GSR Research

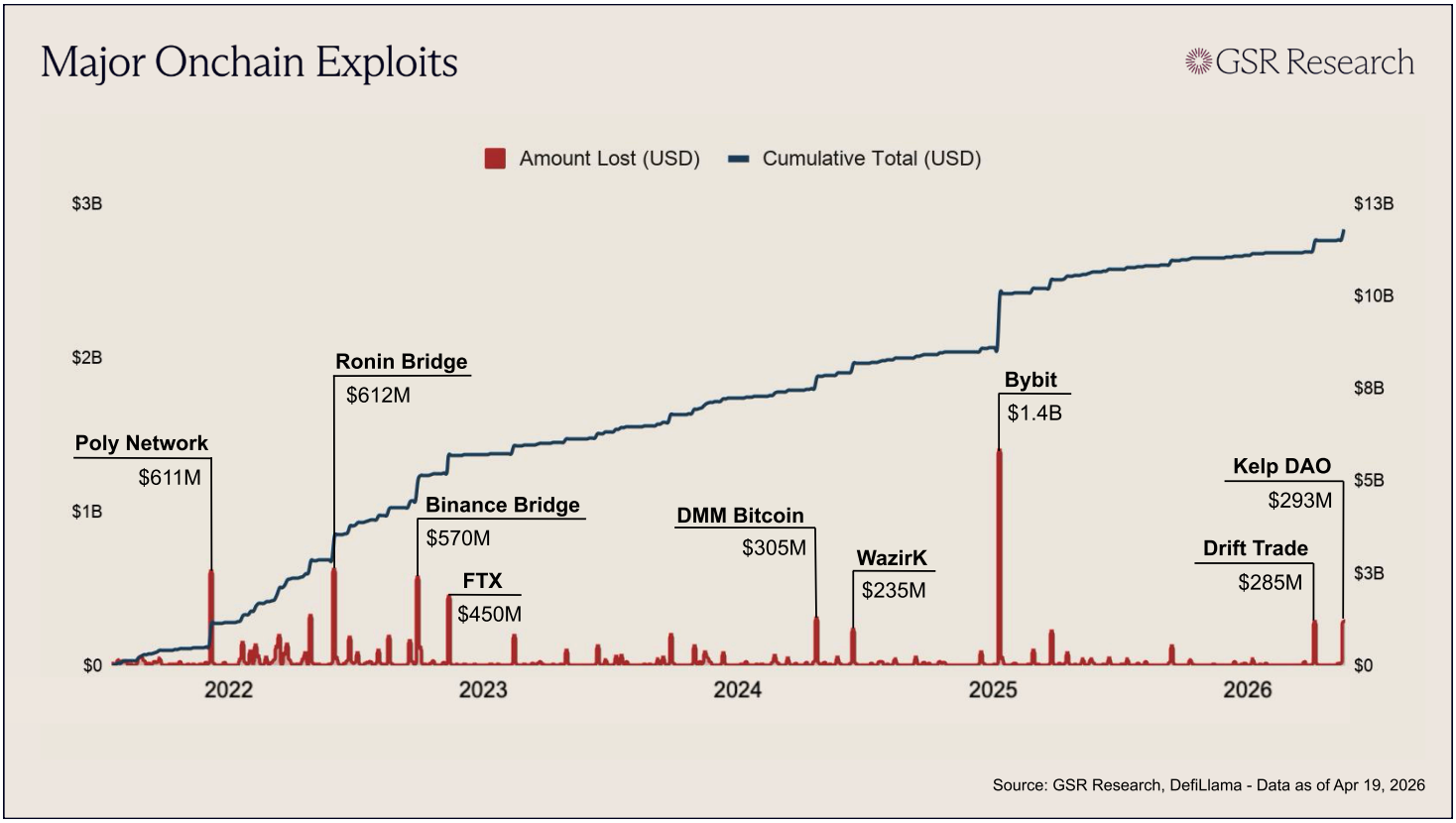
Weekly Update

April 20th, 2026

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

Highlights

Exploits Plague DeFi



Over the past 60 days, more than $600M has been stolen from onchain depositors. On April 1st, Drift, Solana's largest perpetual futures exchange, was drained for $285M in what was expected to be the year's largest exploit. Just 17 days later, Kelp DAO was hacked for over $293M, eclipsing it. The losses come as DeFi yields have compressed toward TradFi rates, raising the question of whether depositing onchain is still worth the risk.

