

BYBIT + glassnode

Digital Asset Market Resilience

A Deep Dive into
the Bybit-Lazarus Hack

2025

Table of Contents

Overview	03	Liquidity Conditions Improve	
Traditional Financial Disruption Events	04	Perpetual Bid-Ask Spread	17
Digital Asset Financial Disruption Events	05	Perpetual Market Depth	19
Bybit-Lazarus Hack	06		
		Exchange Risk Diagnostics	
Case Study: Bybit-Lazarus Hack		Evaluating Bybit's Operational Stability Post-Hack	20
Replenishment of Stolen Assets	08	Whale Withdrawal Ratio	22
		Conclusion	23
Open Interest Recovery			
Perpetual Open Interest [Ethereum]	09		
Perpetual Open Interest [Bitcoin and Solana]	10		
Perpetual Open Interest Percent Change [Ethereum]	11		
Perpetual Open Interest Percent Change [Bitcoin and Solana]	12		
Bybit Open Interest Dominance	13		
Perpetual Volumes Remain Robust			
Perpetual Volume [Ethereum]	14		
Perpetual Volume [Bitcoin and Solana]	15		
Perpetual Volume Dominance	16		

Overview

This report examines the evolving resilience of digital asset markets in the face of major disruption. While financial shocks are not unique to digital assets, traditional markets have seen everything from rogue trading and hacks to flash crashes and global financial crises, the digital asset space is increasingly demonstrating an ability to absorb shocks without triggering systemic fallout.

To ground this exploration, we begin by briefly surveying key disruption events in both traditional finance and the digital asset industry. This context helps frame the report’s central focus: a deep dive into the February 2025 Bybit-Lazarus hack, in which \$1.4B in ETH was stolen from one of the world’s largest exchanges.

Unlike past crises that cascaded through the digital assets ecosystem, the Bybit incident did not produce widespread contagion. Instead, the exchange recovered operations and restored reserves without destabilizing markets, offering a real-time stress test of industry maturity.

By analyzing market conditions before and after the hack through metrics such as trading volumes, open interest, liquidity depth, and internal asset flows, the report assesses the current state of digital asset infrastructure and highlights the mechanisms that can contain disruption in an increasingly interconnected system.

Bybit

Bybit is the world’s second-largest cryptocurrency exchange by trading volume, serving a global community of over 70 million users. Founded in 2018, Bybit is redefining openness in the decentralized world by creating a simpler, open, and equal ecosystem for everyone. With a strong focus on Web3, Bybit partners strategically with leading blockchain protocols to provide robust infrastructure and drive on-chain innovation.


Renowned for its secure custody, diverse marketplaces, intuitive user experience, and advanced blockchain tools, Bybit bridges the gap between TradFi and DeFi, empowering builders, creators, and enthusiasts to unlock the full potential of Web3. Discover the future of decentralized finance at Bybit.com.

Glassnode


Glassnode is the leading market intelligence provider in the digital asset space, primarily focused on institutions. Glassnode's platform delivers unparalleled on-chain analytics, deep insights into BTC, ETH, and selected major digital assets.

Founded in 2017, [Glassnode](https://Glassnode.com) equips institutional investors, hedge funds, banks, and asset managers with near real-time, data-driven intelligence, enabling informed decision-making in a highly dynamic trading environment.

Authors



@UkuriaOC
Glassnode Analyst



@CryptoVizArt
Glassnode Analyst

Traditional Financial Disruption Events

Over the past few decades, financial markets and institutions have faced a range of rare but disruptive shocks, from rogue traders and Ponzi schemes to cyberattacks and global crises. These black swan events, though varied in nature, share a common trait: they exposed deep vulnerabilities in the financial system and reshaped industry practices.

Barings Bank Collapse (February 1995)

A rogue trader, Nick Leeson, accumulated unauthorized losses of \$1.3 billion, wiping out Barings, the U.K.’s oldest merchant bank. The collapse exposed deep failures in internal oversight and risk management.

Dot-Com Bubble Burst (2000–2002)

Fueled by tech euphoria, the Nasdaq plunged nearly 78%, wiping out over \$5 trillion in market value. Hundreds of internet startups collapsed, and the crash triggered a mild recession while resetting investor expectations for growth stocks.

Global Financial Crisis (2008)

A collapse in subprime mortgage markets triggered a \$16 trillion wipeout in global equity. Major institutions failed and governments deployed historic bailouts to prevent total financial collapse.

Flash Crash (May 2010)

U.S. markets plunged nearly 9% in minutes, erasing \$1 trillion in value before rebounding just as fast. Triggered by high-frequency trading feedback loops, the event led to new circuit breaker rules to limit sudden volatility.

Nasdaq Hack (October 2010)

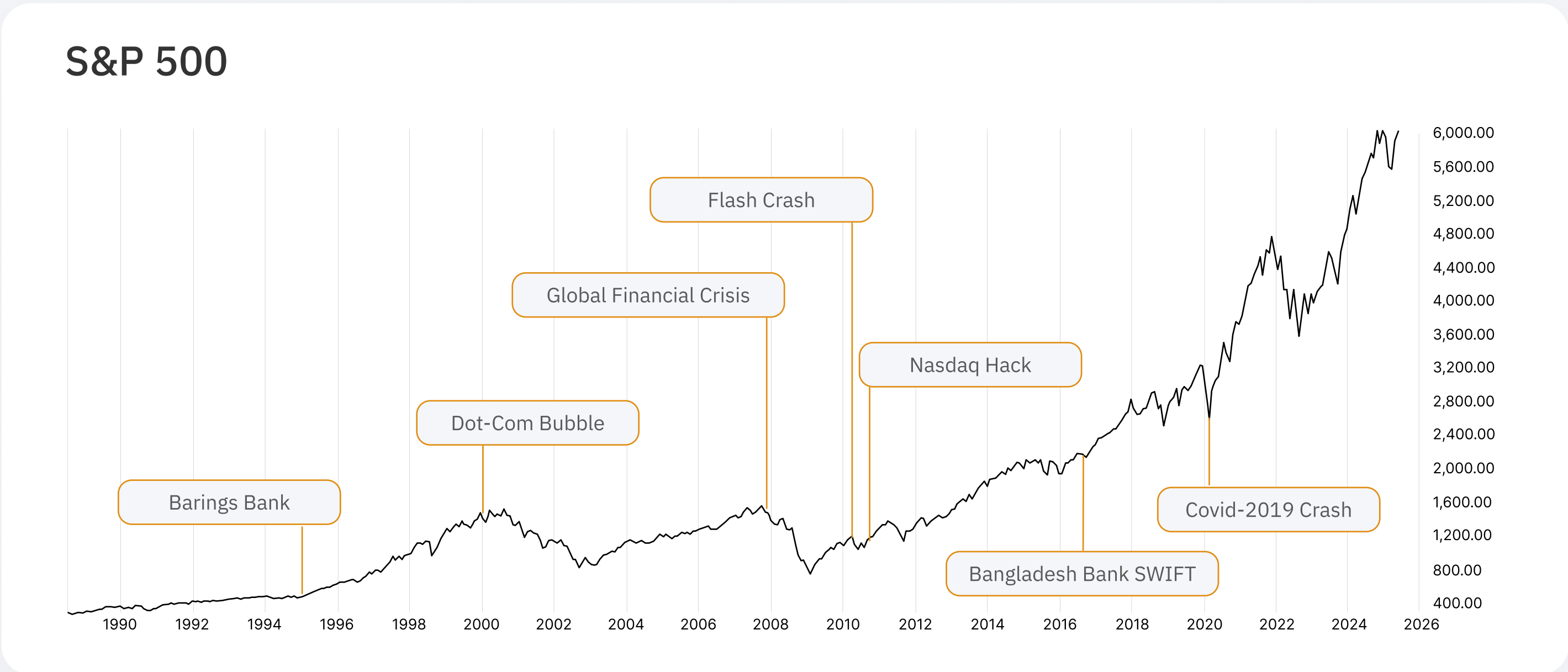
Hackers linked to Russian intelligence breached Nasdaq's internal systems, installing malware capable of disrupting U.S. markets. Though no financial damage occurred, the incident exposed major cybersecurity gaps across global financial infrastructure.

Bangladesh Bank SWIFT Heist (February 2016)

Cybercriminals used SWIFT credentials to steal \$81 million from Bangladesh’s central bank, part of an attempted \$1 billion fraud. The heist revealed glaring weaknesses in global interbank security protocols.

COVID-19 Crash (Feb–Mar 2020)

Global markets fell ~34% in just 33 days amid pandemic panic, marking one of the fastest crashes ever. Trillions were erased from equity markets before emergency stimulus and rate cuts stabilized conditions.



Digital Asset Financial Disruption Events

Similar to the stock market, the cryptocurrency market has also witnessed several black swan events, rare and sudden disruptions resulting in severe losses. These events were often triggered by protocol failures, bridge exploits, or large-scale exchange hacks. Below are five of the most significant, ranked by absolute dollar loss and their share of the total crypto market cap at the time.

Poly Network Exploit (Aug 2021)

A smart contract flaw allowed an attacker to seize \$611 million across Ethereum, BSC, and Polygon. While most funds were later returned, the incident exposed major weaknesses in cross-chain infrastructure and highlighted the urgent need for rigorous contract audits.

Ronin Bridge Hack (Mar 2022)

Hackers drained \$624 million in ETH and USDC from the Ronin Bridge supporting Axie Infinity by compromising validator keys. The breach went undetected for six days and emphasized the security risks tied to centralized validator systems in cross-chain networks.

Terra LUNA/UST Collapse (May 2022)

When Terra’s stablecoin UST depegged, LUNA hyperinflated and collapsed, wiping out over \$60 billion in value, around 5% of crypto’s total market cap. The event triggered a widespread market crash and exposed the systemic fragility of algorithmic stablecoins.

