns more defensive during stress: the withdrawal share rose from roughly 18% in mid-2025 to about 29% in Q1 2026, with the biggest spikes clustering in early February alongside the highest liquidation counts. V4 should eventually tilt more toward borrow and withdraw activity as specialized spokes attract more strategy-heavy users, but the early data may still look deposit-heavy due to initial caps being so



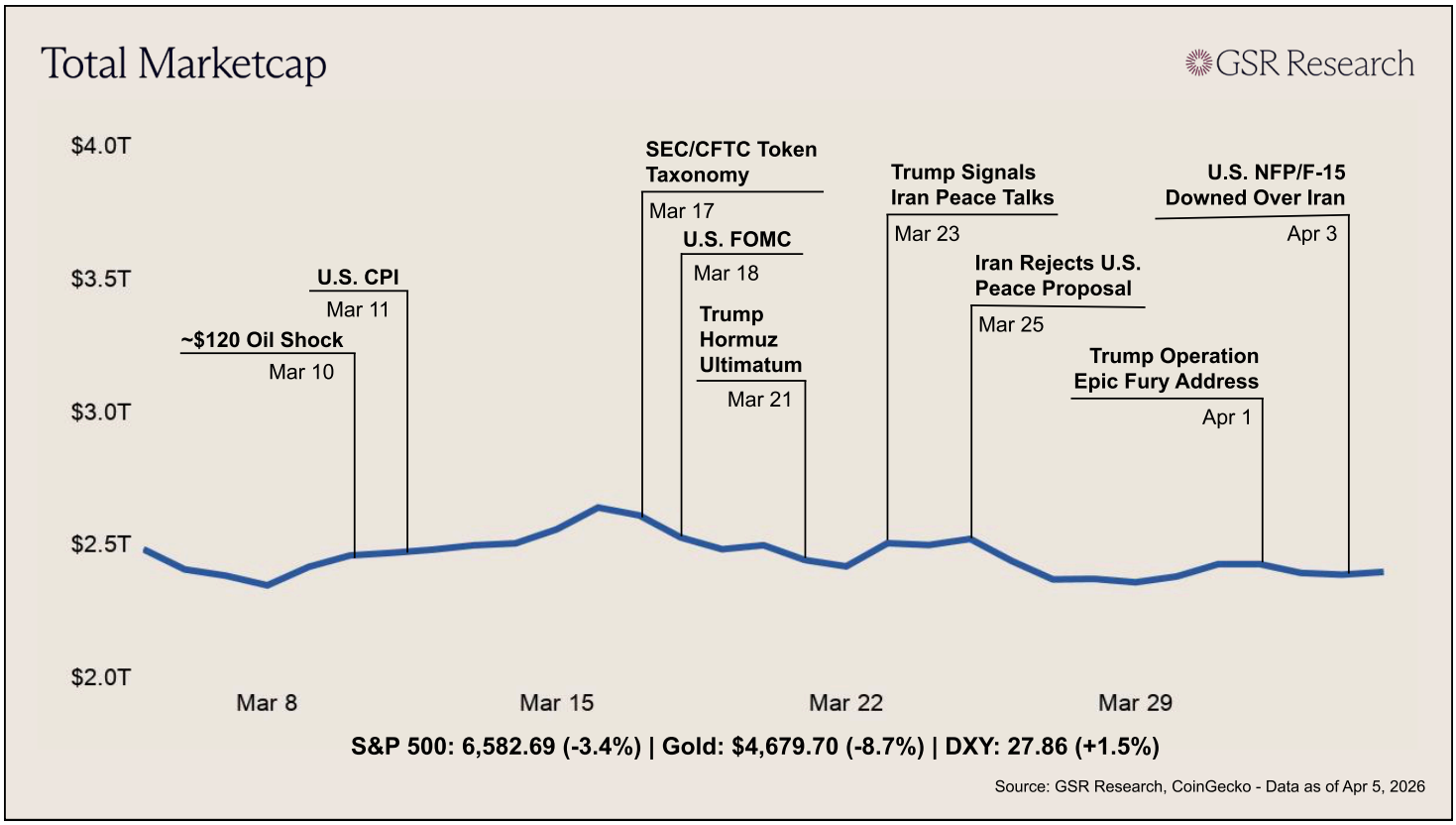
conservative. Over time, Position Managers and multicall should also smooth some of the manual withdrawal spikes, while the target-health-factor liquidation engine will further reduce liquidation activity on the margin by reducing over-liquidation.

If Aave V4 works as intended, it will do more than just replace V3, as it will mark a shift in how onchain credit scales. Instead of fragmenting liquidity across an ever-growing set of pools, V4 concentrates capital and expands outward through modular markets, where new collateral types, structured products, and institutional use cases can plug into shared depth without introducing systemic risk.