Moving Up The Stack

While the scale of the exploits is astonishing, the nature of the attacks is even more concerning. Until very recently, the archetypal crypto exploit consisted of reentrancy bugs, oracle manipulation, or flawed smart contract code. Recent exploits diverge from this. The $1.4B Bybit exploit in February 2026 used a compromised Safe UI to trick signers into approving malicious transactions. Drift's attackers spent 6 months posing as a quant

trading firm in person before using Solana's durable nonces to get Security Council members to unwittingly pre-sign transactions that handed over admin control. Meanwhile, Kelp lost $293M to an RPC-poisoning attack on a LayerZero verifier rather than any bug in its smart contracts. All three attacks have been attributed to North Korea's Lazarus Group, and point to a growing trend: as smart contract code grows more robust, attackers have migrated their exploit stack. Instead of targeting protocol code, recent exploits target operational security, signing infrastructure, developer tooling, and the humans behind them.

AI Accelerant

The shift from simple smart contract bugs to compromising entire operational layers is exactly what makes the trajectory of frontier AI so concerning. Anthropic's Mythos, previewed this month, reportedly found zero-day vulnerabilities in 83% of major operating systems and browsers during internal testing, alarming enough that the lab withheld broad release. There is no public evidence that Mythos or any comparable model was used in Drift, Kelp, or other recent hacks, but shifting the economics of attack does not require Mythos-level capability. Commodity LLMs can already draft convincing spear-phishing at scale, impersonate maintainers in developer channels, and map a protocol's attack surface faster than any human auditor.

This weekend's Vercel compromise, which briefly exposed deployment infrastructure across much of the web, is exactly the kind of incident that becomes cheaper as capability scales. AI tooling may already be contributing to the recent uptick in operational compromises, even if attribution remains elusive.

AI's offensive capabilities outstrip its defensive responses. EVMbench, published by OpenAI and Paradigm in February 2026, makes the asymmetry explicit: today's frontier models score higher in exploiting vulnerabilities than they do when patching them. In the near term, this almost certainly means more, larger hacks, as operational surfaces are probed more systematically. The longer-term picture, however, is more hopeful. The same capabilities that render exploitation more efficient also make continuous auditing, automated patching, and formal verification dramatically more tractable. As reasoning models close the exploit-remediation gap, the defender's structural advantages compound, including time to harden systems, monitoring at scale, and cryptographic guarantees that attackers cannot break. Software is a rare domain where the asymptote of security is full formal verification, and onchain infrastructure is better positioned than most to reach it. With AI-assisted auditing, continuous monitoring, and better tooling around formal verification, the security properties that blockchains already offer can be reinforced and extended over time.

Tempo Launches Zones

On Thursday, Tempo announced Zones, a privacy framework for its stablecoin-focused L1. A Zone is a private execution environment that runs in parallel to Tempo mainnet, allowing participants to transact invisibly to outside observers while still settling on the main chain. The release is Tempo's first major protocol extension since its mainnet launch in September, and reflects a thesis the team has developed through enterprise conversations: stablecoins are ready to carry real commercial flows like payroll, treasury operations, and merchant settlement, but only if those flows can be kept off a public ledger. Zones aim to deliver that privacy without the cryptographic machinery that has historically made onchain privacy slow, expensive, or awkward to use.

