Gate Research

How Crypto Hacks from Mt. Gox to Bybit Reshaped the Market

Abstract

- In 2025, Bybit exchange suffered the largest hack in crypto history, with losses exceeding $1.4 billion. This attack triggered severe market turbulence, exposed security vulnerabilities in centralized exchanges, and accelerated the trend toward decentralization.
- While DeFi projects face frequent attacks, centralized exchanges (CEX) suffer the largest losses per incident. Money laundering methods have grown increasingly sophisticated, with cross-chain transfers emerging as the primary method.
- Hacking incidents consistently trigger price fluctuations in mainstream cryptocurrencies. The Mt. Gox incident caused Bitcoin to plunge 11.72% in a single day, while the Bybit attack led to BTC and ETH dropping 4.44% and 7.84% respectively.
- Following hacks, market sentiment deteriorates and affected project tokens collapse. After the Ronin attack, its token RON fell 20% within 24 hours.
- These attacks spark severe market volatility and trigger panic selling. Bybit saw $5.7 billion in net outflows within two days of the incident, while Ronin Bridge's ecosystem TVL dropped 75.29% within two months. Trust in CEXs has eroded, pushing users toward decentralized wallets and DEXs.
- The attacks create ecosystem-wide ripple effects: The Bybit incident drove USDe down to $0.96 through panic selling, while Chainlink oracle price discrepancies triggered $22 million in Aave liquidations. The Ronin Bridge attack led to capital flight that significantly shrank its DeFi ecosystem.
- The industry must build a three-pillar security system combining "Technology- Regulation-Users". This includes technical upgrades (MPC wallets, zero-knowledge proofs), regulatory compliance (KYC/AML), operational transparency (proof of reserves, insurance), user education (security awareness, bug bounties), and ecosystem collaboration (cross-chain security alliance, open-source technology).
- Major hacks—from Mt. Gox to Poly Network, Ronin Bridge, and Bybit—have driven industry evolution. The crypto sector grows stronger through these challenges, working toward a secure, transparent, and sustainable future through collaborative efforts in technology, regulation, and community.

Keywords:

Gate Research, Mt.Gox, Poly Network, Ronin

Gate Research: How Crypto Hacks from Mt. Gox to Bybit Reshaped the Market

1 Introduction

On February 21, 2025, cryptocurrency exchange Bybit suffered the largest security breach in history, with hackers stealing approximately $1.4 billion worth of assets from its Ethereum cold wallet. This attack not only surpassed previous records set by Poly Network ($611 million in 2021) and Ronin Network ($620 million in 2022) but also triggered severe market turbulence: Bitcoin, Ethereum, and other mainstream assets experienced varying degrees of decline, with the total cryptocurrency market cap evaporating over $100 billion before finally stabilizing at $96,500 and $2,700 respectively two days later. The Bybit hack resulted from an exploitation of platform vulnerabilities, with hackers successfully stealing over 400,000 ETH and 90,000 stETH, totaling more than $1.4 billion.

48 hours later, cross-chain protocol Infini also fell victim to a hack, with attackers exploiting a contract vulnerability to steal 49.5 million USDC, which was subsequently converted to DAI. Although these two incidents were not carried out by the same hacker group, their consecutive occurrence further demonstrates the persistent nature of security threats. These hacking incidents not only resulted in massive financial losses but also exposed security vulnerabilities in the cryptocurrency industry's infrastructure, posing a threat to market stability. From Mt.Gox in 2014 to the series of cross-chain bridge attacks in 2021-2023, and now the Bybit incident in 2025, hacking attacks have intensified, presenting ongoing security challenges for the industry.

This research paper will delve into the current state of hacking attacks and, based on several high-impact cryptocurrency hacking incidents, provide a detailed analysis of their multiple effects on the crypto market, covering both direct and indirect impacts, including market volatility and changes in investor behavior. The article aims to warn of potential further risks in the crypto market and explore future countermeasures.