This shifts the challenge in lending and borrowing markets from attracting liquidity to managing it, with governance, risk operations, and monitoring infrastructure becoming the true limiting factors. In the near term, progress will likely be uneven as caps, credit lines, and spoke configurations are tuned in real time. Longer term, if Aave can prove that unified liquidity plus granular risk controls are both safe and flexible, it could meaningfully expand the design space for DeFi lending, moving the market beyond generalized pools toward a segmented, strategy-driven credit system that more closely resembles traditional financial markets, but with onchain composability layered on top.

Market Update

Macro Landscape



Crypto markets posted a modest bounce alongside equities as diplomatic optimism briefly took hold before giving way to renewed escalation. The total crypto market cap opened near $2.37T, and BTC initially held around $66,500 following two consecutive losing weeks. Sentiment shifted on Wednesday when Trump addressed the nation from the Oval Office suggesting the war could end within two to three weeks. Risk assets rallied in response, with the S&P 500 surging and BTC bouncing off its weekly lows. However, the optimism proved fleeting. Later that day Iran's IRGC threatened to attack U.S. tech companies operating in the Middle East, including Nvidia, Apple, Microsoft, and Google.

By Thursday, Trump acknowledged the conflict would continue for weeks and signed a pair of Liberation Day anniversary tariffs, including tariffs on pharmaceuticals, steel, aluminum, and copper imports. Equities slumped in early trading before recovering intraday on reports that Tehran was working with Oman on a protocol to monitor ships through the Strait of Hormuz. On Saturday, Trump issued a fresh 48-hour ultimatum threatening to destroy Iran's power plants and bridges if the strait was not reopened by Tuesday. Iran's military dismissed the threat, and mediators from Pakistan, Turkey, and Egypt are now working to bring both sides to the table.

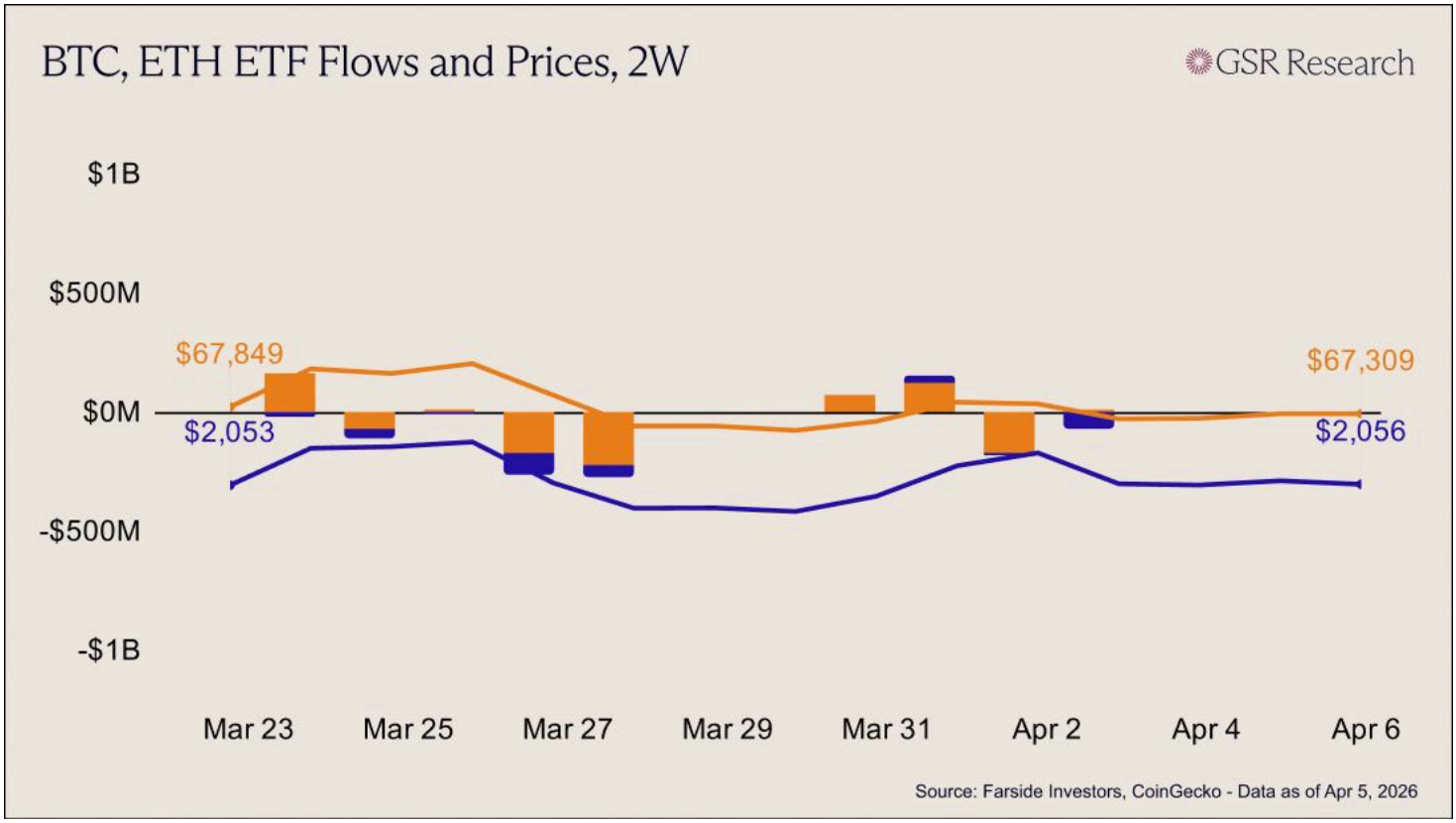
Economic data reinforced the stagflationary narrative that has been building since the war began. The ISM Manufacturing PMI came in at 52.7 on Wednesday, the strongest expansion since August 2022, but the Prices Index jumped 7.8 points to 78.3, its highest since June 2022, driven by steel, aluminum, and petroleum costs. This was the first ISM report in which panelists cited the Iran war as a direct impact on their business, with roughly 40% of negative comments referencing the conflict. On Good Friday, with equity markets closed for Easter, the BLS reported nonfarm payrolls of +178,000, nearly triple the 60,000 consensus. Wages rose just 0.2% for the month and 3.5% year-over-year, the weakest annual increase since May 2021. With the ISM Prices Index at levels not seen since the 2022 inflation surge and Brent crude closing the week above $109, markets are pricing a low probability of a Fed rate cut through year-end.