Bank-Grade Privacy

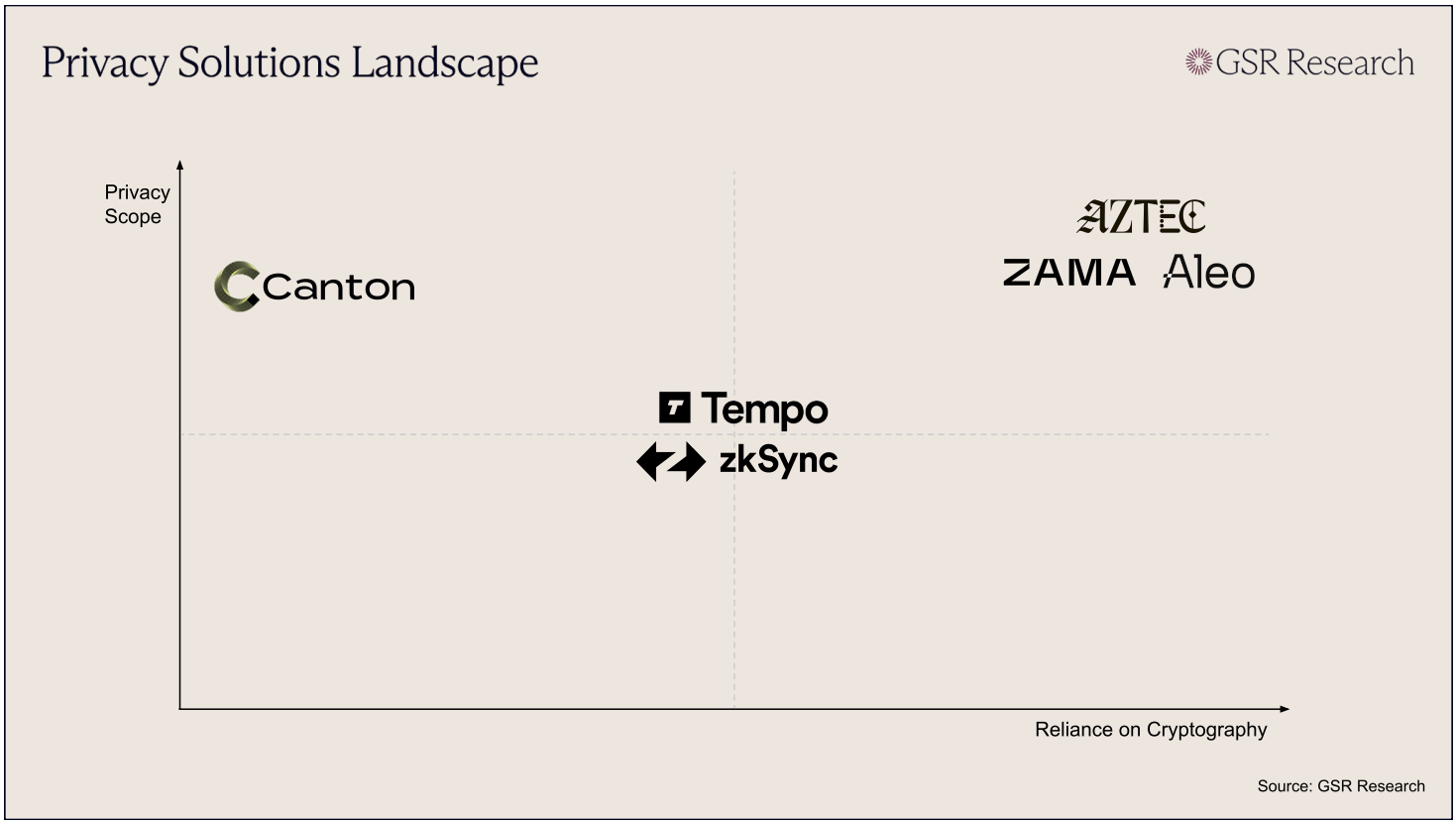
Each Zone is essentially a validium tailored for stablecoin payments. Zones operate as EVM-compatible chains, with their own sequencers. Like other layer-2 scaling solutions, Zones commit batches back to mainnet via validity proofs produced either inside a ZKVM (SP1) or a trusted execution environment like Intel SGX or TDX. Funds deposited into a Zone are locked in a portal contract on mainnet and can only be withdrawn by the account that owns them; Zone sequencers may order transactions, but do not have the authority to move user assets. Interoperability flows through mainnet, so a user can withdraw from one Zone, swap on Tempo's native stablecoin DEX, and redeposit into another in a single operation.

The resulting privacy model more closely resembles a bank or fintech app than a privacy chain. Inside a Zone, operators see every balance and every transaction, while users see only their own activity. Outside observers see nothing beyond deposit and withdrawal events on mainnet, and proofs attesting to execution validity. A company running payroll on a Zone could track exact employee payments, and employees could see their own balances. Yet, no indexer or block explorer would be able to reconstruct these salary schedules. As in TradFi banking and fintech, with Zones, employers and banks can see transaction details, while the public cannot.

