GSR Research

Weekly Update

August 3rd, 2026

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

Highlights

Zcash's Ironwood Upgrade and Formal Verification in Crypto

Zcash activated its Ironwood upgrade last Tuesday, replacing the Orchard shielded pool with a new, formally verified pool after a critical counterfeiting vulnerability had gone undetected in Orchard for four years. Ironwood seals entry into Orchard, which holds roughly 3.66 million ZEC worth about $1.7 billion, and routes all outflows through a turnstile mechanism that caps withdrawals at verified deposits. As we covered previously, the upgrade itself is important for Zcash and helps restore confidence in the protocol. However, there's another interesting story related to the way the upgrade was built: it provides an early example of an emerging approach to crypto development that could transform how protocols are secured.

Proving bugs don't exist

What sets Ironwood apart is that the new pool's zero-knowledge proof circuit was formally verified using the Lean theorem prover, with over 2,700 machine-checked theorems confirming the pool's balance integrity under its stated cryptographic assumptions. Instead of relying solely on auditors to find every possible flaw, the team produced a mathematical proof that the class of bug which broke Orchard simply cannot exist in Ironwood. Co-founder Sean Bowe described the effort as eliminating all sources of undetectable counterfeiting bugs from the new protocol.

Formal verification of code is not new, it has been employed for decades in security critical applications across industries like aerospace and defense. However, given the difficulty associated with it and the scarcity of expert talent, the use of formal verification in crypto has been limited. The Ironwood upgrade illustrates how AI-powered development is beginning to radically change this dynamic by expanding access to these capabilities and greatly reducing development timelines. In Sean Bowe's telling, AI-assisted development is what enabled the turnaround time on the formally verified Ironwood upgrade to occur in just a few weeks.

This feat is reminiscent of the approach Vitalik Buterin outlined in a May post on formal verification: AI writes code in low-level languages while simultaneously generating machine-checked proofs of correctness.

Ironwood is an early production exhibit of that vision. Although it still seems futuristic, evidence is increasingly mounting that the tools to scale this approach are maturing quickly. On Saturday, OpenAI revealed that its unreleased Astra model solved or made substantial progress on ten long-standing problems in mathematics and computer science, with arguments generated by the model and then formalized in Lean. The problems had had seen no major progress for at least a decade each, and the estimated compute cost was roughly $2,000 at current API rates. While this achievement is not directly related to crypto, it shows AI models are becoming remarkably capable at exactly the kind of mathematical reasoning formal verification demands, which should keep pushing its cost down and make it accessible to a wider set of projects.

