[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/bybit-hack-everything-you-need-to-know-about-it

Bybit Hack: Everything You Need To Know About It

On February 21, 2025, hackers infiltrated Bybit's Ethereum wallet, stealing approximately $1.5 billion in digital assets—making it the largest cryptocurrency heist in history. Despite the scale of the breach, Bybit's swift and transparent response helped maintain market stability, preventing major price volatility.

But how did the attack happen? Who was behind it? And could Bybit face a fate similar to that of FTX? This article provides a comprehensive overview of the Bybit exchange hack, including key details, potential implications, and the latest updates on the situation.

Hackers Steal $1.5 Billion From Bybit In Biggest-Ever Crypto Heist

On February 21, 2025, Bybit, a leading cryptocurrency exchange, suffered a massive security breach, losing over $1.4 billion in digital assets. This incident now stands as the largest cryptocurrency theft in history. According to blockchain security firm Cyvers, the stolen funds from this attack account for more than 60% of all crypto-related thefts by value in 2024.

On the evening of February 21, several on-chain analysts and researchers raised alarms on social media, reporting that Bybit's cold wallet had transferred a large amount of ETH and stETH—worth approximately $1.47 billion—to an unknown hot wallet.

Shortly after, Bybit CEO Ben Zhou confirmed the breach. He revealed that hackers managed to forge multiple signatures, allowing them to gain control of a specific ETH cold wallet authorized by Bybit. The attackers then transferred all the ETH stored in the wallet to an unidentified address.

> Bybit ETH multisig cold wallet just made a transfer to our warm wallet about 1 hr ago. It appears that this specific transaction was musked, all the signers saw the musked UI which showed the correct address and the URL was from @safe . However the signing message was to change...

> — Ben Zhou (@benbybit) February 21, 2025

At the time of the attack, Bybit held approximately $16.2 billion in assets, meaning the stolen funds represented around 9% of its total holdings.

The breach initially triggered panic within the crypto community, raising concerns over the exchange's solvency. However, Ben Zhou reassured users via social media. "Please rest assured that all other cold wallets are secure," Ben Zhou, CEO of Bybit, posted on X. "All withdrawals are NORMAL."He also emphasized that even if the stolen assets could not be recovered, Bybit remained financially stable. "All client assets are backed 1-to-1, and we can cover the losses," he stated.

Despite these reassurances, the breach immediately triggered a rush of withdrawals from Bybit as users feared potential insolvency.

Before this incident, the largest crypto hack on record was the Ronin Network attack in March 2022. Ronin, an Ethereum sidechain built for the Axie Infinity game, was exploited for over $600 million worth of ETH and USDC. While Ronin was able to recover a portion of the stolen funds, the majority remained unrecovered.

That attack was attributed to the Lazarus Group, a hacker organization allegedly linked to the North Korean government. In 2024 alone, Lazarus was responsible for stealing approximately $1.34 billion worth of cryptocurrencies, underscoring the growing threat of sophisticated cyberattacks in the digital asset space.

Who is the Hacker?

Who's the hacker? While Bybit and other authorities have yet to officially identify the perpetrators, security researchers from Elliptic and Arkham Intelligence have reportedly linked the attack to the North Korean hacker group Lazarus.

Prominent blockchain investigator ZachBXT also attributed the heist to Lazarus.

Arkham Intelligence later confirmed on X that ZachBXT had submitted "definitive proof" implicating the group.

> BREAKING: BYBIT $1 BILLION HACK BOUNTY SOLVED BY ZACHXBT
>
> At 19:09 UTC today, @zachxbt submitted definitive proof that this attack on Bybit was performed by the LAZARUS GROUP.
>
> His submission included a detailed analysis of test transactions and connected wallets used ahead of… https://t.co/O43qD2CM2U pic.twitter.com/jtQPtXl0C5
>
> — Arkham (@arkham) February 21, 2025

His findings included a detailed analysis of test transactions and wallet connections leading up to the exploit, along with forensic graphs and timing analyses that traced the movement of funds.