Pragmatic Tradeoffs

Since Zones only post state commitments and proofs to mainnet rather than full transaction data, they do not give users the unilateral exit guarantees of a data-available rollup. A malicious or unresponsive operator could in principle censor withdrawals by refusing to sequence them, though it cannot steal the underlying funds. In exchange, users get high throughput, standard wallets, and a compliance surface that regulated institutions can actually work with.

Zones' closest analog is ZKsync's Prividium, which is similar to a permissioned validium via its validity proofs and an operator-visible execution environment. Solutions like Aztec and Aleo lean harder on cryptography, using client-side zero-knowledge proving to hide activity from everyone including the sequencer, but require specialized wallets, non-EVM virtual machines, and

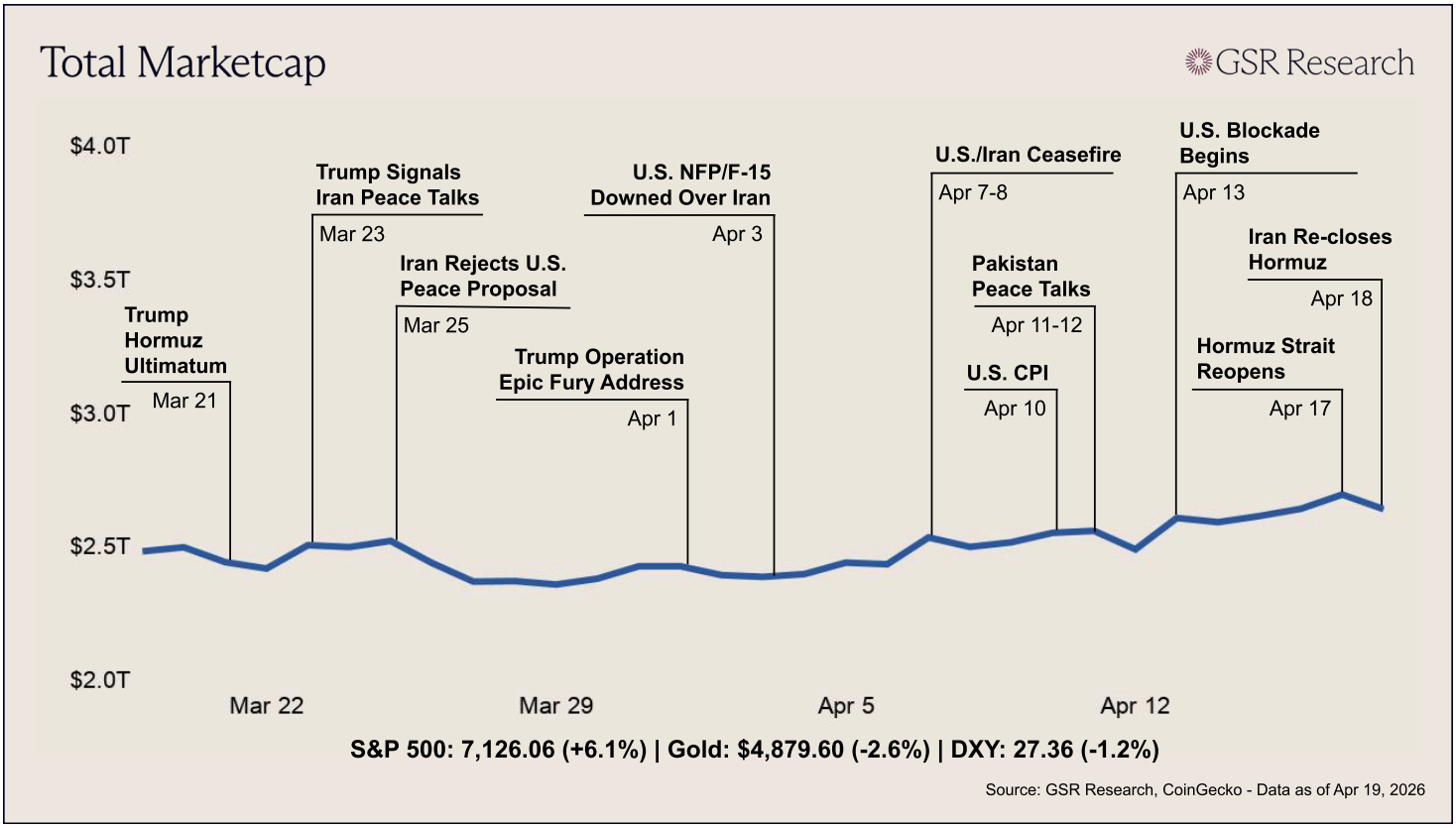


meaningful per-transaction proving time. FHE-based chains like Zama, Inco, and Fhenix push in a similar direction by computing directly on encrypted data, at the cost of throughput overhead. Canton goes the opposite way, skipping general-purpose proofs of execution in favor of a design where participants only ever see their own slice of the ledger, with correctness resting on counterparties and token issuers executing honestly. Tempo Zones tread the middle ground, giving up some privacy against operators to maintain cryptographic correctness without heavy user-side computation or prior trust between counterparties.

Zones fit the pragmatic philosophy Tempo has applied throughout its stack. The chain ships without a native token, lets users pay gas in the stablecoin they are sending, embeds issuer compliance controls directly into the token standard, and now extends privacy via a model that maps onto existing enterprise expectations. Whether these tradeoffs make sense for applications that require full privacy with respect to an operator is a separate question, and one Zones are not currently trying to answer.

Market Update

Macro Landscape



Crypto markets rallied for most of the week as a soft inflation print and Friday's reopening of the Strait of Hormuz overshadowed a new U.S. naval blockade of Iranian ports, though a portion of those gains pared back over the weekend. The total crypto market cap opened near $2.49T with BTC around $70,900 as the blockade took effect at 10 a.m. ET Monday, following the weekend collapse of the Islamabad talks. Sentiment turned decisively on Tuesday after March PPI came in at 0.5% month-over-month versus a 1.1% consensus, with core PPI at just 0.1% against 0.4% expected. The reading suggested the energy shock had not yet bled into broader wholesale prices. WTI fell nearly 8% to $91.28, the S&P 500 climbed 1.18% to 6,967, and BTC pushed to nearly $76,000, its highest level since the February 5 crash.