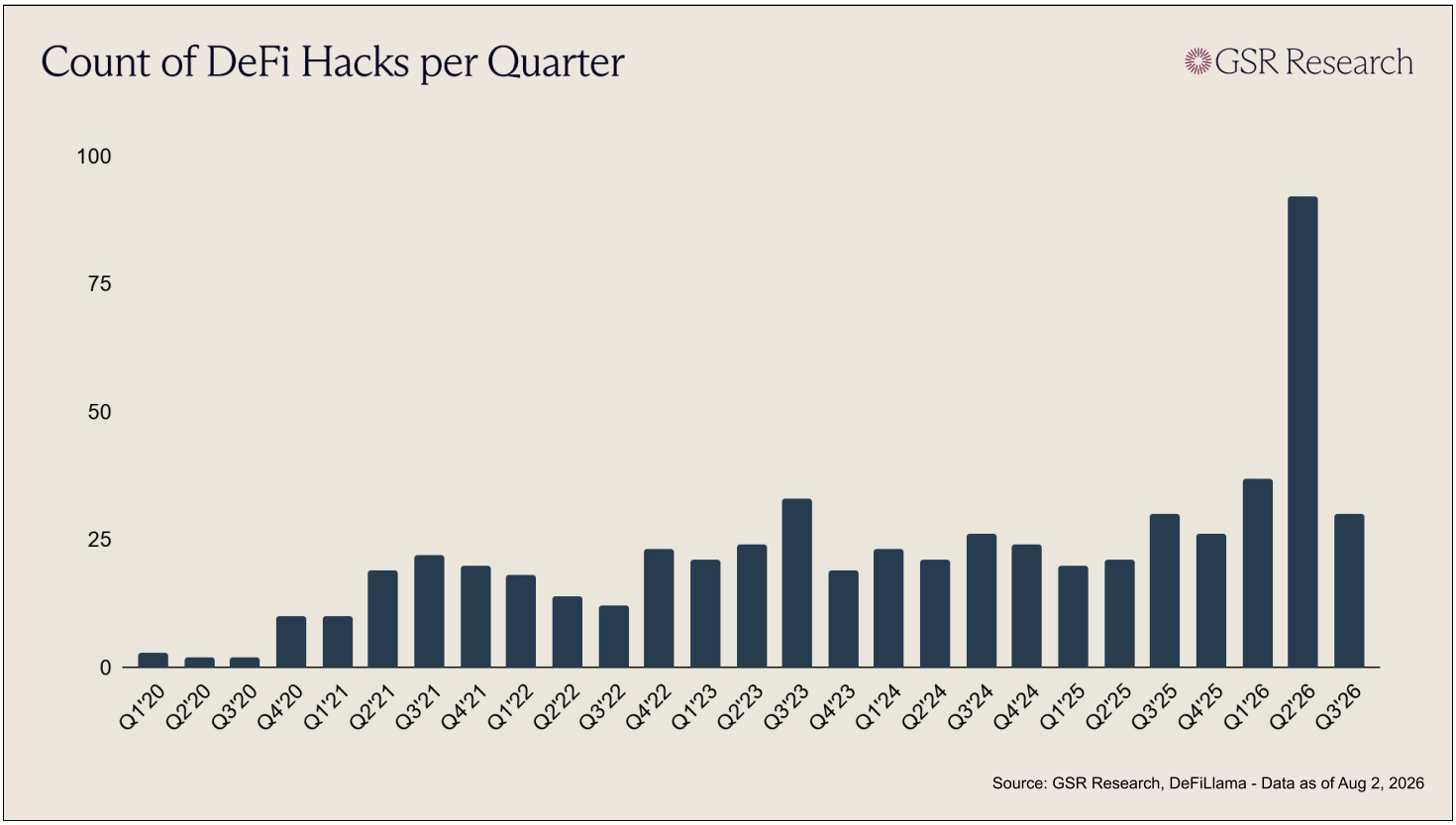
The Flip Side

While this approach to software development in crypto has significant potential to overhaul security, its promise exists alongside a reality that hacking in crypto is, if anything, accelerating thanks to rising AI capabilities. Last week also brought the Coldcard exploit, in which a firmware flaw from 2021 allowed attackers to reconstruct wallet seeds and drain upwards of $114 million in Bitcoin from thousands of wallets. The bug had been in open-source code for five years without being caught. While it hasn't been proven that AI was used to discover the flaw, it’s just the kind of attack that AI-powered code analysis facilitates, as codebases are now exposed to constant AI-assisted scrutiny.

The more capable models become at formal reasoning, the more capable they also become at finding weaknesses in code that hasn't been hardened against them.

The same AI capabilities that make formal verification newly practical are simultaneously lowering the cost of discovering exploitable flaws, and for the near term, most of the industry's code sits far closer to the Coldcard end of the spectrum than to Ironwood's, meaning offense will likely continue to outpace defense in aggregate. Exploit statistics are suggestive of this. Per DeFiLlama’s hack database, DeFi exploits reached a record of 92 in the second quarter of 2026, just as leading AI models achieved advanced cyber capabilities.

However, Ironwood shows the tools to shift that balance now exist and work in production. If AI continues to compress the cost of producing formally verified systems, the most critical pieces of crypto infrastructure, protocols managing billions in user funds, may increasingly be held to a standard that goes beyond hoping auditors catch every bug. Formal verification still has real limits, since it proves code matches a specification, and the specification itself can be wrong. But for the first time, building software that is provably secure against entire classes of bugs is looking like a practical near-term goal for the industry. Zcash just shipped a compelling early example of what that can look like.