The conflict escalated sharply in the second half of the week. On Friday, an American F-15E Strike Eagle was shot down over central Iran, the first U.S. warplane lost in combat since 2003. The missing crew member was extracted by SEAL Team 6 on Saturday night after evading Iranian forces for over 24 hours. The Good Friday and Easter closures left equity and ETF markets offline for the long weekend, removing institutional demand and leaving crypto as one of the few liquid venues for expressing macro views.

The S&P 500 closed Thursday at 6,583, posting a 3.4% weekly gain and its first positive week in six, though the bounce was largely technical after the index had fallen nearly 10% from its January highs. BTC traded up to around $68,900 by Sunday, roughly 3.5% above its prior-week close.

Despite the macro overhang, the week included several positive industry headlines. On Thursday, Coinbase received conditional OCC approval for a national trust bank charter, a significant step toward operating as a federally regulated custodian with $376 billion in crypto assets under custody. The same day, Charles Schwab confirmed that its spot Bitcoin and Ethereum trading platform is on track for launch in H1 2026, with a waitlist now open for the $12 trillion asset manager's clients. The CLARITY Act's path forward remained complicated after Coinbase rejected the updated stablecoin yield compromise the prior week, pushing the Senate Banking Committee markup to late April. As we've pointed out in recent weeks, the accelerating convergence between traditional finance infrastructure and crypto rails continues to lay groundwork that markets will likely reprice once the geopolitical fog lifts.

ETF Flows



ETF flows showed signs of tentative recovery early in the week before succumbing to mid-week volatility. U.S. spot Bitcoin ETFs broke the bearish streak from late March, opening with net creations of +$69.4M on Monday and +$117.5M on Tuesday. This early momentum was abruptly tested on Wednesday by a sharp reversal of -$173.7M, driven by uncharacteristic redemptions in BlackRock's IBIT and Fidelity's FBTC. A marginal stabilization of +$9.0M on Thursday left the four-day trading period at a slim net positive of +$22.2M. Correspondingly, Bitcoin prices climbed from a Monday low of $66.7k to a weekly peak of $68.2k on Tuesday, before the mid-week outflow forced a retreat toward the $66.9k handle.

Ether ETF flows mirrored this pattern but with significantly less resilience. The week began with two green prints (+$5.0M and +$31.2M), but the trend crashed into a heavy wall of selling toward the close. The -$71.2M redemption on April 2nd, which was largely fueled by exits from BlackRock's ETHA, wiped out all early-week gains, leaving Ether funds with a net weekly outflow of -$42.1M. This lack of sustained institutional demand kept Ethereum in a precarious technical position; while it briefly reclaimed the $2,139 level on Wednesday, it swiftly retreated to $2,057 by Thursday's close. ETH continues to struggle for a narrative breakout, as the spot products fail to find the same dip-buying support seen in the Bitcoin complex.