Lazarus Group is notorious for executing high-profile cyber heists, having siphoned billions of dollars from the crypto industry over the years.

The group was also linked to the infamous Ronin Network attack in March 2022, where more than $600 million in ETH and USDC was stolen.

Despite mounting evidence from security analysts, Bybit has not yet officially confirmed the attackers' identities.

However, in a post on X, the exchange acknowledged ZachBXT's contributions, thanking him for "always keeping the space sharp" and stating that his efforts in investigating the hack "didn't go unnoticed."

Bybit Defies Odds: Bybit Responds Quickly to the Hack

Bybit's response to the hack was defined by swift action, transparency, and professionalism. CEO Ben Zhou took immediate ownership of the situation, addressing the community within 30 minutes via X and hosting a live session just an hour after the breach. The two-hour livestream provided real-time updates and in-depth explanations, ensuring that stakeholders were kept informed and reassured. Bybit's prompt and open communication helped prevent widespread panic, reinforcing trust in the exchange and setting a high benchmark for crisis management in the crypto industry.

Despite the scale of the attack, Bybit's 1:1 reserve guarantee ensured that all client assets remained fully protected. Ben Zhou reassured users that the exchange remained solvent and capable of covering the losses, emphasizing that every client asset was backed on a one-to-one basis. This financial commitment underscored Bybit's stability and dedication to user security.

In response to the attack, Bybit worked closely with regulators and law enforcement agencies, facilitating a swift and coordinated effort to address the breach. This collaboration not only reinforced the exchange's commitment to compliance but also set a precedent for stronger partnerships between the crypto industry and regulatory bodies. As investigations continue, the incident may pave the way for enhanced security measures and regulatory frameworks aimed at mitigating future threats.

Bybit also demonstrated remarkable operational resilience, efficiently processing over 350,000 withdrawal requests within 12 hours of the hack. Despite the surge in activity, all transactions were completed without significant delays, highlighting the team's expertise in managing crisis situations. The exchange quickly restored normal operations, with user activity rebounding to pre-hack levels within 24 hours. This rapid recovery reinforced client confidence and showcased Bybit's ability to maintain stability even in the face of adversity.

Bybit's handling of the breach sets a new industry standard for crisis response. The exchange transformed a potentially catastrophic event into an opportunity to demonstrate resilience, transparency, and responsibility. Beyond Bybit's operational excellence, the incident also underscores the growing maturity and unity within the crypto industry, as exchanges and stakeholders work together to strengthen security and trust in the digital asset space.

What can We Learn from Bybit Hack?

Bybit's recent security breach has sent shockwaves through the crypto industry, highlighting vulnerabilities in multi-signature cold storage solutions and underscoring the urgent need for more advanced security measures. Industry experts, including Ledger CEO Pascal Gauthier, Fireblocks, and Binance co-founder Changpeng Zhao (CZ), have weighed in on the incident, offering valuable insights into how such attacks could have been prevented and the critical steps exchanges must take to enhance the security of digital assets.

How can Crypto Exchanges Prevent from being Hacked?

Improve Transaction Transparency and Reduce Blind Signing

One of the biggest risks in crypto security is blind signing, where users and platforms approve transactions without fully understanding what they are authorizing. Ledger CEO Pascal Gauthier highlighted that such vulnerabilities could be significantly reduced with the widespread adoption of Clear Signing—a security measure that ensures users can fully verify transaction details before signing. As the global leader in self-custody solutions, securing over 20% of the world's digital assets, Ledger continues to advocate for enhanced security standards to protect both individuals and institutions from sophisticated cyber threats.

"These hacks are preventable, and enterprise-grade security is necessary for large transactions. As cryptocurrency becomes more widely adopted, scams and phishing attacks also rise. Clear Signing is the only way to securely authorize a transaction—that's why Ledger is implementing Clear Signing for the entire ecosystem, which requires support from partners to properly integrate," said Gauthier.