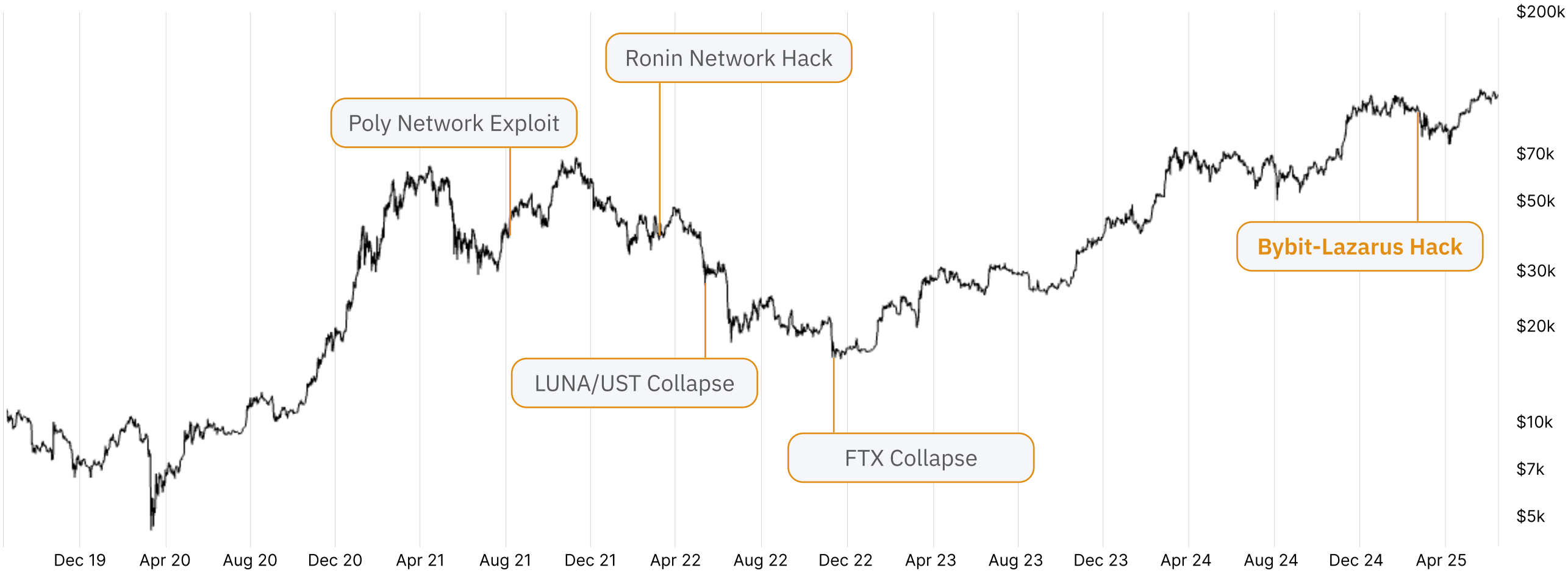
FTX Collapse (Nov 2022)

The failure of FTX led to an estimated \$8–10 billion in customer losses after revelations of fund misuse between the exchange and Alameda Research. The collapse halted withdrawals, triggered industry-wide contagion, and became the most damaging centralized exchange failure in crypto history.

Bybit-Lazarus Hack (Feb 2025)

In the largest centralized exchange hack on record, attackers stole \$1.4 billion in ETH from a Bybit cold wallet. While user funds were reimbursed and operations quickly restored, the breach renewed concerns over custodial security and off-chain operational risks.

Bitcoin Price (2019-2025)



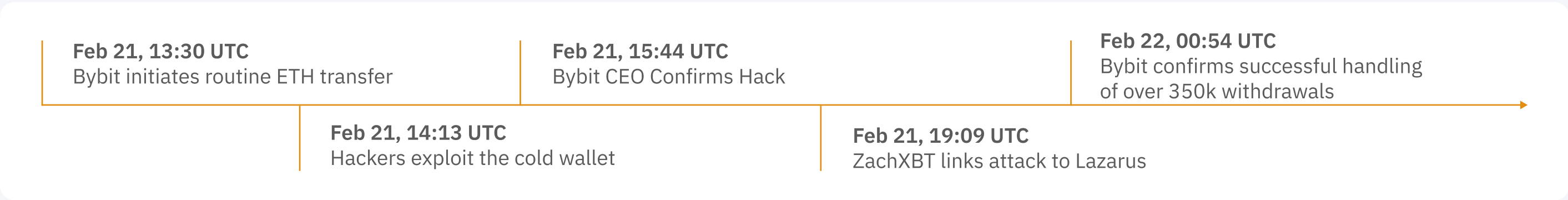
Bybit-Lazarus Hack

While the crypto space has endured massive collapses like Terra and FTX, not every disruption leads to systemic fallout. A recent example is the hack on the Bybit exchange on February 21, 2025, where \$1.4B in ETH was stolen. Despite the scale, Bybit acted swiftly, restoring funds, maintaining operations, and preserving market confidence.

Unlike past crises, this incident highlights how strong internal controls and transparent crisis management can

prevent contagion. The market remained stable, showing the maturing resilience of the industry.

We now provide a brief overview of Bybit’s platform, followed by a focused case study, including a timeline of key events and analysis of its post-hack recovery.



Key Insights

- Bybit executed a near-complete recovery of its Ethereum and Ethereum-derivative reserves following the hack, with balances rebounding from a post-incident low of 236k ETH to 729k ETH. This recovery brings holdings within 6% of the pre-hack total of 779k ETH, signaling restored operational stability and user trust in the platform’s custody infrastructure.
- The hacking event triggered a broad-based drop in open interest across Ethereum, Bitcoin, and Solana contracts on Bybit. Encouragingly, all three have since fully recovered, with Bitcoin returning to pre-hack levels, while Ethereum and Solana have surpassed them.
- Perpetual trading volumes across major assets remained stable throughout the hack, highlighting sustained user confidence despite the incident. Following the event, Bitcoin and Solana recorded average daily volumes of \$10B and \$1.7B, respectively, while Ethereum volume recently surged to an all-time high of \$8.5B/day.
- Post-hack, Ethereum, Bitcoin, and Solana experienced a sharp widening of bid-ask spreads and a steep drop in market depth, indicating significant liquidity stress lasting until mid-April. Since then, both spreads and market depth have steadily normalized beyond pre-incident levels, reflecting a strong recovery in both liquidity and market confidence.
- Glassnode’s proprietary Internal Reshuffling Ratio and Whale Withdrawal Ratio both spiked sharply following the Bybit hack, reflecting intense internal asset movements and large-scale withdrawals by major holders. Notably, both indicators quickly normalized, indicating that operational stress and whale-driven withdrawals were temporary and did not lead to sustained systemic risk.

Case Study:

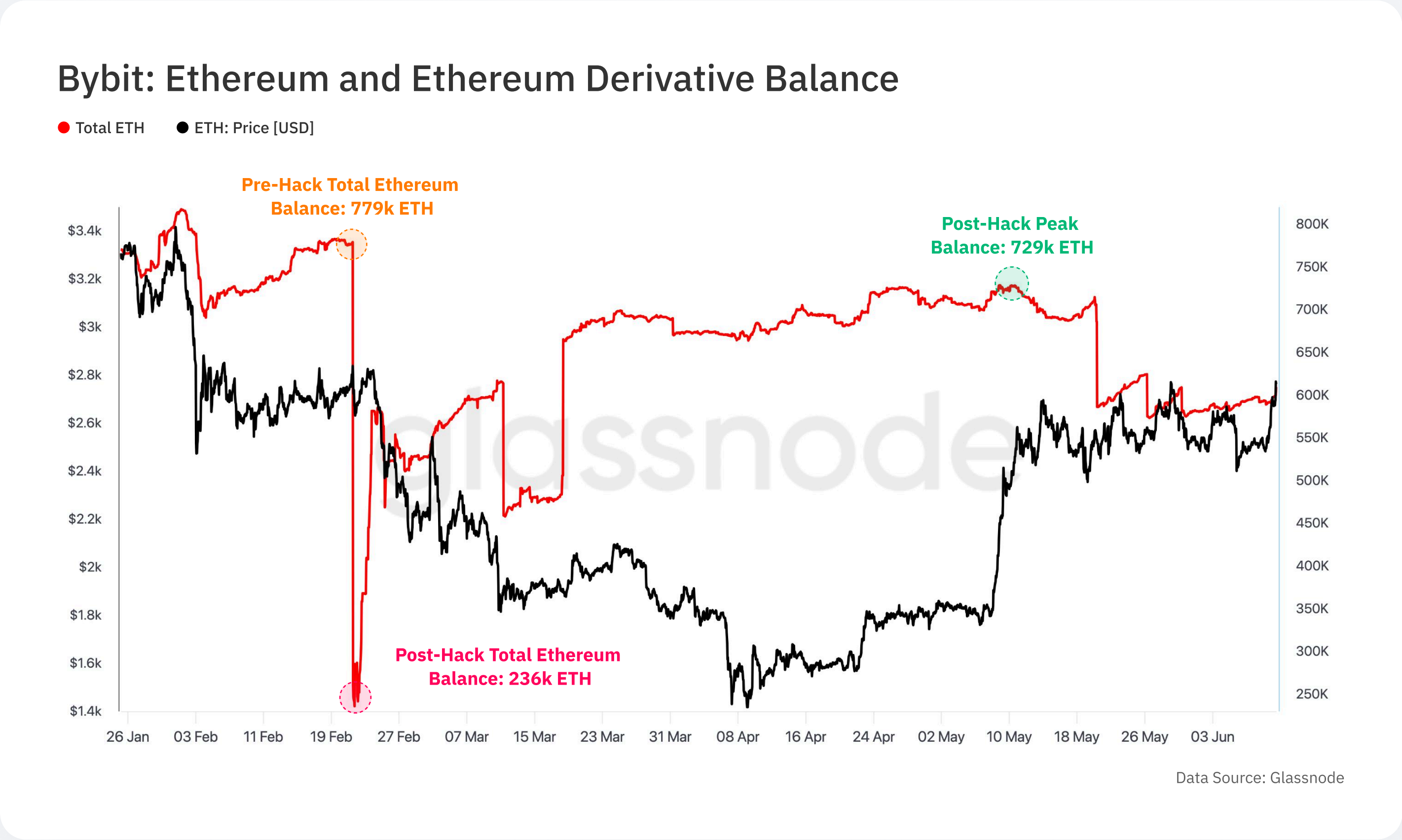
Bybit-Lazarus Hack

Replenishment of Stolen Assets

On February 21, 2025, Bybit experienced one of the largest exchange hacks in crypto history after suffering a major security breach. The attacker exploited smart contract permissions to drain 403,996 ETH (approximately \$1.13B) from the platform’s Ethereum cold wallet, redirecting the funds to an unidentified address. The breach extended beyond Ethereum, with losses spanning multiple liquid staking derivative tokens, bringing the total loss to approximately \$1.48B:

- **Ethereum (ETH):** 403,996 ETH
- **Staked Ethereum (stETH):** 91,076 stETH
- **mETH:** 8,000 mETH
- **cmETH:** 15,000 cmETH

Prior to the hack, Bybit’s holdings totaled over 779k ETH and associated derivatives, with reserve balances dropping sharply to just 236k ETH in the immediate aftermath. Since then, a near-complete recovery has taken place, with holdings rebounding to a peak of 729k ETH, underscoring a rapid and effective asset restoration effort.



Open Interest Recovery

Perpetual Open Interest

Ethereum

Over the years, Bybit has remained an industry leader within the digital asset derivatives market, consistently ranking among the top five exchanges for open interest and trading volume. In this section of the report, we examine the immediate impact of the hack on Bybit’s derivatives marketplace, as well as its subsequent recovery and return to normal operations over the following months.