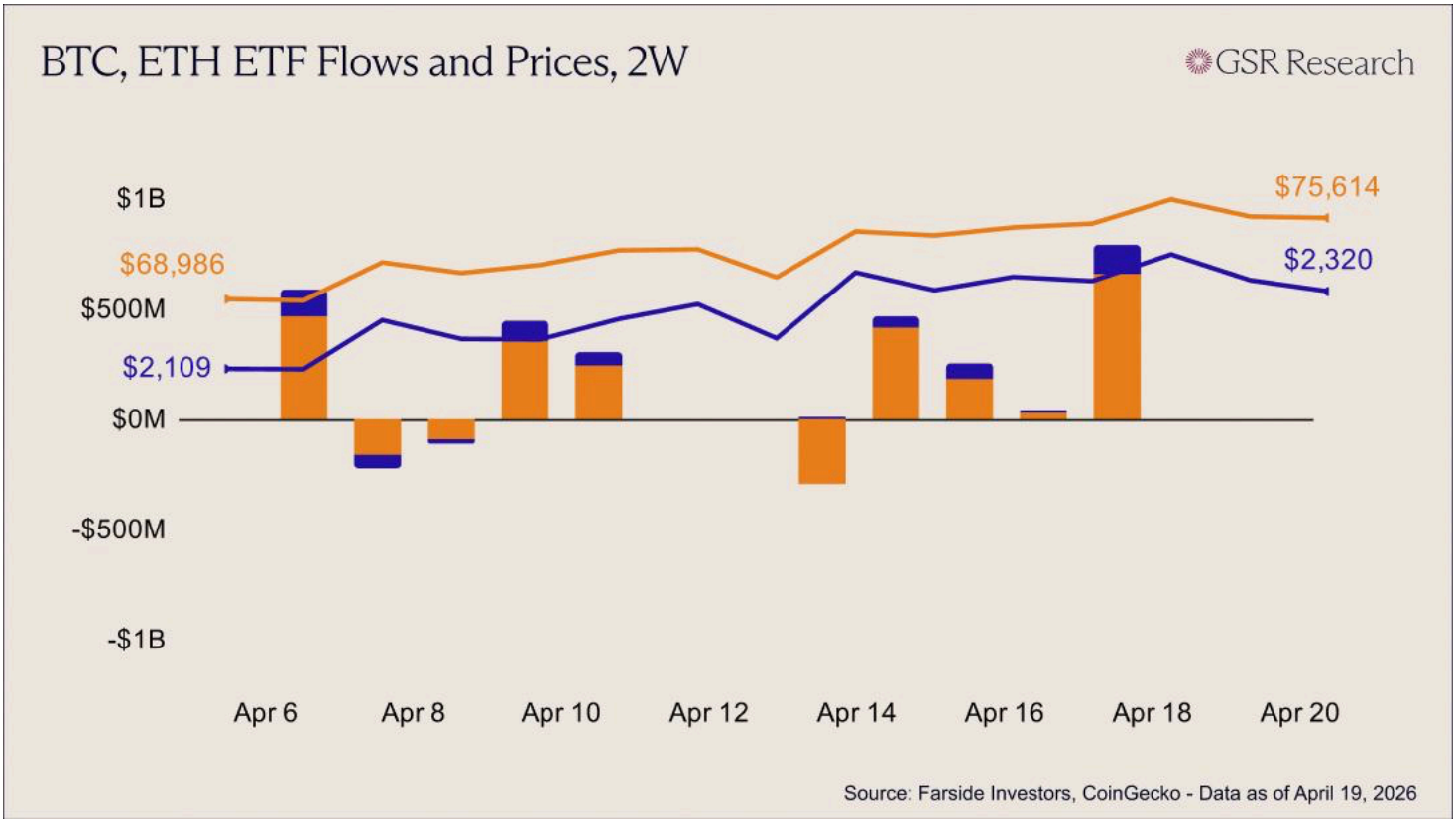
The rally gathered momentum into the back half of the week. On Thursday, jobless claims fell to 207K, China posted a 5.0% Q1 GDP print that beat consensus, and a U.S.-brokered 10-day Israel-Lebanon ceasefire took effect at 5 p.m. ET. The decisive catalyst arrived Friday, when Iranian Foreign Minister Araghchi declared the Strait of Hormuz fully open to commercial traffic for the duration of the Lebanon truce. Brent crude plunged 11% to below $89, the S&P 500 closed at a fresh record 7,126, marking its best week since May 2025, and the Nasdaq notched its 13th consecutive winning session, its longest streak since 1992.

BTC broke through $78,000 to an intraday high of $78,348, its highest level since before the war began in late February, triggering over $800M in short liquidations.

The rally began to reverse over the weekend. Iran's IRGC declared Saturday that control of the Strait had returned to its "previous state" in response to the continued U.S. port blockade, with Iranian gunboats firing on two Indian-flagged tankers attempting to transit.

Conditions deteriorated further Sunday as the USS Spruance seized the Iranian cargo ship Touska in the Gulf of Oman, prompting Trump to threaten to knock out every power plant and bridge in Iran absent a deal. Focus now turns to whether Pakistan can broker another round of talks before the April 22 expiry of the original ceasefire, and to the April 28-29 FOMC meeting, where the soft PPI has largely removed hike risk without giving the Fed much new room to accelerate cuts.

ETF Flows



ETF flows this week marked a decisive return of institutional demand after the prior period's choppiness, with both BTC and ETH seeing sustained creations into the back half of the week. U.S. spot Bitcoin ETFs began the period on uneven footing, with a sharp outflow on Apr 13 (-$291M), which proved to be a brief reset rather than a trend reversal. Flows rebounded aggressively on Apr 14 (+$411M) and remained firmly positive through the rest of the week (+$186M, +$26M, and a standout +$663M on Apr 17), driving a strong net positive outcome.

Ether ETFs followed with a cleaner and more consistent recovery profile. After modest flows earlier in the period, ETH saw uninterrupted inflows from Apr 13 onward, building steadily each session (+$10M, +$53M, +$68M, +$18M) before accelerating into a strong close (+$127M on Apr 17). Unlike prior weeks where ETH flows have been more fragile and easily reversed, the recent stretch shows a narrowing of the relative weakness versus BTC.