Rethink Multi-Sig and Move to Distributed MPC Wallets

Both CZ and Fireblocks have highlighted the security weaknesses inherent in multi-signature (multi-sig) cold storage solutions. While multi-sig remains a widely adopted method for securing digital assets, it is not without its risks—particularly if one or more signature providers are compromised.

Fireblocks advocates for a more secure alternative: Distributed Multi-Party Computation (MPC) wallets. Unlike traditional multi-sig setups, MPC wallets distribute cryptographic key fragments across multiple independent parties, ensuring that no single entity has full control over the private key. This significantly reduces the risk of a single point of failure leading to a breach, offering a more resilient defense against sophisticated cyberattacks. Fireblocks itself has implemented MPC technology, reinforcing its belief that this approach provides superior signing security for digital asset custody.

Enforce Enterprise Governance and Approval Flows

Ledger and Fireblocks emphasize the critical need for enterprise-level security governance, outlining key measures that can significantly reduce the risk of breaches:

Multi-level transaction approvals – Implementing a tiered approval process, such as requiring CFO authorization for high-value transactions, adds an extra layer of oversight.

Whitelisting trusted wallet addresses – Restricting fund transfers to pre-approved addresses helps

prevent assets from being sent to malicious actors.

Hardware-based verification – Enforcing transaction security through hardware-level authentication strengthens protection beyond software-based defenses.

Beyond these measures, enterprises must adopt B2B custody solutions tailored for institutional security needs. Pascal Gauthier further highlighted that security governance should extend beyond transaction signing. Organizations must enforce off-chain governance frameworks to prevent internal vulnerabilities from escalating into catastrophic financial losses.

Secure Exchange Assets with Off-Exchange Trading Solutions

Another crucial recommendation is minimizing reliance on exchange-controlled wallets by adopting off-exchange trading solutions. These models enable institutions to trade securely while maintaining funds in segregated collateral accounts, rather than storing assets in hot wallets that are more susceptible to breaches. This approach enhances security by reducing exposure to exchange-related risks while ensuring liquidity for trading activities.

What Traders can Learn from Bybit Hack?

The Bybit hack highlights the critical importance of self-custody and implementing proper security practices to protect individual users. Here are key steps you can take to safeguard your assets:

- Use wallets with clear transaction visibility to avoid blind signing and ensure you fully understand what you're authorizing.
- Verify every transaction before approval, particularly when interacting with smart contracts, to prevent unauthorized actions.
- Diversify your custody solutions by combining self-custody options, hardware wallets, and institutional-grade security to minimize risk.
- Stay informed about security best practices and keep up to date with the measures exchanges are taking to protect user funds.
- Properly manage backups and store seed phrases in secure, offline locations to avoid exposure to online threats.

By following these practices, you can significantly reduce your vulnerability and take greater control of your digital asset security.

Conclusion

In February 2025, Bybit, a prominent cryptocurrency exchange, was targeted in a cyberattack that resulted in the theft of approximately $1.5 billion worth of digital assets—making it one of the largest heists in the history of the crypto industry. This breach served as a stark wake-up call for the entire sector, underscoring the urgent need for exchanges and custodial providers to bolster their security measures and better protect user funds.

\ Trade On BTCC With 10 FREE USDT! /

Register Now To Earn Rewards Up To 10,055 USDT

About BTCC

Fully licensed and regulated in the **U.S., Canada, and Europe**, BTCC is a well-known cryptocurrency exchange, boasting an impeccable security track record since its establishment in 2011, with **zero reported hacks or breaches**. BTCC platform provides a diverse range of trading features, including **demo trading, crypto copy trading, spot trading,** as well as**crypto futures trading** with a leverage of up to **500x**. If you want to engage in cryptocurrency trading, you can start by signing up for BTCC.