Within just one week of the security breach, perpetual open interest across Bybit’s Ethereum contracts fell aggressively from \$3.3B to \$1.8B. Coupled with a

concurrent drop in Ethereum’s price, open interest declined further to a cycle low of \$1.5B in early April, its lowest level since February 2024.

Nevertheless, since reaching this low, the market has demonstrated a robust recovery, with open interest rebounding to \$3.9B, remarkably surpassing pre-hack levels. This suggests that customer confidence in Bybit was restored quickly, with traders willing to return to the platform.

ETH: Futures Open Interest Perpetual

● ETH: Futures Open Interest Perpetual - Bybit [USD] ● ETH: Price [USD]



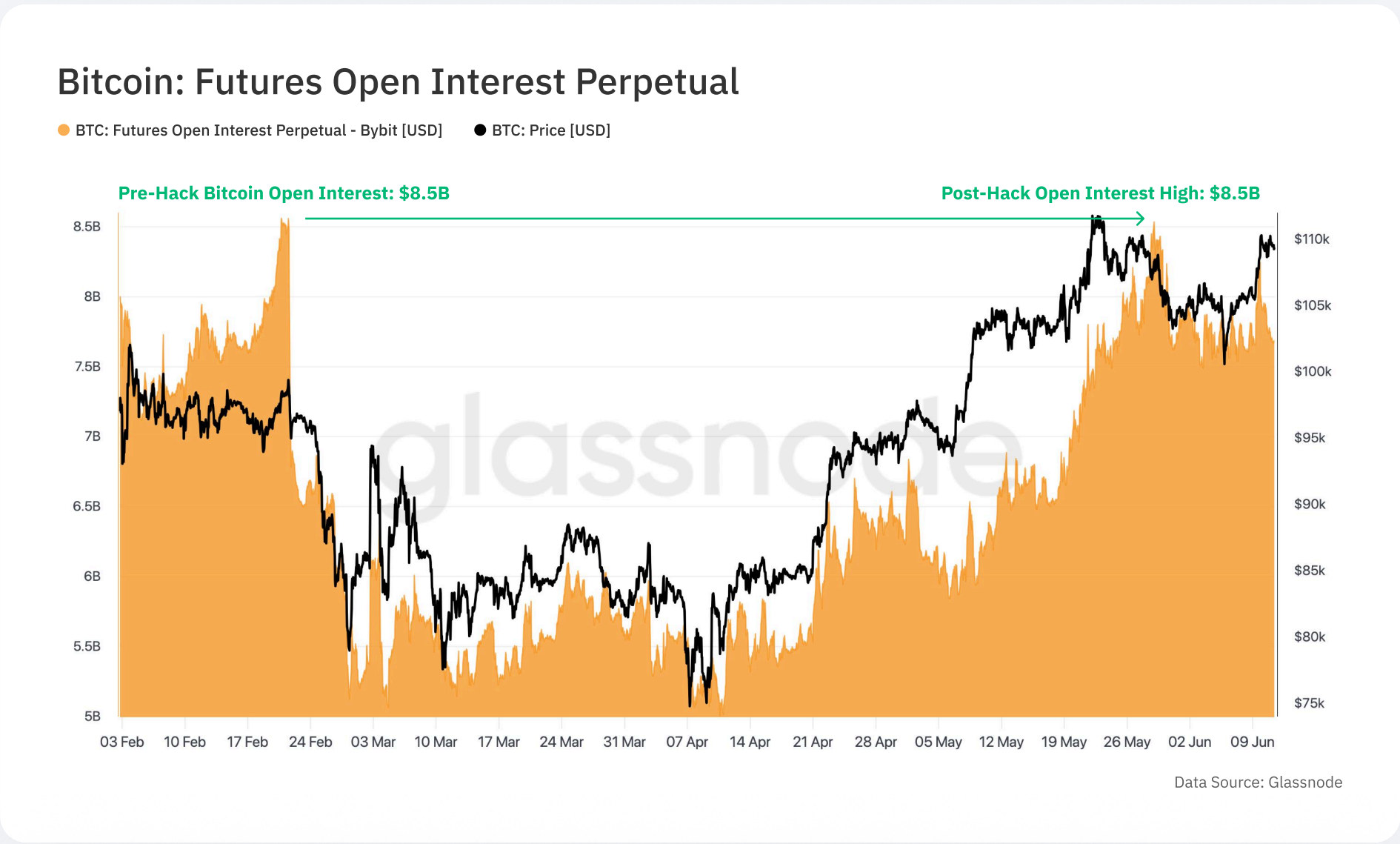
Data Source: Glassnode

Perpetual Open Interest

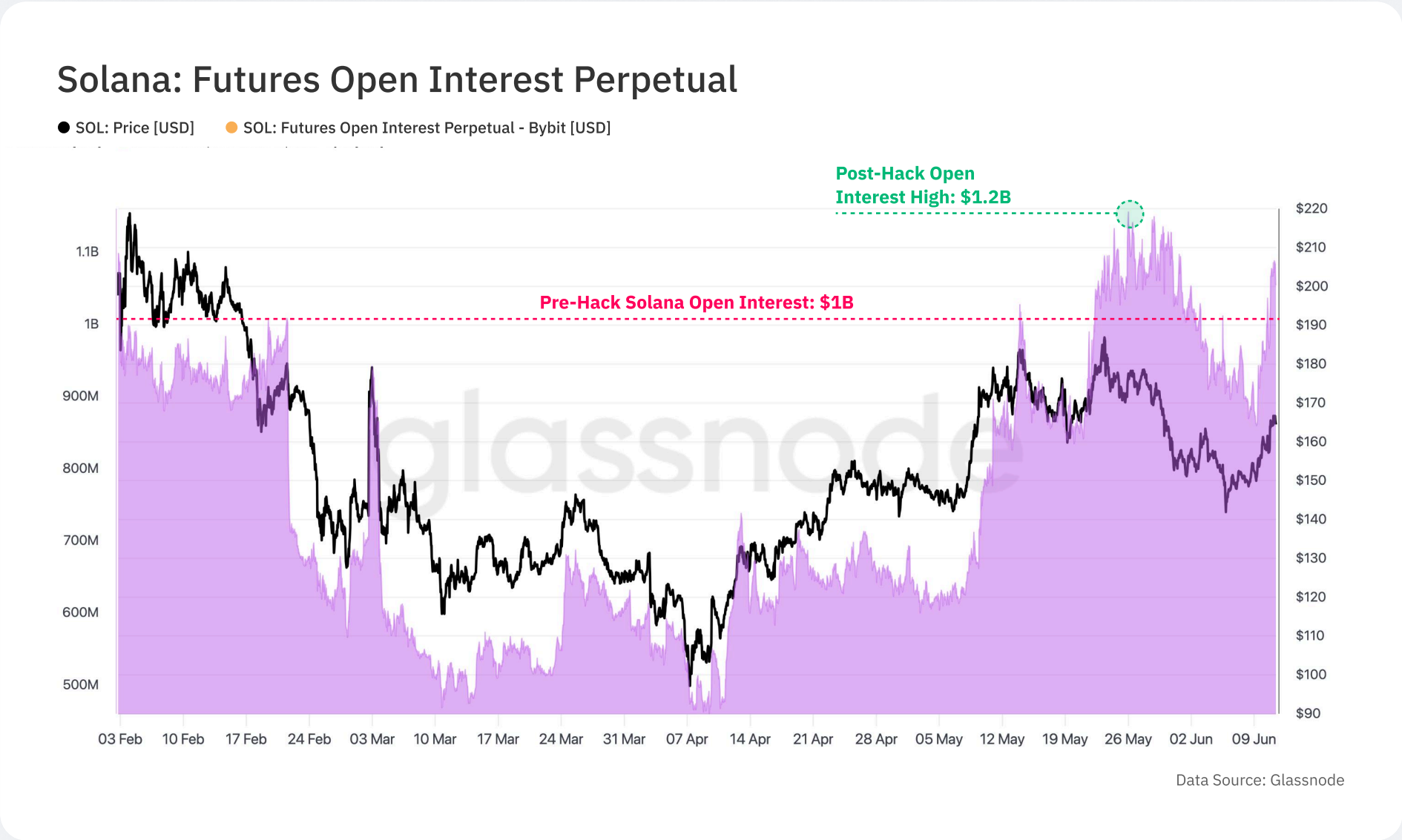
Bitcoin and Solana

A similar trend was observed across other major assets, with Bitcoin open interest dropping sharply from \$8.5B to \$5.1B in the week following the hack. Solana exhibited a comparable pattern, with open interest

falling from \$1B to \$570M over the same period. These broad-based declines indicate that the contraction in open interest was not isolated to Ethereum, but was indicative of a market-wide response.



Since then, the market has staged a strong recovery, with Bitcoin open interest returning to its pre-hack level, while Solana contracts have surpassed theirs, reaching peaks of \$8.5B and \$1.2B, respectively. This resurgence across all three major assets underscores renewed investor confidence in Bybit’s derivatives platform and reflects growing a appetite for trading, speculation, and hedging among its user base.