1inch Aqua Targets DeFi's Idle Liquidity

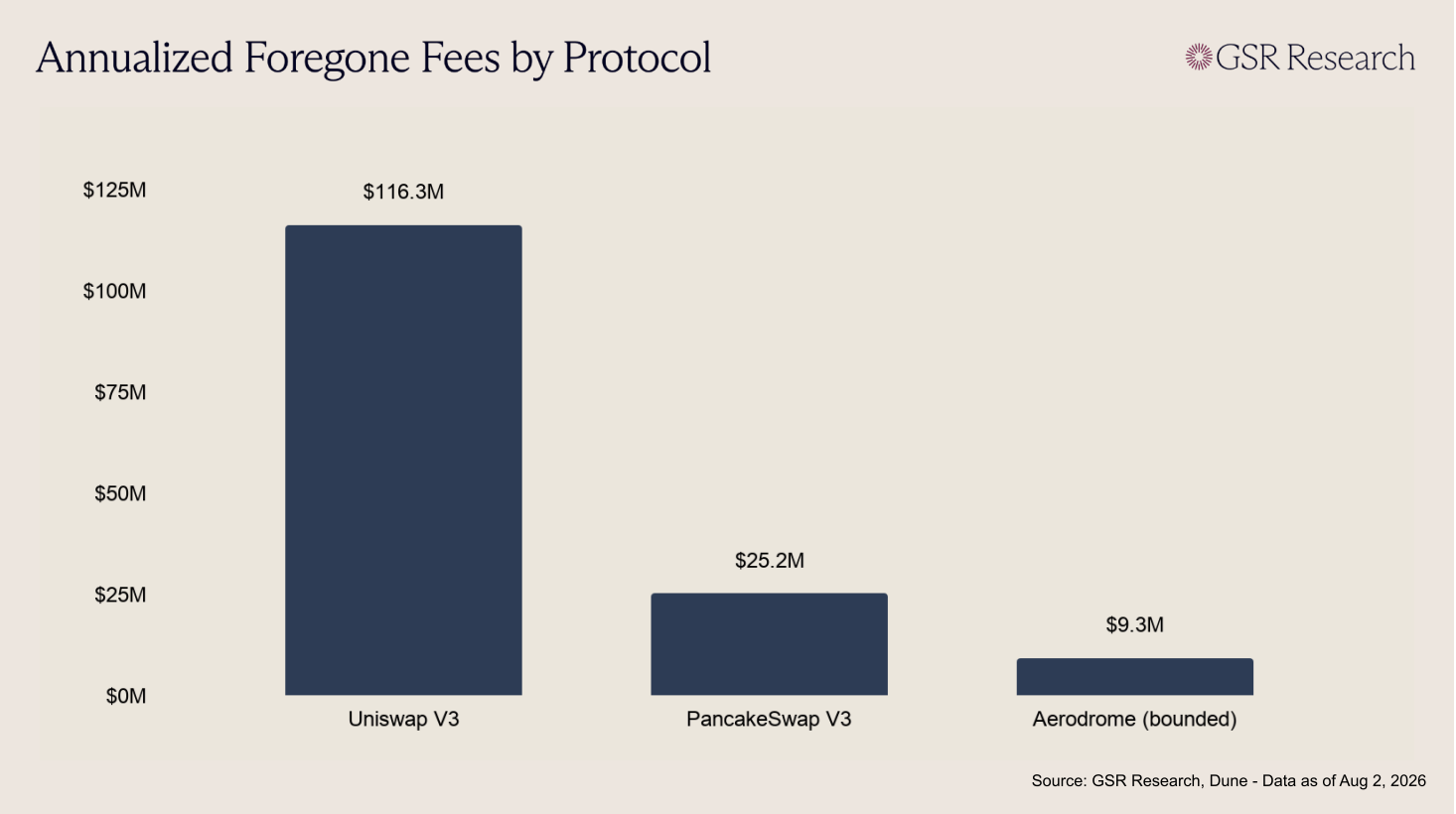
1inch opened Aqua to the public last week, taking its self-custodial shared liquidity layer live across 13 EVM chains 8 months after a developer-only release. The design is a direct challenge to the pooled deposit model that has defined onchain liquidity since Uniswap first popularized AMMs in 2018. Rather than locking tokens in a contract, a provider approves a wallet balance and lets that same balance stand behind multiple quotes at once, with tokens only moving out of the LP's wallet the moment a trade settles. 1inch is betting that the next edge in DeFi is utilization rather than deposits, and that the way to win liquidity is to stop asking for custody of it.