Overall, the majors remained largely range-bound throughout the week as the market entered a consolidation phase. Bitcoin traded flat from $66.7k to $67.3k (+0.9%), while Ether moved from $2,024 to $2,056 (+1.6%).

Despite the intra-week push toward higher resistance levels, the inconsistent ETF tape suggests that institutional conviction remains cautious following the volatility of mid-March.

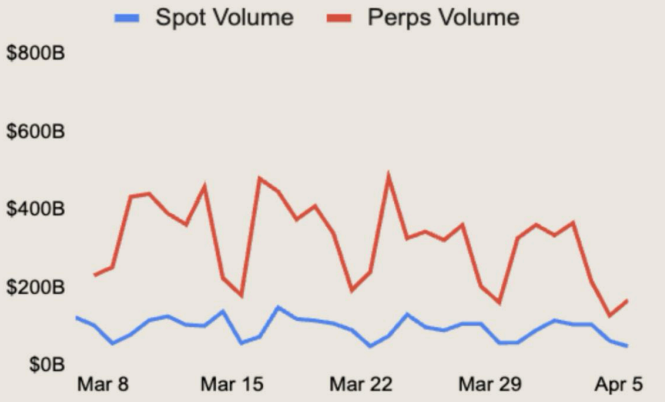
Sector Performance

Sector Performance, Top Gainers, Losers, & Volume

GSR Research

Sector	24h	7d	30d	200d	1y
Privacy	1%	5%	3%	154%	248%
Gaming	-1%	3%	30%	-41%	-53%
RWA	-1%	3%	1%	-39%	-12%
Infra	-1%	2%	-3%	-50%	-32%
NFT	-2%	2%	11%	-58%	-48%
Meme	-2%	1%	11%	-46%	-13%
AI	-2%	1%	13%	-44%	-17%
DePIN	-2%	0%	25%	-40%	-13%
L2	-2%	0%	-6%	-66%	-40%
L1	-1%	-1%	2%	-33%	2%
CEX	-1%	-1%	-6%	-17%	34%
Social	-1%	-1%	-10%	-67%	154%
DeFi	-2%	-3%	0%	-23%	34%
DEX	-1%	-5%	5%	-41%	90%
Perps	-1%	-5%	12%	-33%	140%

Top Gainers (7D)		Top Losers (7D)	
ALGO	46.21%	RAIN	-21.33%
VET	13.64%	NIGHT	-15.57%
ZEC	12.15%	ENA	-14.22%
M	11.85%	APT	-8.77%
JUP	11.54%	HYPE	-8.77%



Source: GSR Research, CoinGecko - Data as of Apr 5, 2026

Most sectors traded flat on the week, following the price action of the majors. ALGO (+46.21%) was this week's top gainer, as the Google Quantum AI research paper on threats to major blockchains mentioned Algorand twice as many times as any other project. Additionally, the privacy sector posted a 5% week-over-week gain, due to a Zcash (+12.15%) surge early in the week. The ZK-focused L1 had some choppy performance following its historic 1300% rally in Q4 2025, but has since consolidated and is now positive across all timeframes.

Perps (-5%) were the worst performer on the week as HYPE fell 9% and Aster traded flat. Despite Hyperliquid being the standout performer of the bear market, perps are down 33% on the 200d timeline, meaning they have been outperformed by the privacy, centralized exchange, and DeFi sectors since September. For each of these categories, their performances have largely been driven by a singular project (Zcash, Whitebit, Hype).

The Week Ahead: What to Watch

Wednesday, Apr 8	U.S. FOMC Minutes
Thursday, Apr 9	U.S. PCE Inflation Data (Feb) U.S. Initial Jobless Claims China CPI and PPI Inflation Data
Friday, Apr 10	U.S. CPI Inflation Data (Mar) U.S. Michigan Consumer Sentiment Index

Other Stories

Franklin Templeton buys Coinfund spinoff and establishes Franklin Crypto *WSJ*

CFTC Sues 3 States to reaffirm its jurisdiction over prediction markets *CFTC*

Coinbase receives conditional OCC approval *Coinbase*

Midas raises $50M to tackle pain point for tokenized asset investors *CoinDesk*

Charles Schwab plans to launch BTC and ETH trading in H1 2026 *CoinDesk*

Drift suffers exploit likely at the hand of DRPK hackers *CoinDesk*

Circle unveils plans for wrapped bitcoin token cirBTC *The Block*