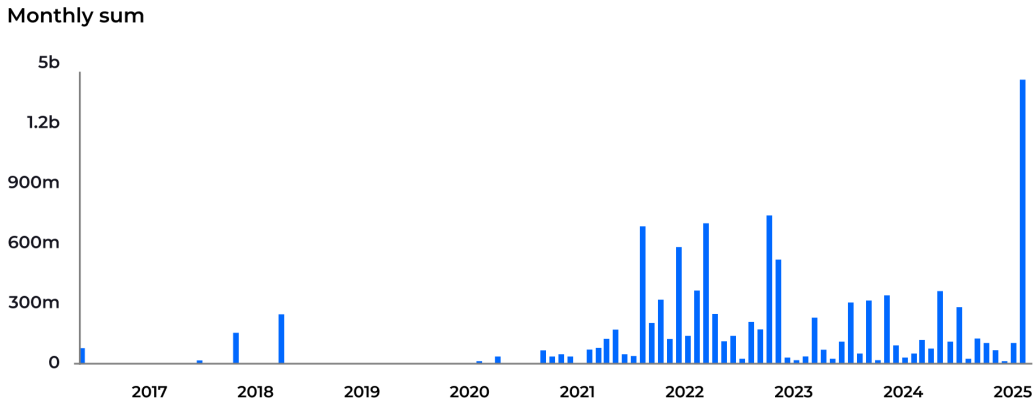
2 Current State of Crypto Market Hacking Attacks

2.1 Crypto Market Security Alert: Frequent DeFi Attacks, Heavy CEX Losses

The decentralized nature of the crypto market makes it vulnerable to attacks. Recent hacking incidents have not only caused massive losses for market participants but have also severely impacted market trust and security. According to DeFiLlama data, from 2017 to February 2025, losses from hacking attacks have grown exponentially, with total losses reaching $10.62 billion,

and this trend continues to intensify, seriously threatening the market's long-term development.

Figure 1: Crypto Market Losses from Hacking Attacks 2017 - 2025



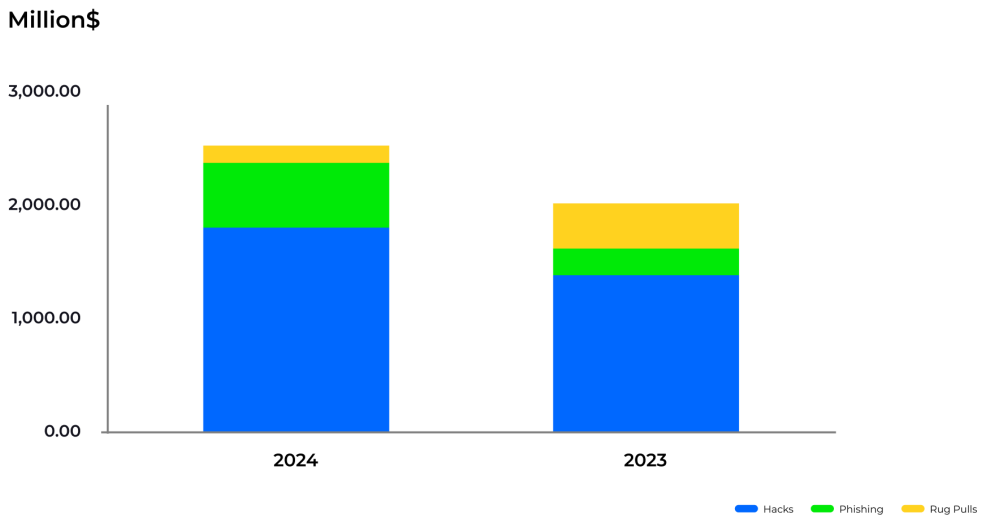
Gate Research, Data from: DefiLlama, 2025.2.21

Gate Research

Crypto market losses from hacking attacks reached $1.272 billion in 2024. In just the first two months of 2025, these losses have already hit $1.511 billion—surpassing the entire previous year's total. While DeFiLlama tracks hack-related losses, security incidents in the crypto market extend beyond just hacking attacks. Gate Research's report "Gate Research: From Hacking Attacks to Regulatory Reflection – Analysis of Cryptocurrency Security Status in 2024" categorizes security incidents into three main types: Hacks, Rug Pulls, and Phishing.