The Idle Majority

1inch commissioned Dune to measure the utilization of concentrated liquidity across majorprotocols, with the study rebuilding every liquidity position in roughly the top 200 pools across Uniswap v3 and v4, PancakeSwap v3, and Aerodrome, tracking about $1.84B of liquidity in an average week across 7 chains through the first half of the year. Roughly 85% of it, about $1.6B, was underutilized at any given moment. Within the v3 family, only 13.7% of capital was actively used, 56.9% sat in range but was never touched by the week's trades, and 29.4% was out of range entirely, with about $542M fully out of range in an average week. The foregone economics are meaningful, as out-of-range providers give up roughly $150M a year in fees measured against the 35 cents per dollar per year that in-range capital earned, with $116.3M of that on Uniswap, $25.2M on PancakeSwap, and a bounded $9.3M on Aerodrome. The $150M in foregone revenue is not a pot waiting to be collected, since fees come

from trading volume rather than parked capital, and moving every idle dollar into range would simply spread the same fee pot more thinly.

However, this study does measure what idle providers in aggregate gave up.



The idleness is also structural rather than transient. 36.7% of idle capital, roughly $200M, had gone untouched for more than 90 days, which was overwhelmingly a human problem rather than a bot problem, as individual wallets own 91% of Uniswap v3 capital on Ethereum and account for 94 cents of every idle dollar, while automated managers stay in range far more reliably. Larger positions go idle less often but hold most of the idle dollars, with positions above $1M accounting for roughly 47% of all idle capital. Newer architecture has not fixed it either, as Uniswap v4's out-of-range share is effectively identical to v3's. Ultimately, concentrated provision as currently designed asks humans to do a market maker's job without a market maker's tooling.

Quotes Without Deposits

Aqua replaces the pooled model with a registry. A provider approves a token allowance, set per token and per chain and revocable at any time, then creates positions by choosing a pair, a range, and a fee, while the tokens never leave the wallet. When a swap matches a position, the protocol pulls the required tokens and pushes back the proceeds plus fees in a single atomic transaction, and when nothing matches, the balance sits untouched and fully controlled.

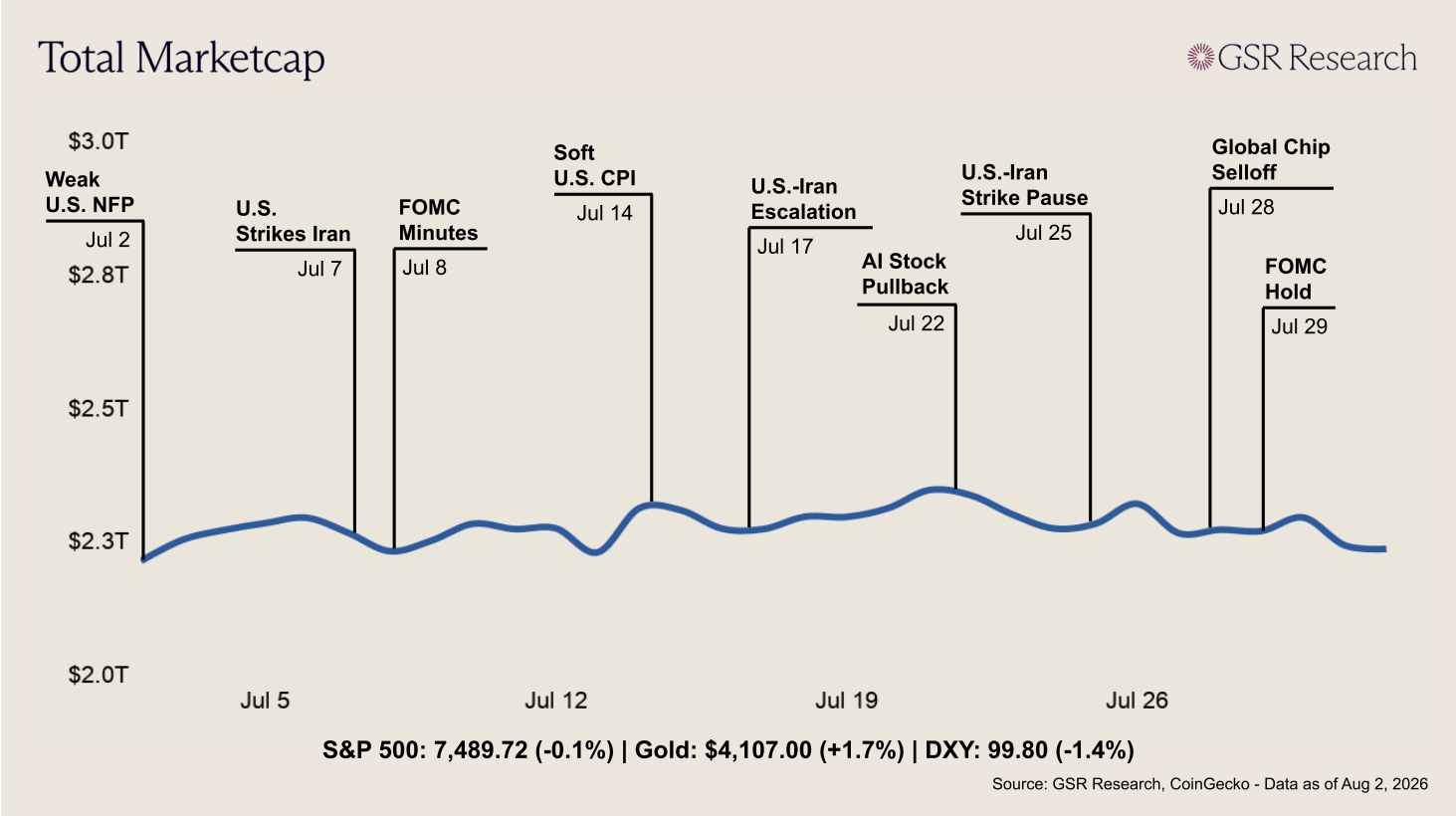
Closing a position moves no tokens because none were ever deposited. The headline efficiency claim is that one balance can back several positions at once, with 1inch's example being a $100k balance quoting $300k across 3 positions. Nothing is borrowed and exposure is capped by the wallet balance rather than the quoted size, so an underfunded position simply stops filling instead of being liquidated, resuming when topped up.