Perpetual Open Interest Percent Change

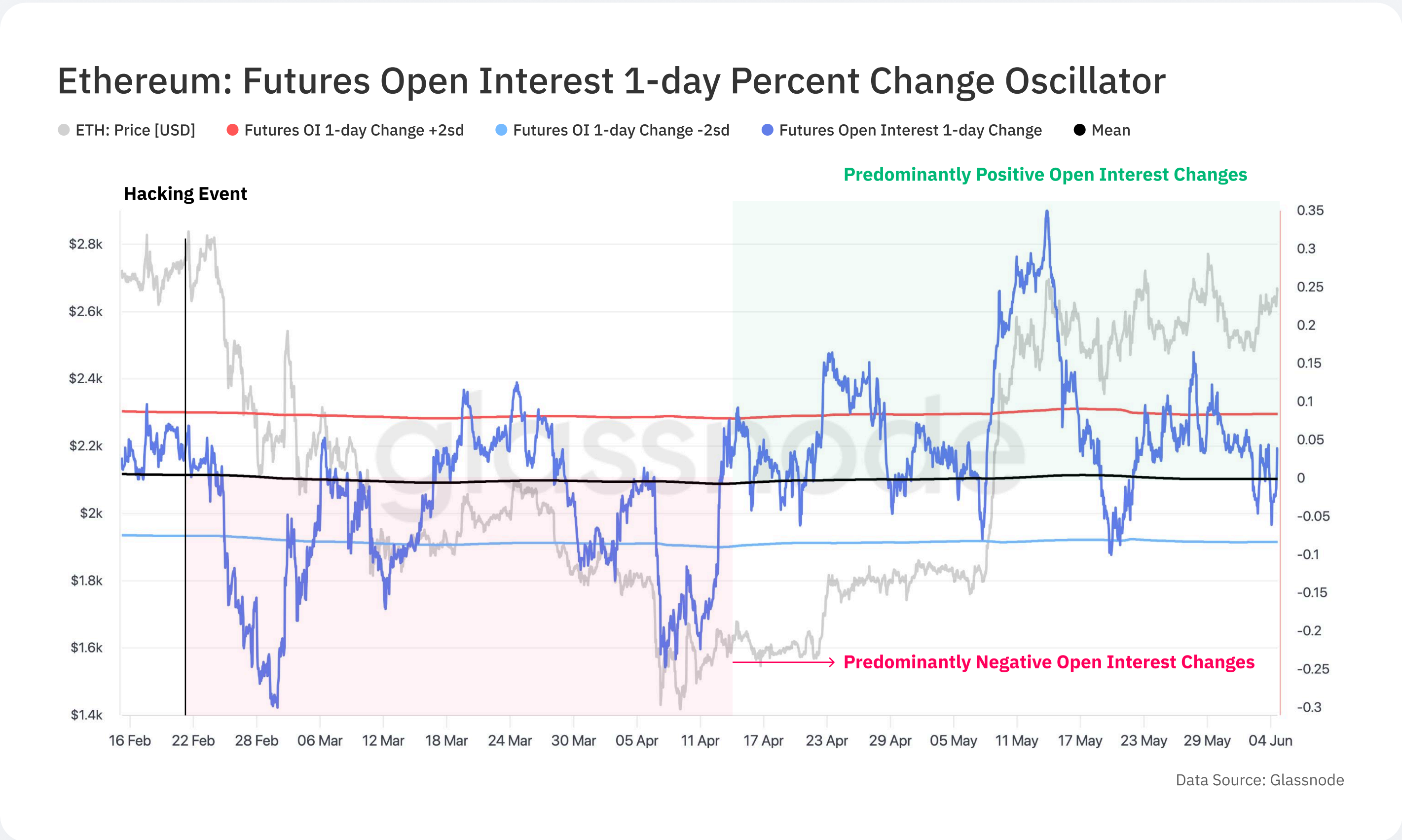
Ethereum

By analyzing the daily percentage change in Ethereum perpetual open interest, we can assess the severity of the drawdown immediately following the hacking event.

Notably, sharp and sustained declines were observed starting on February 22nd, the day after the breach. The peak of this event ranks among the most severe contractions in Ethereum open interest on Bybit, with only 34 trading days recording larger drops. A decline of

this magnitude suggests a pronounced unwinding of positions, driven by both heightened risk aversion and forced deleveraging.

Nonetheless, over the past two months, open interest changes have been predominantly positive, with the majority of values clustering near the long-term average and occasionally exceeding the two standard deviation threshold.



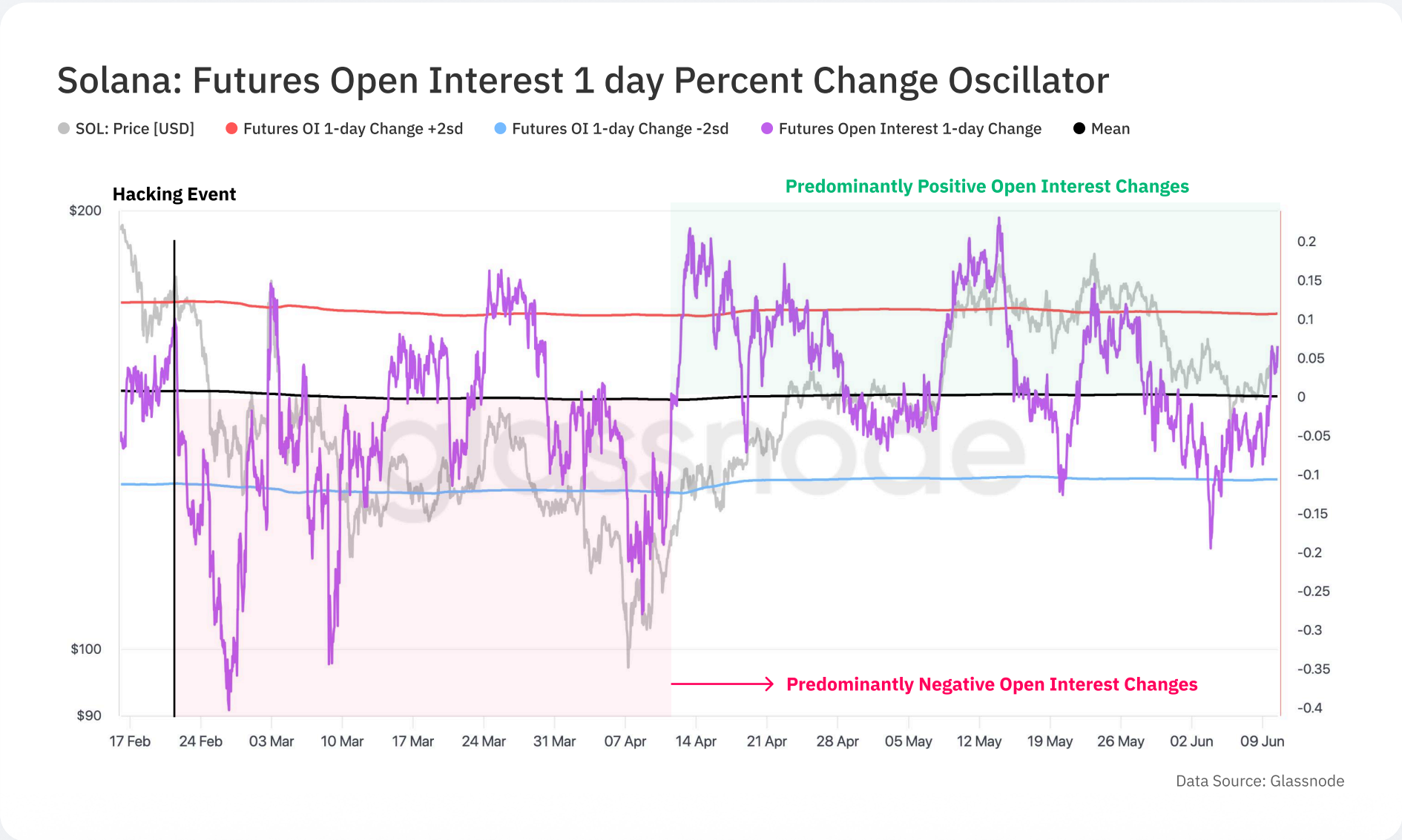
Perpetual Open Interest Percent Change

Bitcoin and Solana

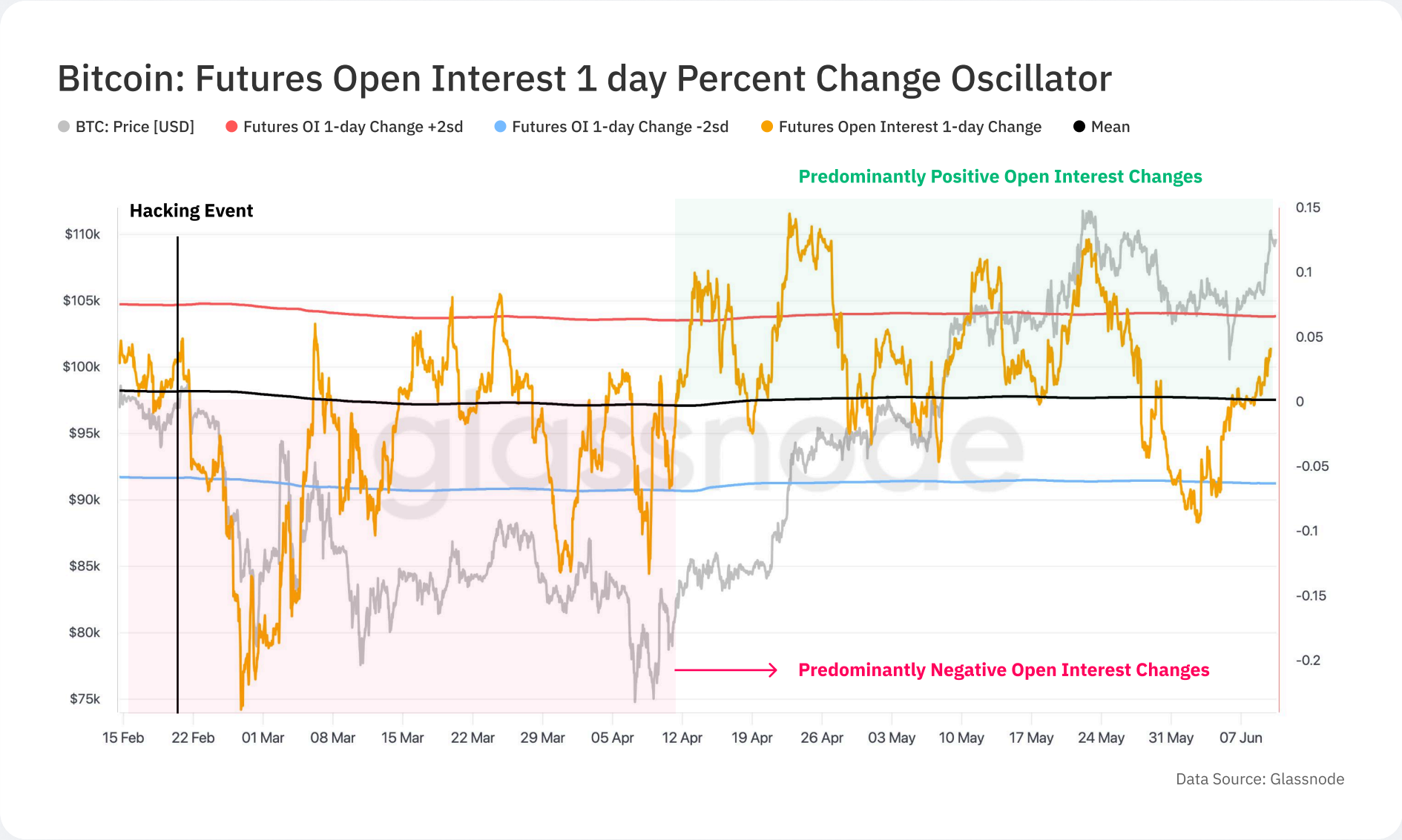
In confluence, the daily percentage change in perpetual open interest for Bitcoin and Solana contracts reveals a starkly similar pattern of stress following the breach.

The declines immediately after the hack stand out as anomalies, reflecting an aggressive but short-lived clearing of leveraged positions.

This broad-based reaction suggests that the event was a significant shock for investors, impacting market sentiment and positioning across all major assets, not just Ethereum.



However, over the past two months, open interest in Bitcoin and Solana contracts has shown consistent growth. This notable rise across the major assets underscores a strengthening of investor confidence and an increased appetite for risk, reinforcing the broader normalization observed across Bybit’s perpetual market.