According to monitoring data from security audit company Beosin's Alert platform, total losses in the Web3 space due to hacking attacks, phishing scams, and project rug pulls reached $2.513 billion in 2024. Among these, losses from hacking attacks and phishing scams increased significantly compared to 2023, with phishing scam losses surging by 140.66%. In contrast, losses from project rug pulls decreased by approximately 61.94%.

Figure 2: Losses from Different Types of Crypto Asset Security Incidents 2023-2024

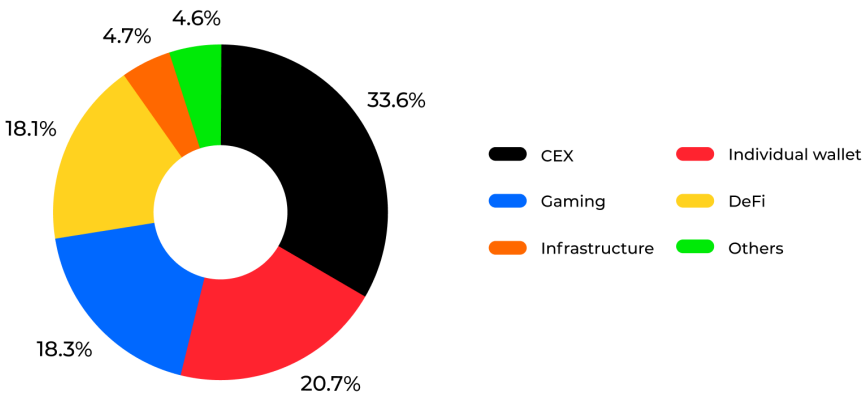


Gate Research, Data from: Footprint Analytics，@Beosin

Gate Research

Analyzing the types of projects attacked reveals that while hacks target various projects, DeFi platforms face the highest frequency of attacks at 50.7% of all incidents. Yet DeFi projects account for only 18.1% of total losses, placing them fourth in terms of value lost. Centralized exchanges (CEX), despite experiencing just 6.8% of attacks, suffer 33.6% of all losses, making them the most severely impacted sector. **This pattern shows that while DeFi projects face more frequent attacks, CEX security breaches result in far greater losses per incident, highlighting exchange security as the Web3 ecosystem's primary challenge.**

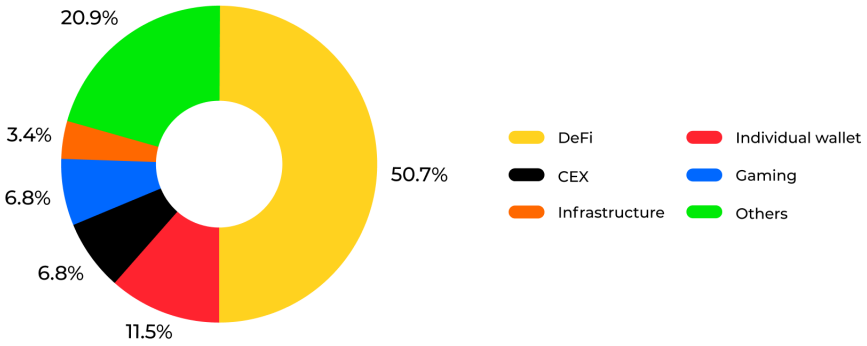
Figure 3: Market Share of Loss Amount by Project Type in 2024



Gate Research, Data from: Footprint Analytics，@Beosin

Gate Research

Figure 4: Market Share of Loss Projects by Project Type in 2024



Gate Research, Data from: Footprint Analytics，@Beosin

Gate Research

Data from early 2025 further confirms this trend. According to DeFiLlama's compilation of hacking incidents in 2025 (incomplete statistics), while DeFi projects accounted for half of all incidents, CEX attacks resulted in losses of up to $1.485 billion, representing 98% of total losses. This data highlights the security vulnerabilities in centralized exchanges and the massive impact of hacking attacks on the market.