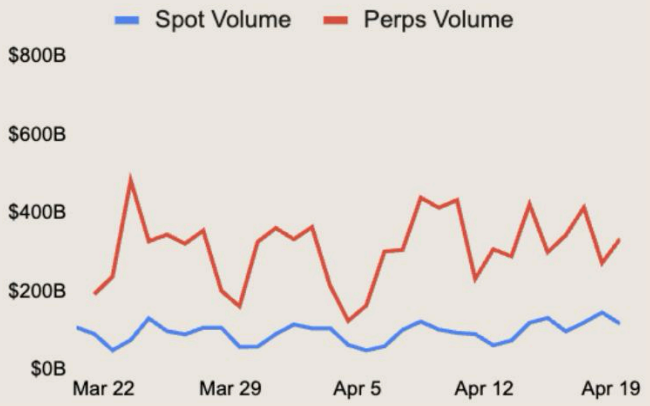
Bitcoin rallied from $70.8k on Apr 12 to a peak near $77.1k on Apr 17 before consolidating slightly around $75.6k into Apr 19, marking a strong breakout from the prior range. Ether followed with an even sharper move, climbing from $2,192 to $2,421 at the highs before settling near $2,320.

Sector Performance, Top Gainers, Losers, & Volume

GSR Research

Sector	24h	7d	30d	200d	1y
Meme	-3%	12%	14%	-21%	3%
Gaming	-1%	10%	10%	-50%	-52%
NFT	0%	6%	6%	-54%	-49%
Infra	-2%	5%	2%	-47%	-29%
L2	-2%	5%	-2%	-66%	-38%
DeFi	-3%	5%	4%	-26%	22%
AI	0%	4%	1%	-37%	-19%
L1	-1%	4%	3%	-32%	12%
DEX	-4%	3%	2%	-33%	56%
CEX	-1%	3%	-2%	-12%	41%
RWA	-1%	3%	3%	-22%	-7%
Social	-3%	2%	0%	-62%	137%
Perps	-5%	2%	7%	-23%	87%
DePIN	-1%	1%	-3%	-41%	-34%
Privacy	-2%	-6%	14%	73%	403%

Top Gainers (7D)		Top Losers (7D)	
DEXE	58.75%	ZEC	-16.72%
ENA	25.77%	TON	-11.76%
M	20.56%	WLD	-10.66%
MORPHO	15.84%	JST	-9.34%
APT	12.97%	RENDER	-7.36%



Source: GSR Research, CoinGecko - Data as of Apr 19, 2026

With the majors trading upwards on positive geopolitical news the altcoin sector rallied again. The categories with the highest returns on the week were Memes (+12%), Gaming (+10%), and NFTs (+6%), a combination likely not seen since 2021. Ethena rallied 25% despite the increase in DeFi exploits and the broader market conditions of compressed yields. The yield-bearing stablecoin protocol has recently shifted its reserve strategy toward more diversified and conservative backing, a move the market has interpreted as a step toward less reflexive yield generation.

The privacy sector is the only category down on the week due to a 17% loss in Zcash. The L1 continues to be one of the most volatile assets in the top 100, as it has featured in either the top gainers or losers in nearly every one of our sector performance updates since February.

The Week Ahead: What to Watch

Tues, Apr 21	Kevin Warsh Fed Chair Confirmation Hearing U.S. Retail Sales (March)
Wednesday, Apr 22	Scheduled Expiry of U.S.-Iran Ceasefire Tesla (TSLA) Q1 2026 Earnings
Thursday, Apr 23	S&P Global Flash PMIs (U.S., Eurozone, U.K., Japan) U.S. Initial Jobless Claims
Friday, Apr 24	Michigan Consumer Sentiment Index (April)

Other Stories

SEC exempts certain crypto UI providers from broker-dealer registration *The Block*

Kraken parent company agrees to acquire Bitnomial for up to $550M *CoinDesk*

Deutsche Borse invests $200M in Kraken parent Payward *The Block*

Polymarket looks to raise $400M at a $15B valuation *The Block*

Charles Schwab begins rollout of crypto trading platform *The Block*

UK FCA publishes cryptoasset perimeter guidance *Decrypt*

Drift secures up to $128M from Tether for user recovery after exploit *Fortune*

Aave DAO passes proposal routing 100% of product revenue to token holders *Unchained*