BTCC is among the best and safest platforms to trade cryptos in the world. The reasons why we introduce BTCC for you summarize as below:

Industry-leading security

BTCC attaches great importance on security. Since founded in 2011, BTCC has never been hacked or been a victim of any other kind of successful malicious attack, which fully illustrates its security capabilities. Through measures like segregation of assets, 1:1 storage of users' assets, money laundering prevention and identity authentication and no collateralising tokens for loans, BTCC enjoys good reputation in asset security.

High Liquidity & Volume

BTCC is ranked top 10 by trading volume on both CoinMarketCap and CoinGecko, the world's two largest crypto information platforms. BTCC prides itself on providing crypto futures trading services to users worldwide with market-leading liquidity, offering perpetual futures on over 300 cryptocurrencies, including BTC, ETH, DOGE, LTC, SOL, XRP, SHIB, etc.

Extremely low fees

Charging high fees means less return for investors. Compared with other major exchanges, BTCC only charges 0.06% for both takers and makers, which are far below the industry average. According

to the largest and most recent empirical study on crypto exchange trading fees, the average spot trading taker fee is 0.2294% and the maker fee is 0.1854%.

High and rich bonus

BTCC holds all kinds of campaigns where investors can participate to win exciting bonus. For example, new users can get rewards up to 10,055 USDT coupon through completing relevant missions, like registration, identity verification, first deposits, cumulative futures trading volume, etc. Besides, becoming VIP also can enjoy rewards like VIP-exclusive perks, including discounts on trading fees, access to exclusive campaigns, BTCC merch, priority customer support, fast withdrawal, and many more.

Excellent customer service

BTCC also gains great reputation in terms of customer support. If you are confused or have problem in the process of trading currencies, you can obtain customer support via email and live chat, BTCC offers 24/7 online customer service for you.

You May Like:

[BTCC Exchange Review 2025]

[8 Types of Crypto Scams to Avoid in 2025]

[Best Non KYC Crypto Exchanges In February 2025]

[Understanding KYC In Crypto: How To Complete KYC On BTCC]

[What Is Spot Trading In Crypto & How To Start Crypto Spot Trading On BTCC: A Comprehensive Guide For 2025]

[A Beginner’s Guide: What Is Copy Trading & How To Start Copy Trading On BTCC]

[Best Crypto Exchanges Australia 2025]

[Pi’s Open Mainnet Goes Live On February 20: Everything You Need To Know About It]

[How To Buy Pi Network (PI): A Comprehensive Guide In 2025]

[Pi Network Mainnet Launch Now Goes Live: Pi Network Price Prediction Post Mainnet Launch]

[Pi Network (PI) Price Prediction: Will Pi Coin Reach $500 After Major Exchange Listings?]

[How to Sell Pi Coin in Canada: A Complete Guide for 2025]

[What Is Pi Network Dog (PIDOG) Meme Coin: PIDOG Rides High As PI Mainnet Introduces It In First 20 Apps]

[Mutuum Finance (MUTM) Coin Review & Analysis: Next 100x Gem?]

What Is DeepSeek? Everything You Need To Know About It

Official TRUMP ($TRUMP) Price Prediction: Next 100X Trump-Themed Meme Coin?

Melania Meme ($MELANIA) Coin Review & Analysis: Melania Trump launches Her Own Meme Coin $MELANIA

BeerBear (BEAR) Meme Coin Review & Analysis: 100X Meme Coin On Solana?

The Last Dwarfs ($TLD) Meme Coin Review & Analysis: Next 100X Meme Coin?

BTCC vs. Kraken

BTCC vs. Coinbase vs. Crypto.com

Compare BTCC vs. Binance: Which is a Better Choice for Canadian Traders in 2025?

Compare BTCC vs. BitMart 2024: Which is a Better Choice for Your Demand

Compare BTCC vs Gate.io: Which is Best in 2025

BTCC vs CoinJar: Which One is Better?

BTCC vs. MEXC: A Complete Comparison In 2025

BTCC vs. Bitbuy

BTCC vs. NDAX: which is a better choice for crypto trading in Canada?