Figure 5: Hacking Incidents in 2025 (as of February 21, 2025)

Name	Loss Amount	Category	Date	Attack Method	Related Link
Bybit	$1.4 billion	CEX	2025-02-21	Wallet Theft	https://x.com/benbybit/status/1892963530422505586
Cardex	$400,000	GameFi	2025-02-22	Security Vulnerability Attack	https://x.com/0xCygaar/status/1891948692204368122
Four.Meme	$183,000	Memecoin launch platform	2025-02-23	Business Logic Vulnerability	https://x.com/peckshieldalert/status/1889210001220423765
zkLend	$9.55 million	DeFi	2025-02-24	Smart Contract Vulnerability	https://x.com/zkLend/status/1889515118368829559
Ionic Protocol	$4 million	DeFi	2025-02-25	Social Engineering	https://x.com/CyversAlerts/status/1886829735130407065
DogWif Tools	$10 million	Meme	2025-02-26	Malicious Software Deployment	https://x.com/kookcapitalllc/status/1884285558635323437
Phemex	$85 million	CEX	2025-02-27	Hot Wallet Attack	https://ktromedia.com/152490/
Orange Finance	$787,000	DeFi	2025-02-28	Multi-Signature Configuration Error	https://x.com/0xorangefinance/status/1876863611458801890
Moby	$2.5 million	DeFi	2025-03-01	Hacker Modifies	https://x.com/Moby_trade/status/1877096336140677458
MoonHacker	$300,000	DeFi	2025-03-02	Contract Flash Loan Attack	https://x.com/dedaub/status/1874838342485102852

Gate Research, Data from: DefiLlama, 2025.2.21

Gate Research

2.2 Money Laundering Methods by Hackers Intensify Market Instability and Erode Confidence

Frequent hacking incidents not only cause direct economic losses but also severely impact the security and stability of the crypto market. The substantial losses suffered by centralized exchanges (CEX) expose vulnerabilities in asset custody and security management, amplifying market volatility and weakening investor confidence.

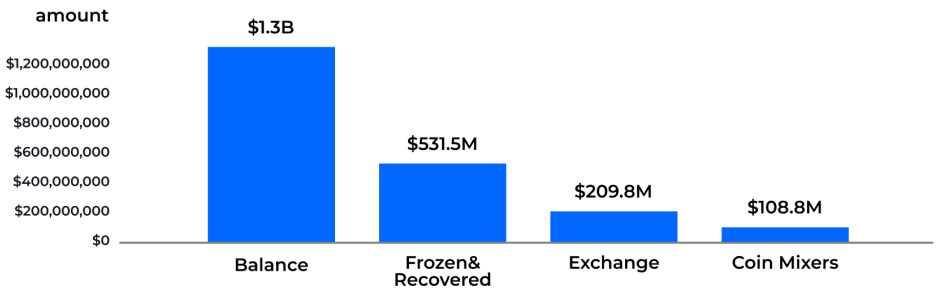
After stealing large sums, hackers use sophisticated money laundering techniques to hide their tracks and avoid detection. They leverage decentralized mixers, cross-chain bridges, OTC transactions, and multi-chain transfers to create an effective laundering network. This makes it difficult for law enforcement and project teams to track the funds, while threatening market liquidity and regulatory compliance.

Currently, after stealing cryptocurrencies, hackers employ the following methods to obscure fund sources and eventually cash out:

1. Converting to highly liquid tokens (such as ETH, USDT);
2. Dispersing funds across multiple wallets to reduce single address exposure risk;
3. Using mixers or blending services to break fund tracking paths;
4. Cross-chain transfers and fund splitting through DEX to increase tracking difficulty;
5. Converting to stablecoins or other anonymous assets to enhance anonymity;
6. Cashing out through OTC or fiat channels to ultimately legitimize funds.