Bybit Open Interest Dominance

Additionally, we can evaluate Bybit’s share of open interest across the top three assets as a proxy for its dominance within the derivatives landscape. Following the breach, Bybit’s share of open interest dropped from 25% to a low of 18%, marking a significant contraction in market dominance.

However, its relative open interest has since rebounded to approximately 21%, indicating a partial but meaningful recovery. Despite the initial setback, Bybit has retained its position among the top three exchanges by open interest, suggesting that while confidence was briefly dented, core market participation has remained robust.



Perpetual Volumes Remain Robust

Perpetual Volume

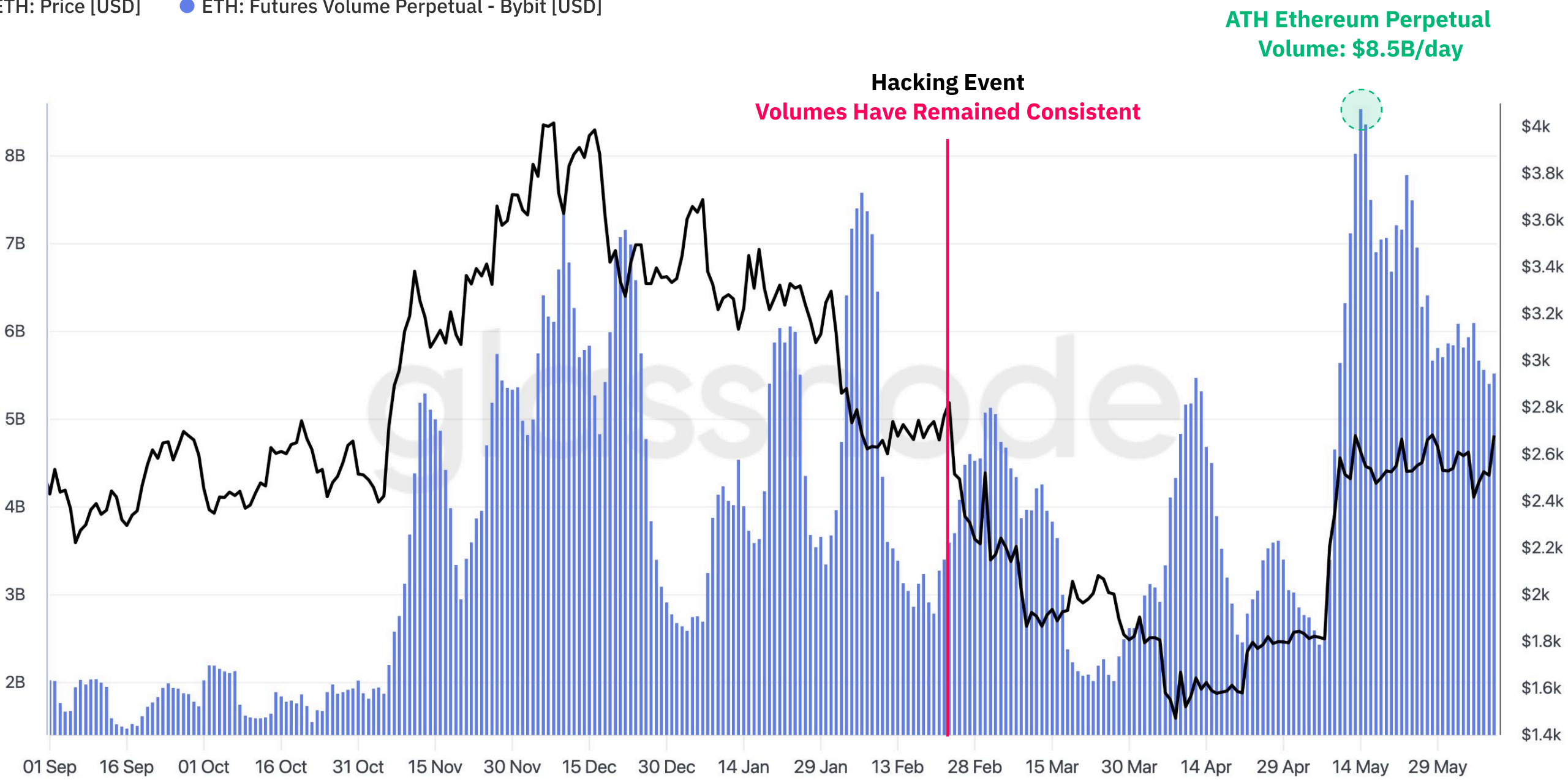
Ethereum

When examining perpetual trade volumes for the Ethereum asset, we observe stability in trading activity before and after the hack event, with volumes remaining largely unchanged. Additionally, following Ethereum’s outperformance in recent weeks, trade volume on Bybit has surged, reaching a new all-time high of \$8.5B/day, a remarkable milestone given that Ethereum was the primary asset targeted in the hack.

This resilience suggests that market participants maintained confidence in Bybit’s trading infrastructure, with recent activity driven more by external Ethereum-related catalysts than by internal security concerns.

Futures Volume Perpetual

● ETH: Price [USD] ● ETH: Futures Volume Perpetual - Bybit [USD]



Data Source: Glassnode

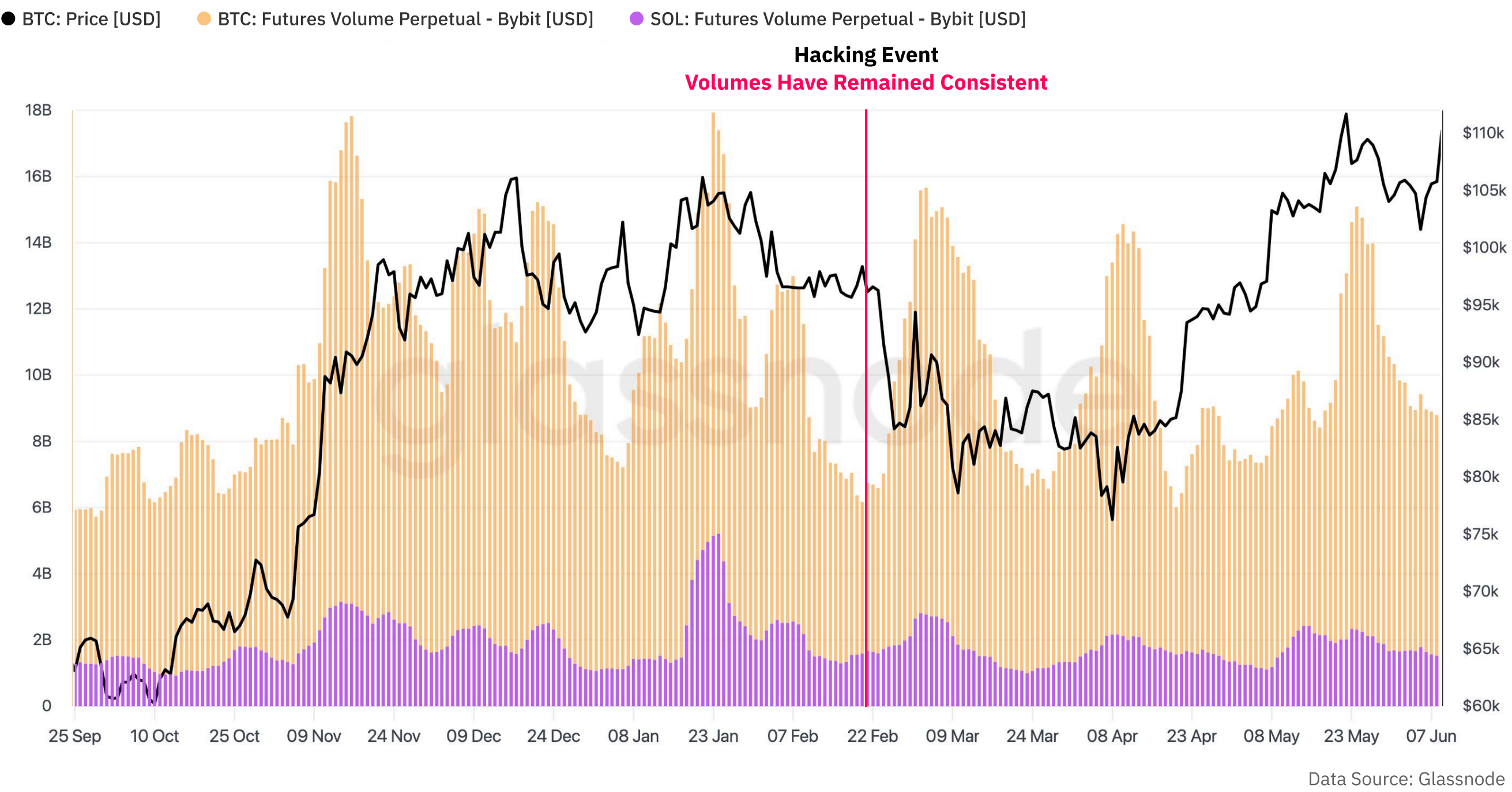
Perpetual Volume

Bitcoin and Solana

A similar trend emerged in the Bitcoin and Solana perpetual markets, where trade volumes remained steady and largely unaffected by the shock of the hack. Since the incident, average daily volumes have held at \$10B for Bitcoin and \$1.7B for Solana, indicating that trading activity across major assets remained resilient.

The consistency in perpetual volumes suggests that traders retained confidence in Bybit’s platform and operations, which continued uninterrupted despite the challenging circumstances.