Two design choices define the product's character. Fills route exclusively through verified resolvers, the same vetted counterparties behind 1inch's Fusion auctions, which the team markets as risk-controlled liquidity. Because every position has a single owner, there is no shared fee moment for just-in-time bots to snipe, an attack that academic work estimates can erode passive LP profits by up to 44% per trade. The launch is paired with a Merkl-run incentive program worth roughly $1.37M over 3 months, with rewards paid on filled volume rather than parked capital.

The Overbooking Question

Aqua blurs the line between passive liquidity provision and market making, letting anyone run RFQ-style quoting from a wallet, which places it closer to the RFQ side of the RFQ vs CLOB debate than to the pools it is positioning itself as a better alternative to. A $100k balance quoting $300k is coordinated overbooking rather than multiplied liquidity, since only $100k of trades can ever settle at once, and the model pays off only if positions are rarely called simultaneously. That assumption may break down in key moments, for instance in a fast one-way move when correlated positions all draw on the same balance. The verified resolver requirement narrows who can fill and deepens dependence on 1inch's own routing, and the design includes no direct 1INCH value capture, no burn or revenue share, so token upside depends entirely on volume returning to the aggregator.

Macro Landscape



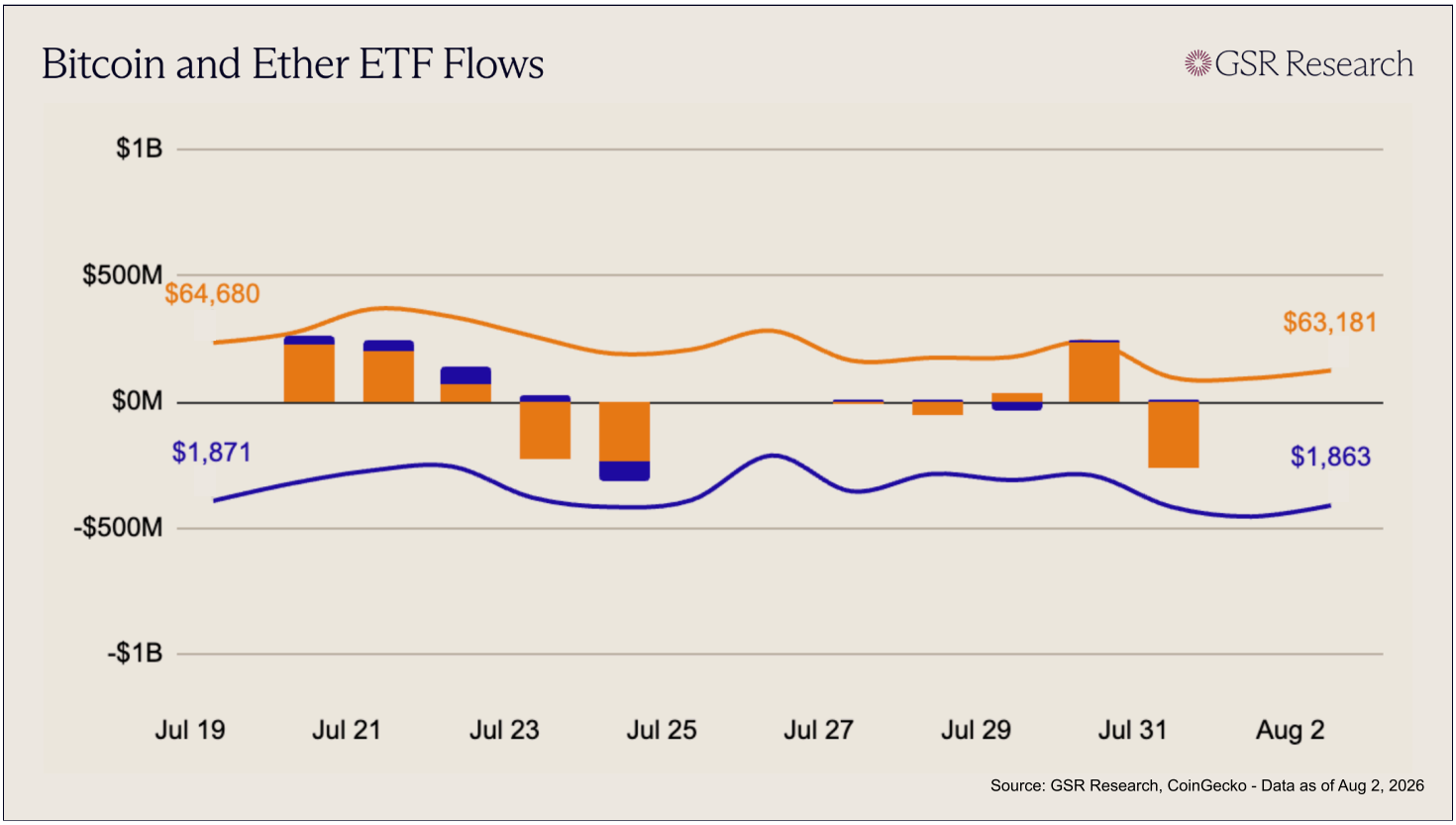
Crypto finished the week lower, with total market value falling from about $2.3 trillion to roughly $2.2 trillion. Bitcoin opened near $65,000, crashed below $62,500 during a historic rout in global chip stocks, recovered above $65,000 on strong tech earnings, then faded over the weekend to around $63,181 heading into Monday.