Based on these laundering techniques, hackers' tools generally include mixers/tumblers, cross-chain bridges and decentralized finance platforms (DEX/DeFi), over-the-counter (OTC) and centralized exchanges (CEX), privacy coin conversions (such as Monero, Zcash), NFT transactions, and other emerging tools. Despite hackers using various laundering methods, many stolen funds remain scattered across hacker-controlled addresses. According to Beosin's data, of the total funds stolen in 2024, approximately $1.312 billion remains in hacker addresses (including cross-chain transfers and multi-wallet dispersion), accounting for 52.20% of total stolen funds. Some of these funds have been split using cross-chain tools.

Figure 6: Flow of Stolen Funds in 2024

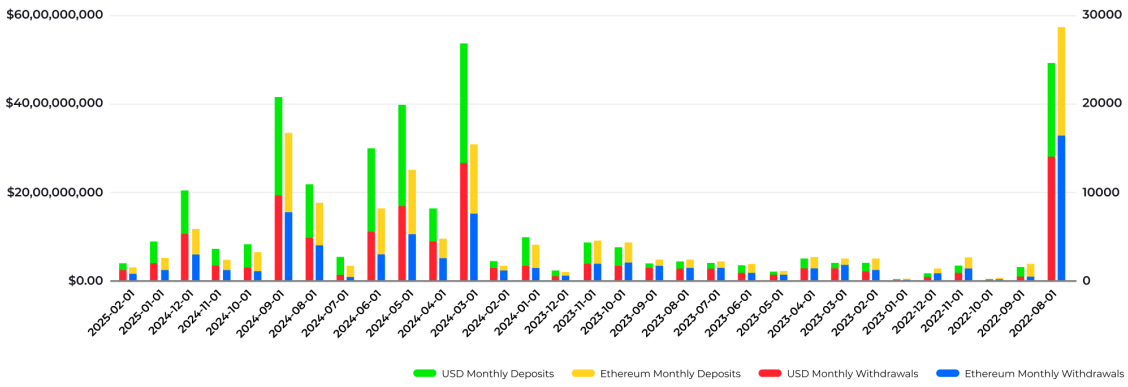


Gate Research, Data from: Footprint Analytics，@Beosin

Gate Research

Since the U.S. OFAC sanctioned Tornado Cash in August 2022, the amount of stolen funds entering this mixer has dramatically decreased. As shown in the graph below, Tornado Cash's inflow and outflow volumes experienced a cliff-like drop from September 2022, with only a slight recovery by March 2024. According to Beosin's data, only about $109 million in stolen funds were transferred to mixers in 2024, accounting for 4.34% of total stolen funds. In comparison, this ratio was 23.6% and 38.7% in 2023 and 2022 respectively, showing a significant downward trend.

Figure 7: Tornado Cash Inflow and Outflow Amounts Over the Past Three Years



Gate Research, Data from: Dune，@legionx

Gate Research

Overall, hackers are making fund tracking increasingly difficult through multiple cross-chain transfers, mixer conversions, and fund splitting. This poses serious challenges for market compliance. Money laundering by hackers is not just a problem of individual project losses, but a systemic risk affecting the entire market's security and stability, while also presenting new

challenges for regulatory authorities and project teams.

3 Analysis of Crypto Market Impact from Hacking Incidents

Hacking incidents impact the crypto market in multiple ways. They cause direct financial losses while damaging market confidence, prompt regulatory action, drive technological innovation, and reshape the industry landscape. These attacks typically trigger investor panic, increase market volatility, and lead governments to impose stricter cryptocurrency regulations.

3.1 Direct Impact: Massive Financial Losses and Widening Victim Base

In recent years, frequent hacking incidents have resulted in tens of billions of dollars in losses. From the Mt. Gox exchange incident in 2014 to the Bybit incident in 2025, single attacks often result in hundreds of millions of dollars in losses. Among these, the North Korean hacker group Lazarus Group is one of the most active hacking groups in the crypto industry, launching multiple attacks over the past few years targeting exchanges, cross-chain bridges, DeFi protocols, and personal wallets, with cumulative stolen funds exceeding several billion dollars. Notably, the scale of funds stolen by North Korean hackers from crypto platforms may be even larger than known statistics indicate.