Bitcoin and Solana : Futures Volume Perpetual Bybit

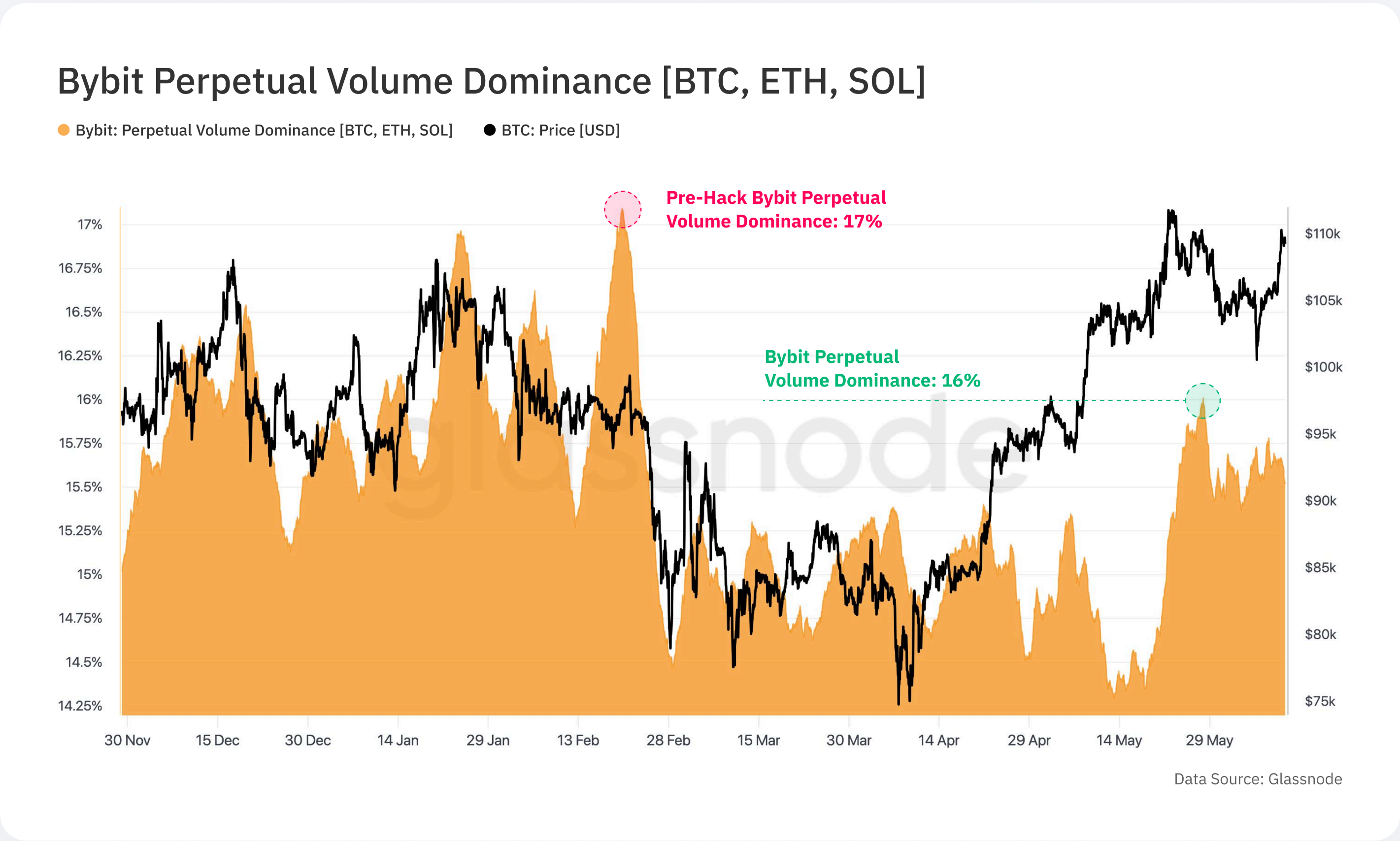


Perpetual Volume Dominance

When assessing Bybit’s relative share of perpetual volume across major assets (BTC, ETH, and SOL), a noticeable decline in market share followed the event, with Bybit’s dominance falling from 17.0% to 14.3%.

While aggregate volumes across these assets remained strong, competing exchanges captured a larger portion of

trading activity during this period. Nevertheless, Bybit has shown strong signs of recovery, with perpetual market dominance rebounding to a post-hack peak of 16.0%.



Liquidity Conditions Improve

Perpetual Bid-Ask Spread

Strong liquidity conditions are a fundamental pillar of a functioning exchange, ensuring that traders can enter and exit positions efficiently, with minimal price impact and lower transaction costs. In severe cases, thin liquidity can destabilize market structure, making it difficult for the exchange to facilitate orderly trading.

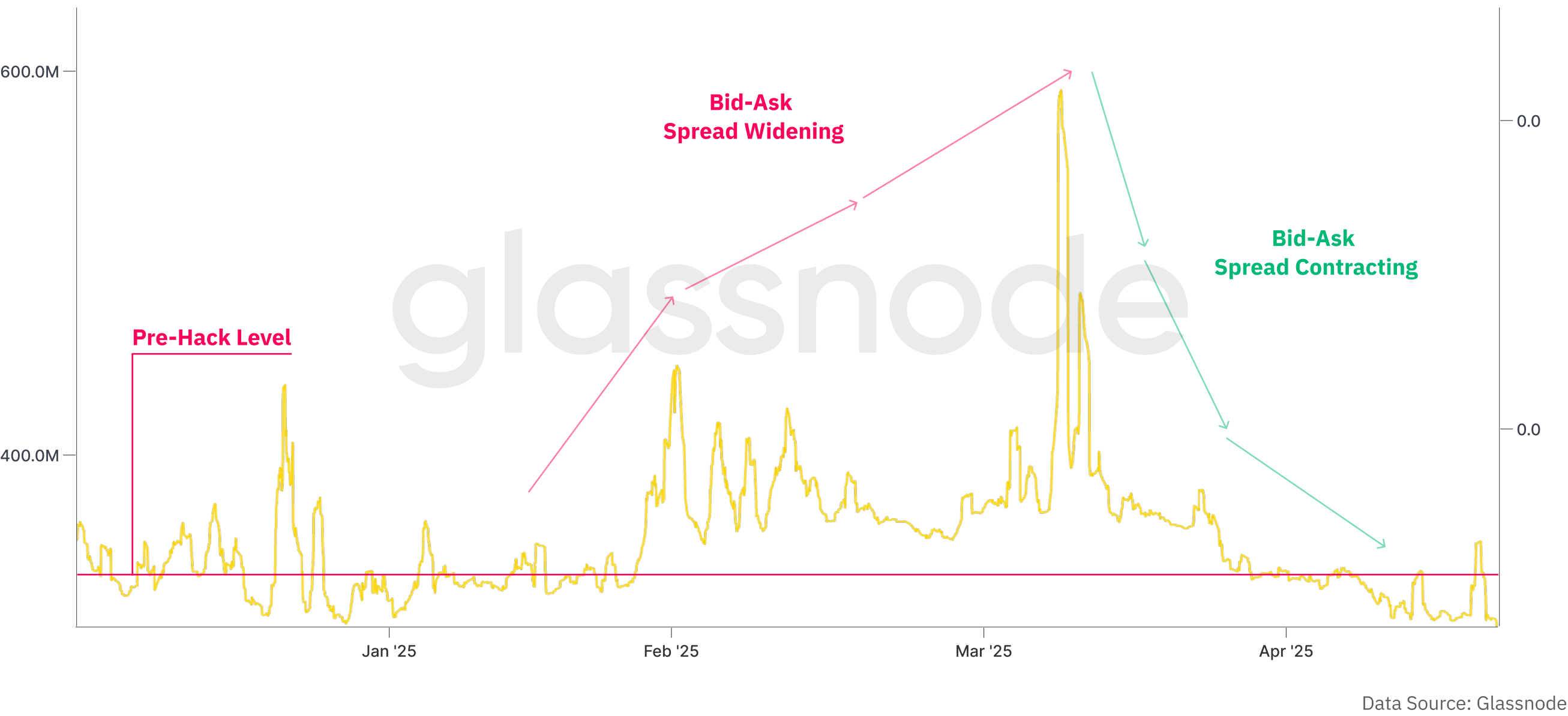
One way to gauge liquidity is by analyzing the bid-ask spread. By comparing spreads for BTCUSDT, ETHUSDT, and SOLUSDT before and after the hack, we can assess the market’s response and evaluate how effectively Bybit’s derivatives returned to normal trading conditions.

In the immediate aftermath of the hack, bid-ask spreads widened significantly, signaling a sharp decline in market liquidity. This dislocation persisted through February into mid-April, with spreads reaching their widest points during this period.

Encouragingly, bid-ask spreads have steadily narrowed in recent months, returning to levels close to those observed before the incident. This ongoing normalization suggests a restoration of liquidity and a broader recovery in market confidence.