The week started with a brief window of calm as oil plunged Monday after the US and Iran paused strikes, with Brent falling nearly 9% to $88. Also on Monday, Chinese memory maker CXMT debuted on the Shanghai exchange with shares up over 400%, and reports surfaced that China had begun mass-producing its own chipmaking tools. South Korea's Kospi cratered 10.8%, triggering circuit breakers, with Samsung down over 13% and SK Hynix losing nearly 15%. The selloff swept through Asia and into US markets, and crypto sold off in lockstep, with Bitcoin falling to its weekly low near $62,400. Leopold Aschenbrenner's Situational Awareness, the high-profile AI hedge fund that had been up 439% through June on leveraged chip bets, lost 67% of its portfolio value over the course of July and was forced to sell its public book to Citadel. On Wednesday, Iran launched missiles at a US base in Jordan, sending Brent back up nearly 8% to $90.74.

Wednesday's FOMC meeting also had a major impact on markets. It was one of the hardest to call meetings in recent memory, with futures markets pricing a roughly one third chance of a surprise hike heading in. The committee voted 9-3 to hold rates, but three members voted for a hike, and Chair Warsh again refused to offer any forward guidance. In response, the 30-year Treasury yield hit 5.24%, its highest since 2007, and futures continued to price a September hike as the most likely outcome. Thursday's Q2 GDP print came in at 1.5% annualized, below the 1.8% consensus, while June core PCE landed at 3.3%, in line but still well above the Fed's target.

