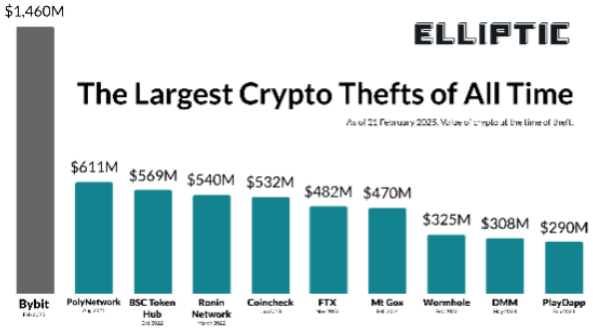
The Bybit heist: money heist in the crypto world

Image source: Bybit

PRIVATE BANKING

Introduction

On 21 February 2025, the cryptocurrency industry was stunned by an unprecedented security breach at Bybit, one of the world's leading crypto exchanges. Attackers diverted roughly 400,000 ethereum, valued at approximately $1.5 billion, from one of Bybit's cold wallets during what appeared to be a routine fund transfer. Recognised as the largest digital asset theft in history, the heist has sent ripples across the crypto world, shaking investor confidence and prompting regulators to scrutinise digital asset security measures.



Attackers diverted roughly 400,000 ethereum, valued at approximately $1.5 billion, from one of Bybit's cold wallets during what appeared to be a routine fund transfer. Recognised as the largest digital asset theft in history, the heist has sent ripples across the crypto world, shaking investor confidence and prompting regulators to scrutinise digital asset security measures.

How the attack unfolded

The breach was the result of a sophisticated manipulation of Bybit's transaction process. What initially appeared as an ordinary fund transfer from an offline cold wallet to a warm wallet quickly devolved into chaos when attackers altered the smart contract logic and masked the signing interface. This front-end manipulation enabled the hackers to display what seemed like a legitimate transaction, while executing a hidden malicious order that redirected control of the ETH cold wallet. The rapidity of the attack meant that the diversion of 400,000 ethereum went undetected until the abnormal activity was flagged by routine monitoring systems. Cybersecurity experts have noted that this method, which bypasses standard authentication protocols, is indicative of an evolution in digital asset attack strategies.

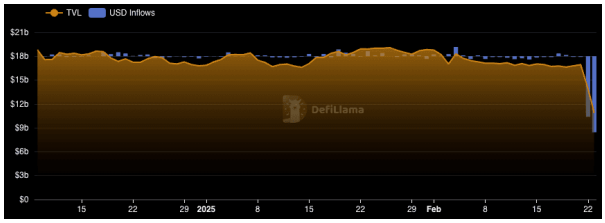
Who might be behind the heist

In the aftermath of the breach, investigative efforts have pointed toward the notorious Lazarus Group as the likely culprit. This hacking collective has a long and storied history of high-profile cyberattacks targeting financial institutions and cryptocurrency platforms alike. Analysts have observed several hallmarks in this heist that mirror Lazarus's established modus operandi. Chief among these is the sophisticated manipulation of transaction processes and the ability to mask malicious activity behind a veneer of legitimacy.

Security researchers from firms such as Elliptic and Arkham Intelligence have reportedly detected technical patterns in the breach that match previous Lazarus operations. Adding further weight to these findings, independent cybersecurity expert ZachBXT has also identified Lazarus as the likely architect behind the heist. Although neither Bybit nor official regulatory bodies have confirmed these suspicions, the convergence of multiple independent analyses suggests that the breach may indeed be part of a broader, state-affiliated cyber campaign.

Market reaction and financial impact

In the immediate aftermath of the breach, the market was plunged into chaos as investors reacted with fear and uncertainty. The news of the $1.5 billion theft set off a chain reaction. Within hours, a massive panic withdrawal was triggered across the platform, resulting in approximately $4 billion in withdrawals in a desperate bid to safeguard assets.



The shock didn't only impact Bybit. Bitcoin, often seen as a safe haven for the crypto market, experienced drastic price correction, dropping from around $99,398 to roughly $94,938 in a matter of hours, before eventually stabilising. Ethereum, which was directly involved in the heist, also saw its price dip by nearly 4% immediately following the incident, reflecting broader investor apprehension about the security of digital assets. Trading volumes surged dramatically during this period of heightened volatility, as many market participants hurriedly liquidated their positions.

Bybit's response and recovery efforts

In response to the crisis, Bybit moved swiftly to mitigate the damage and restore confidence among its user bases. The exchange's CEO publicly reassured stakeholders by affirming that Bybit remains solvent despite the loss, adding that the money would be covered by the firm or by a loan from partners. He emphasised that all client assets are fully backed on a one-to-one basis, a critical point intended to soothe fears of a systemic collapse. Moreover, Bybit has taken a proactive stance by offering a 10% reward on any funds that are eventually recovered. This incentive is part of a broader effort to encourage cooperation from the community and expedite the recovery process.

At the same time, Bybit is also collaborating with leading cybersecurity firms and regulatory authorities to trace the stolen assets and strengthen the overall security framework. These recovery efforts seek to reclaim lost funds while highlighting the importance of rigorous risk management and robust defence mechanisms in digital finance.

Choosing the right solution for you

In light of the recent Bybit breach, choosing the optimal solution for managing digital assets is more critical than ever. While hot wallets provide easy access and the convenience needed for day-to-day trading, they are often vulnerable to cyber threats and expose investors to significant counterparty risk. On the other hand, cold storage provides strong protection against hacking, but its inherent physical limitations, such as recovery issues and reduced convenience for active trading, can hinder swift asset management during market opportunities.

Traditional banks, with their rigorous regulatory oversight and time-tested security protocols, can offer a trusted gateway for both individual and institutional investors, particularly when they have confidence in the asset class and are committed to forging a bridge between conventional and decentralised finance. Their robust frameworks help mitigate common vulnerabilities, ensuring that digital asset management is both secure and reliable.

By relying on the established safeguards of traditional financial institutions, investors can better navigate challenges such as cyber threats and operational risks. This approach addresses concerns associated with less secure solutions, while still supporting access to dynamic market opportunities.

Recognising the importance of these principles, Syz Group has developed its own solution for this problem, reflecting on the strength of traditional banking security.

Conclusion

The Bybit breach exposes critical vulnerabilities that even leading exchanges cannot ignore, serving as a wake-up call for the entire crypto ecosystem. The sophisticated tactics used in the attack, the ensuing market turmoil, and the rapid recovery efforts underscore the urgent need for robust security and proactive risk management. As digital finance continues to evolve, traditional banks provide a balanced approach to safeguarding investments, merging regulatory-grade security with accessible trading capabilities. This incident reinforces the importance of adapting to emerging threats and adopting strategies that ensure a secure digital future.

For further information

Banque Syz SA
Quai des Bergues 1
CH-1201 Geneva
T. +41 58 799 10 00
syzgroup.com

Charles-Henry Monchau, CFA, CAIA, CMT
Chief Investment Officer
charles-henry.monchau@syzgroup.com

Hashim Almadani
Intern
hashim.almadani@syzgroup.com