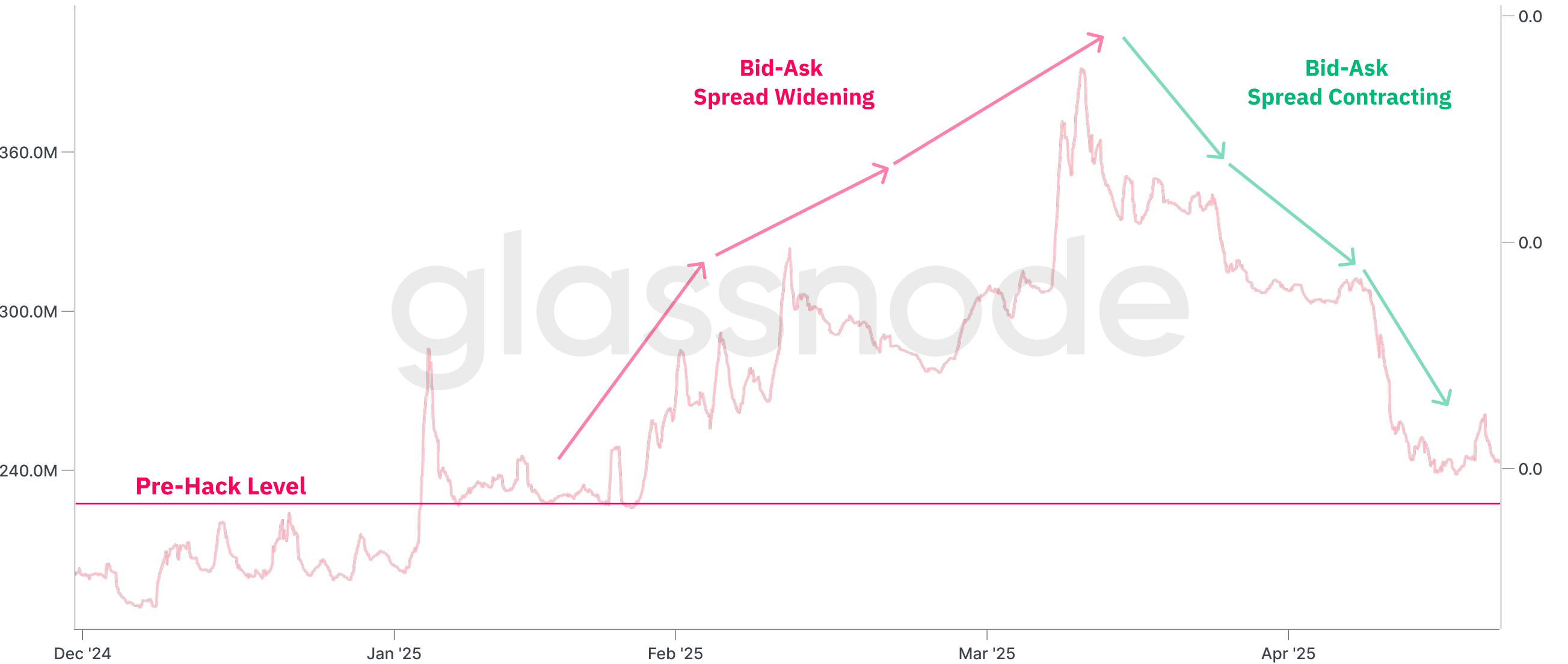
Bitcoin: Bid-Ask Spread

● BTC Bid-Ask Spreads



Ethereum: Bid-Ask Spread

● ETH Bid-Ask Spreads



Data Source: Glassnode

Solana: Bid-Ask Spread

● SOL Bid-Ask Spreads



Data Source: Glassnode

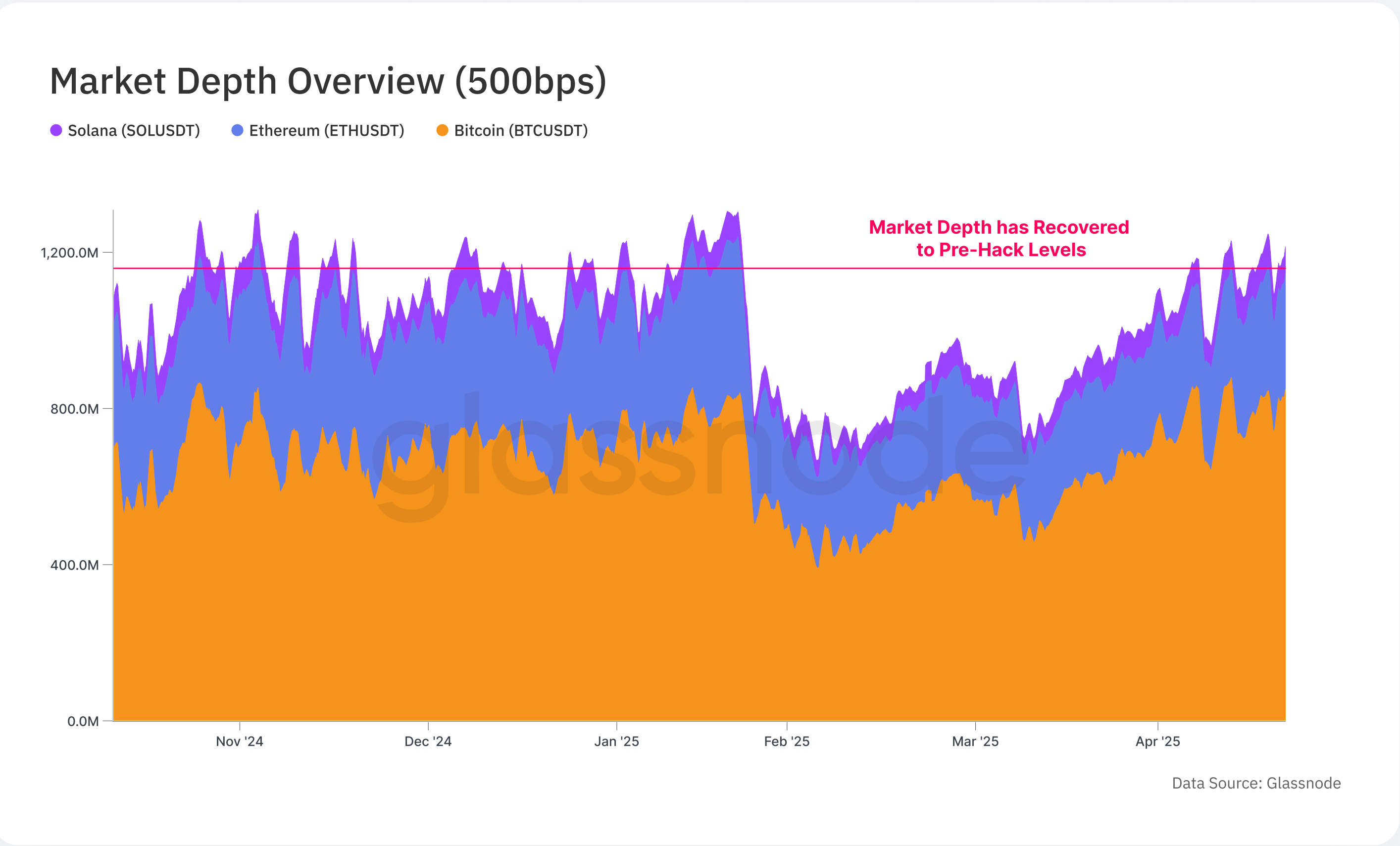
Perpetual Market Depth

To complement the analysis, we can examine the $\pm 5\%$ market depth across the aforementioned pairs, representing the volume of buy and sell orders beyond the best bid and ask price.

Following the hack, a sharp contraction in market depth was observed across all pairs, indicating a widespread withdrawal of limit orders within $\pm 5\%$ of the mid-price.

This behavior is typical during periods of elevated uncertainty, as participants de-risk and retreat from providing liquidity.

Notably, depth has since recovered. By May, market depth levels across all pairs surpassed pre-incident values, suggesting a strong return of active participation from market makers.



Exchange Risk Diagnostics:

Evaluating Bybit's Operational Stability Post-Hack

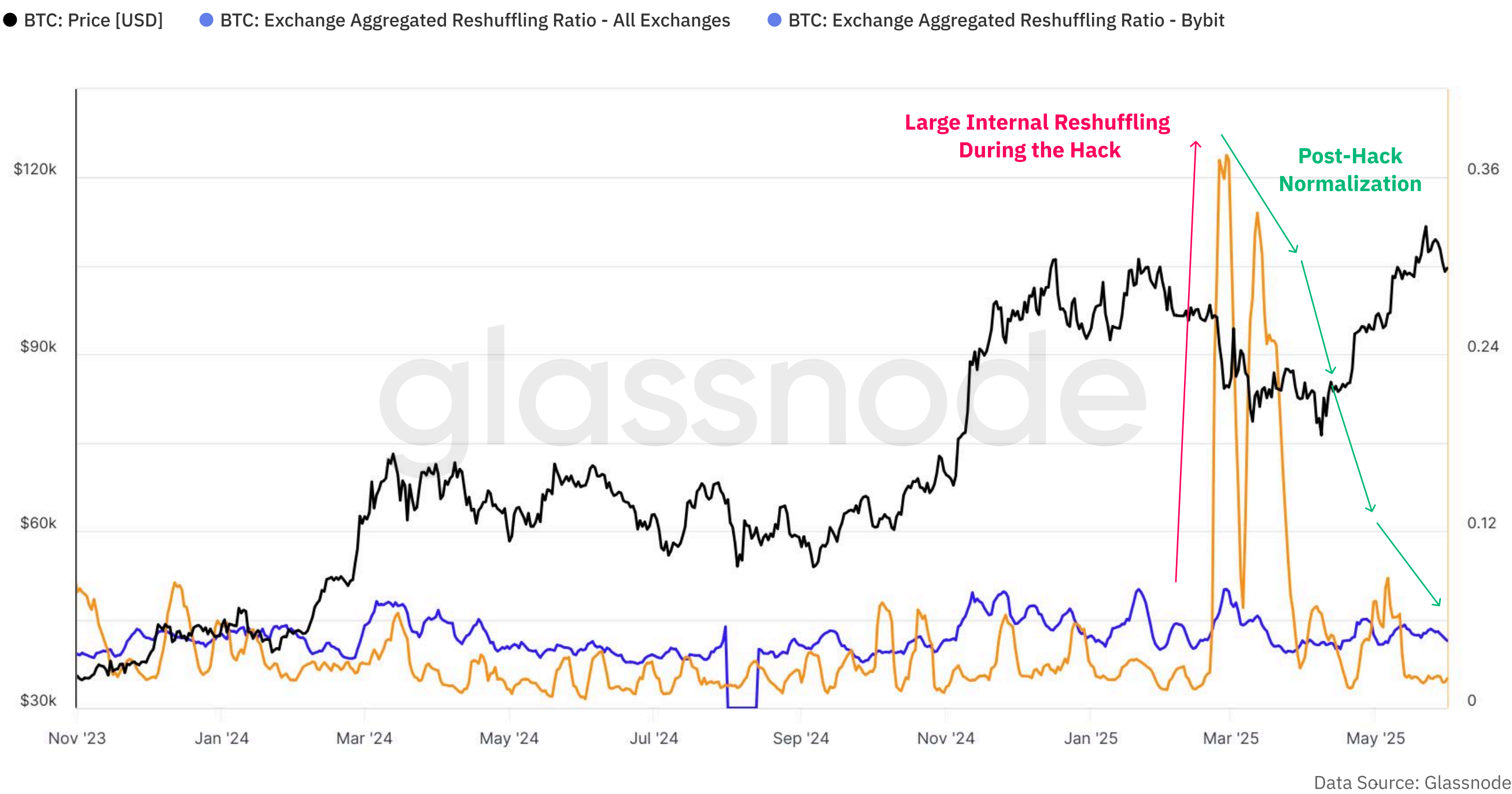
In the aftermath of high-profile collapses like FTX, assessing exchange-specific operational risks has become imperative. To address this need, Glassnode developed a bespoke framework focused on identifying early warning signs of internal stress and liquidity strain. This framework comprises two proprietary indicators:

- **Internal Reshuffling Ratio** — Measures the intensity of internal fund movements within an exchange. Elevated and erratic values may flag instability in liquidity management.
- **Whale Withdrawal Ratio** — Tracks large-scale withdrawals to non-exchange entities. A spike could suggest internal stress, reduced user trust, or attempts to exit amidst uncertainty.

Using this framework, we examine Bybit’s on-chain activity surrounding the security breach. By analyzing shifts in these indicators before, during, and after the incident, we can assess both the magnitude of operational disruption and the trajectory of recovery.

At the peak of the incident, Bybit’s Internal Reshuffling Ratio surged to ~37%, meaning more than a third of its total assets were being actively moved internally each day. This was over 4.6x higher than the industry average of ~8%, indicating intense operational stress. The elevated ratio persisted for over a month, likely due to emergency fund reallocation, wallet restructuring, or enhanced internal audits triggered by the breach.