The mood in equities turned late in the week after Microsoft and Amazon both beat expectations and showed AI spending producing visible revenue. Microsoft added roughly $450 billion in market value on Thursday alone, and the S&P 500 eked out a roughly 1% weekly gain. Crypto failed to follow the equity rebound. Brent settled Friday at $90.12, capping a 24% July gain, its strongest month since March, and Bitcoin slid further over the weekend to around $63,181.

ETF Flows



Bitcoin ETFs finished the week modestly negative, with a choppy flow profile that swung between inflows and outflows. The week opened with two small red days, including -$12M on Jul 27 and -$50M on Jul 28, before flipping positive on Jul 29 (+$32M) and surging on Jul 30 (+$233M). That rebound was quickly reversed on Jul 31, when outflows of -$265M more than erased the prior day's strength. IBIT and FBTC did most of the heavy lifting on the positive days, while IBIT, FBTC, BITB, and GBTC were the main drags on the negative close. Across the five sessions, BTC ETFs saw about $62M of outflows, showing that demand was still active but not stable enough to sustain the midweek recovery.

Ether ETFs were a bit more constructive and ended the week slightly positive. The week started with two solid inflow sessions on Jul 27 and Jul 28, adding +$12M and +$9M, respectively. A setback followed on Jul 29, when ETH ETFs saw -$33M of outflows, but flows recovered again on Jul 30 (+$13M) and Jul 31 (+$9M). ETHA was the main source of support across the week, while FETH and ETHE were the largest sources of weakness on the down day. Overall, ETH ETFs gained roughly $10M for the week, which is modest, but it still points to steadier demand than BTC and a flow profile that held up better through the late-week volatility.

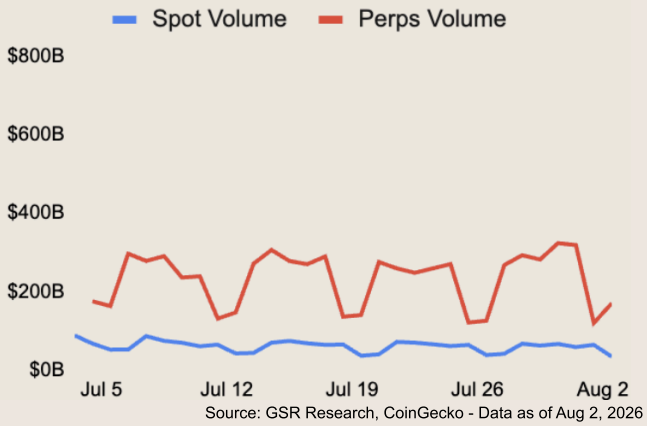
Sector Performance

Sector Performance, Top Gainers, Losers, & Volume

GSR Research

Sector	24h	7d	30d	200d	1y
Social	1%	10%	21%	-17%	-6%
Gaming	-9%	-1%	9%	290%	-41%
RWA	1%	-2%	-2%	-24%	-33%
CEX	0%	-2%	-2%	-21%	-1%
L1	1%	-2%	-4%	-25%	19%
Privacy	0%	-2%	7%	-16%	676%
AI	1%	-2%	4%	1%	-21%
L2	0%	-2%	-2%	-42%	-13%
Meme	1%	-3%	-4%	-43%	-39%
DePIN	0%	-3%	-12%	-37%	-49%
NFT	-6%	-3%	1%	173%	-52%
Infra	1%	-4%	1%	-24%	-44%
DeFi	1%	-5%	-7%	20%	-6%
DEX	0%	-5%	-11%	42%	6%
Perps	0%	-9%	-21%	67%	23%

Top Gainers (7D)		Top Losers (7D)	
PUMP	17.39%	STABLE	-16.94%
ADA	15.31%	VVV	-16.58%
UNI	8.70%	HYPE	-11.04%
JUP	4.95%	RAIN	-10.01%
ENA	4.84%	币安人生	-9.78%



Source: GSR Research, CoinGecko - Data as of Aug 2, 2026

Social was the lone sector in the green this week, up 10%, with the rest of the board flat to down. PUMP (+17.39%) topped the gainers for a second straight week as platform revenue climbed 30% week over week to $7.56m, eclipsing Hyperliquid's, and the team bought back and burned $3.73m of the token, with the buyback demand absorbing a large scheduled unlock. ADA (+15.31%) rebounded from multi-year lows as attention turned to the network's Dijkstra scaling era following July's Van Rossem upgrade. UNI (+8.70%) touched a 6-month high after governance approved extending protocol fees to v4 pools and Robinhood Chain with 97% support, directing revenue toward buying and burning UNI, and JUP (+4.95%) and ENA (+4.84%) rounded out the board as the value-accrual bid extended to other fee-generating names.

The rest of the board was red, with Perps (-9%), DeFi (-5%), and DEX (-5%) the biggest laggards. Perps and DEX weakness ran through HYPE (-11.04%), which broke below support as Multicoin and Paradigm completed a $291m unstake, wallets tied to Multicoin, Selini, and Bitwise moved tokens to exchanges, and the market braced for the August 6 unlock to core contributors. DeFi's decline was led by RAIN (-10.01%), with the prediction markets infrastructure token still carrying a heavy locked-supply overhang. STABLE (-16.94%) led the losers, and VVV (-16.58%) reversed after two weeks atop the gainer board. Gaming finished down 1%, sliding 9% in the final session as BEAT crashed roughly 24%, while 币安人生 (-9.78%) rounded out the losers as the $575m BNB Chain memecoin cooled.

The Week Ahead: What to Watch

Monday, Aug 3	China Caixin Manufacturing PMI Data U.S. ISM Manufacturing PMI Data
Wednesday, Aug 5	U.S. ADP Employment Report U.S. ISM Services PMI Data Circle Q2 Earnings
Thursday, Aug 6	U.S. Initial Jobless Claims
Friday, Aug 7	U.S. Non-Farm Payrolls & Unemployment Rate Data

Other Stories

Morgan Stanley debuts Ether and Solana ETPs with staking and the market's lowest fee *The Block*

Tillis and Gallego send new ethics compromise to the White House in Clarity Act push *The Block*

Binance US plans to offer prediction markets to its customers *X @Eleanor Terrett*

Strategy sells another 1,638 BTC for $105 million *The Block*

South Korea's Bithumb officially targets 2028 IPO, outlines multi-year roadmap *The Block*

Tether posts strong Q2 performance, generates $1.5B net operating profit *Tether*

Uniswap launches Earn with Morpho to pay yield on idle assets *The Block*

SEC is ready to write crypto market rules if Clarity fails, Atkins says *Decrypt*

This material is provided by GSR (the "Firm") solely for informational purposes. It is not intended to be advice or a recommendation to buy, sell or hold any investment mentioned. Investors should form their own views in relation to any proposed investment. It is intended only for sophisticated, institutional investors and does not constitute an offer or commitment, a solicitation of an offer or commitment, or any advice or recommendation, to enter into or conclude any transaction (whether on the terms shown or otherwise), or to provide investment services in any state or country where such an offer or solicitation or provision would be illegal.

The Firm is not and does not act as an advisor or fiduciary in providing this material. This material is not an independent research report, and has not been prepared in accordance with any legal requirements by any regulator (including the FCA, FINRA or CFTC) designed to promote the independence of investment research. This material is not independent of the Firm's proprietary interests, which may conflict with the interests of any counterparty of the Firm. The Firm may trade investments discussed in this material for its own account, may trade contrary to the views expressed in this material, and may have positions in other related instruments. The Firm is not subject to any prohibition on dealing ahead of the dissemination of this material.

Information contained herein is based on sources considered to be reliable, but is not guaranteed to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made by the author(s) as of the date of publication, and are subject to change without notice. The Firm does not plan to update this information.

Trading and investing in digital assets involves significant risks including price volatility and illiquidity and may not be suitable for all investors. The Firm is not liable whatsoever for any direct or consequential loss arising from the use of this material. Copyright of this material belongs to GSR. Neither this material nor any copy thereof may be taken, reproduced or redistributed, directly or indirectly, without prior written permission of GSR.

Please see gsr.io/regulatory-legal-notices for additional Regulatory Legal Notices relevant to US, UK and Singapore.