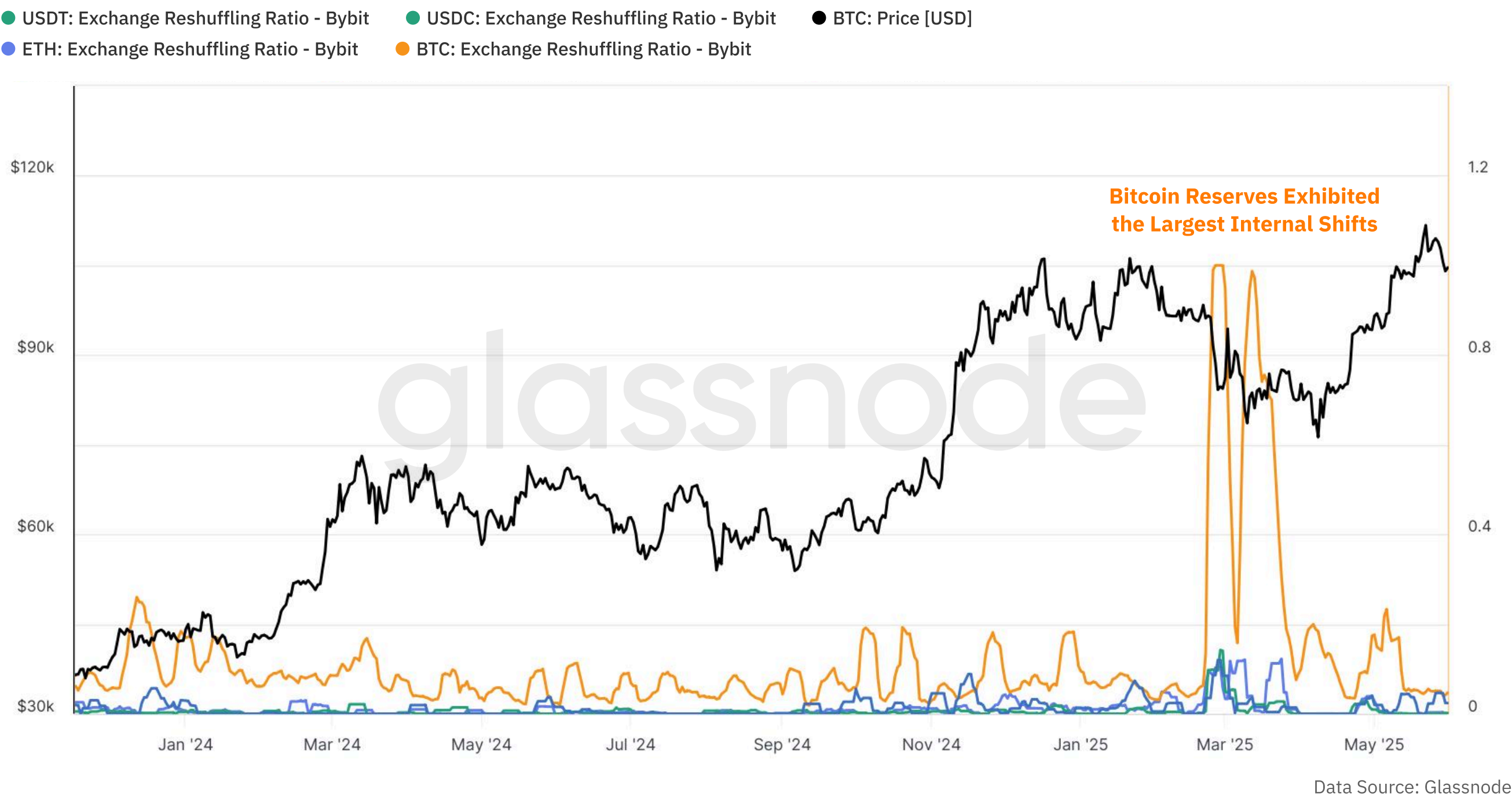
Bybit: Exchange Aggregated Reshuffling Ratio



A similar pattern emerges when examining the Internal Reshuffling Ratio for individual assets on Bybit. Notably, Bitcoin experienced an extreme spike, with the ratio exceeding 90%, and remained elevated for a prolonged period compared to other tokens. This suggests that Bitcoin reserves were likely the primary asset mobilized to meet the heightened wave of user withdrawals following the breach.

In contrast, reshuffling activity across other major assets, including Ethereum, gradually subsided and returned to normal levels within a month, highlighting the restoration of internal liquidity operations.

Bybit: Top Assets Exchange ETH Reshuffling Ratio



Whale Withdrawal Ratio

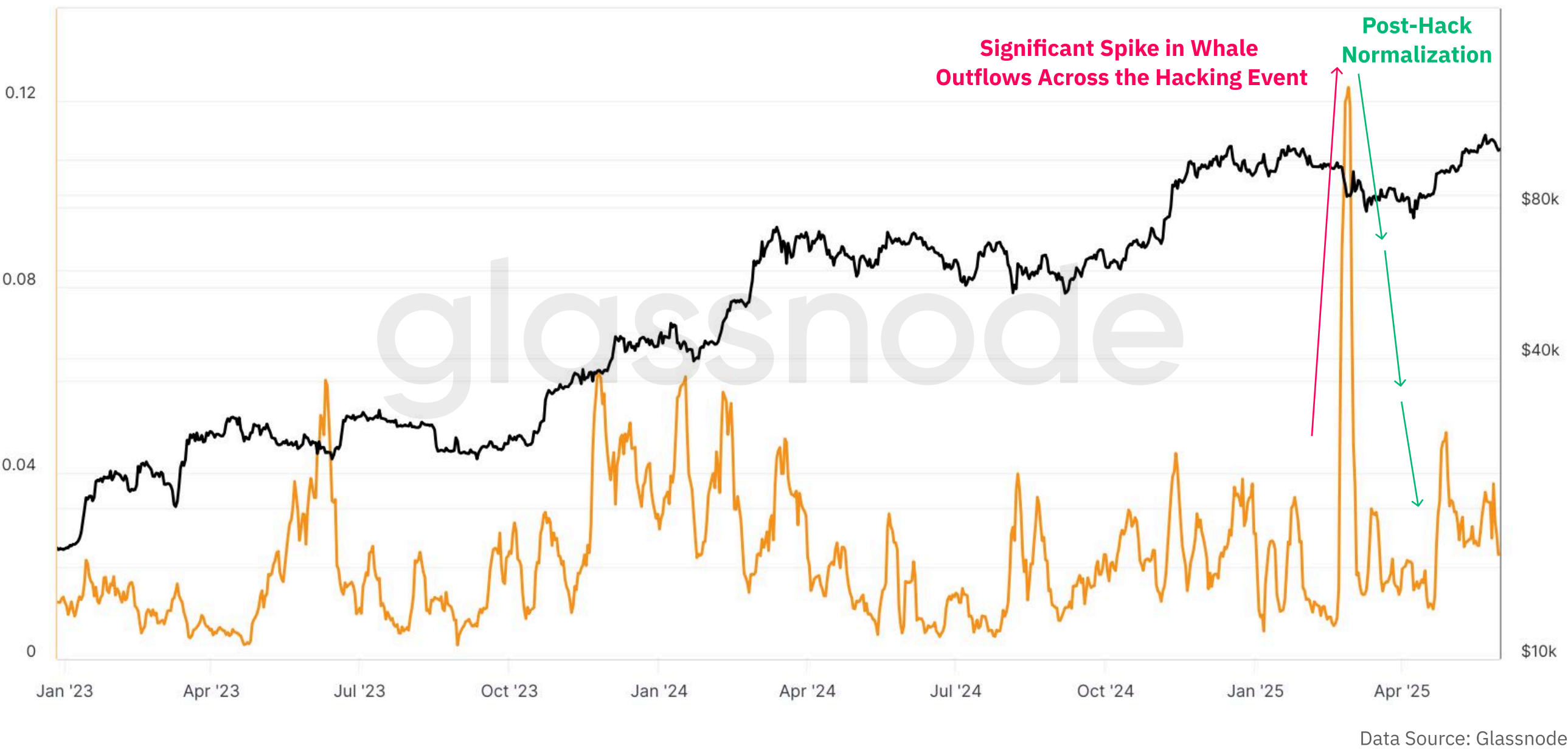
With Bitcoin showing the most significant deviation in internal fund movements, we can employ our second risk indicator, the Whale Withdrawal Ratio, to assess the behavior of statistically large holders on Bybit following the hack event.

In the two weeks following the breach, the ratio spiked to around 12%, marking a 3x increase relative to its typical upper range. This surge indicates an aggressive

withdrawal response by large entities, likely reflecting precautionary fund migration. Importantly, the metric normalized shortly thereafter, suggesting that the duration of whale-driven stress was short-lived and did not escalate into broader systemic pressure.

BTC: Exchange Whales Outflow

● BTC: Price [USD] ● BTC: Exchange Whales Outflow - Bybit



Conclusion

The February 2025 Bybit-Lazarus hack marked one of the largest security breaches in crypto history, resulting in the loss of over \$1.4 billion in ETH and staking derivatives. Yet, in contrast to prior black swan events such as the collapses of FTX and Terra, this incident did not trigger systemic fallout.

Through swift operational response, transparent communication, and strong internal controls, Bybit restored user funds, stabilized its platform, and contained contagion risk.

Across multiple indicators, including perpetual open interest, trading volumes, and liquidity metrics, the market exhibited a brief but controlled contraction followed by a steady and robust recovery.

Ethereum, Bitcoin, and Solana markets all saw a retracement in open interest post-hack, but later rebounded to, or exceeded, pre-incident levels. Notably, Ethereum perpetual volume surged to an all-time high of \$8.5B/day, reflecting market confidence in Bybit's infrastructure.

From a liquidity standpoint, initial stress was evident in widened bid-ask spreads and reduced market depth, yet both metrics normalized by mid-Q2 2025, suggesting the return of institutional market makers and overall trading health. While Bybit's share of perpetual market volume and open interest declined briefly, the exchange has since regained ground and remains a top player in crypto derivatives.

Risk diagnostics, namely the Internal Reshuffling Ratio and Whale Withdrawal Ratio, showed clear but temporary spikes, consistent with internal fund restructuring and precautionary large-holder exits. Their rapid normalization further underscores the short-lived nature of stress and the effectiveness of Bybit's operational recovery.

Overall, this report highlights a significant shift in crypto market structure: **an increasing capacity to absorb and rebound from large-scale disruptions. Bybit's case is not just a recovery story, but a stress-tested validation of institutional-grade practices now taking root in digital asset markets. If such resilience becomes the norm, it may pave the way for greater investor confidence and long-term maturity across the broader crypto ecosystem.**

Disclosure:
This report was commissioned by Bybit and prepared independently by Glassnode. The content herein is provided for informational purposes only and does not constitute investment advice, a recommendation, an offer, or a solicitation to buy or sell any financial instrument, digital asset, or to participate in any investment strategy. This material is intended solely for sophisticated or institutional investors and should not be relied upon for accounting, legal, or tax advice. Recipients should conduct their own due diligence and consult independent professional advisors before making any investment decisions.

Disclaimer:
The information provided in this report is for general informational purposes only and does not constitute investment, financial, legal, or other professional advice. While Bybit strives to ensure the accuracy and reliability of the information presented, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the report or the information contained herein.
Any reliance you place on such information is therefore strictly at your own risk. Bybit shall not be held responsible for any loss or damage arising directly or indirectly from the use of or reliance on the information provided in this publication.
The views and opinions expressed in this report do not necessarily reflect those of Bybit or its affiliates. Past performance is not indicative of future results. All trading involves risk, and you should only trade with funds you can afford to lose.