Figure 8: Number of North Korean Hacker Attacks and Amount Stolen Over the Years

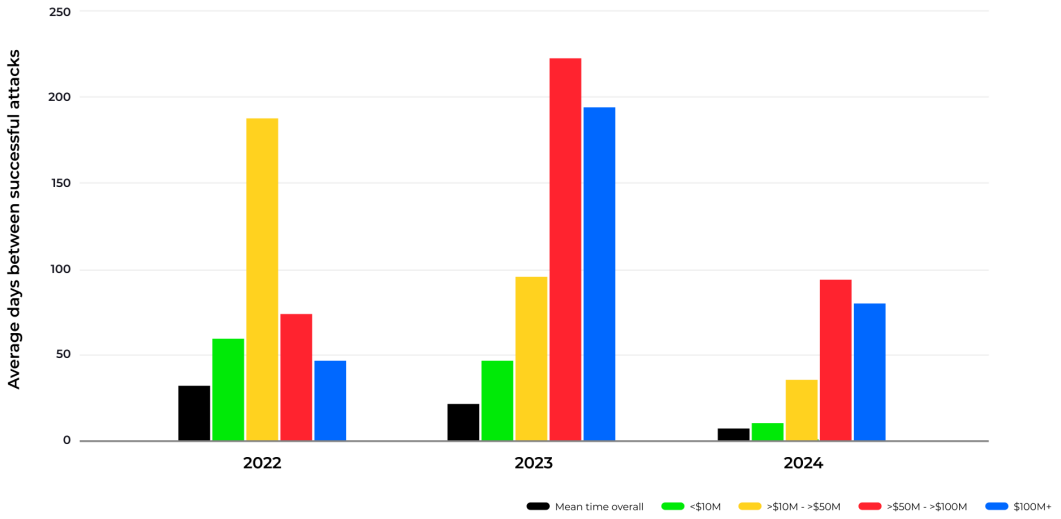
Year	Number of Attacks	Amount Stolen
2016	1	$2 million
2017	5	$29 million
2018	10	$522 million
2019	9	$271 million
2020	4	$300 million
2021	7	$506 million
2022	15	$1.1 billion
2023	20	$660 million
2024	47	$1.34 billion (102.88% increase)

Gate Research, Data from: chainalysis

Gate Research

The scope of North Korea's cryptocurrency attacks is gradually expanding. In 2024, North Korean hacker groups launched more frequent attacks targeting assets worth $50-100 million and over $100 million compared to 2023, indicating significantly improved attack efficiency against high-value targets, which will result in losses for more users and institutions. Meanwhile, the number of small-scale attacks (such as the $10,000 level) is also rising, showing that regular investors can equally become targets, as North Korean hackers' strategy extends to a broader target demographic. Furthermore, the density of North Korean hacker attacks is increasing - although some attacks involve smaller amounts, their frequency and coverage have expanded significantly.

Figure 9: Distribution of North Korean Hackers' Crypto Market Attack Scales Over the Years



Gate Research, Data from: chainalysis

Gate Research

3.2 Indirect Impact: Market Confidence and Investor Behavior

Following a hacking incident, the market typically reacts quickly, with related assets (such as BTC, ETH, and the tokens of the attacked project) often experiencing short-term declines. Market sentiment indices generally decrease after such events, though the extent of the impact depends on the scale and scope of the hack.

We analyzed four of the top five largest cryptocurrency hacking incidents in recent years in terms of stolen funds and examined their impact on BTC and ETH prices. The data shows that while BTC often experiences some degree of decline following a hacking incident, the timing and magnitude of the drop can vary. In some cases, the market reacts immediately on the day of the attack, while in others, the decline occurs later as the incident escalates and a crisis of trust spreads. The following section will provide an in-depth analysis of the indirect impact of these four hacking incidents on the cryptocurrency market:

Figure 10: Details of Four Major Cryptocurrency Security Incidents Involving Large-Scale Hacks

Date	Target	Amount Stolen	Attack Method
February 24, 2014	Mt. Gox (largest Bitcoin exchange at the time)	Approximately 850,000 BTC (worth $470M at the time, about $80B at current prices)	Exchange private key leak + Transaction Malleability vulnerability
August 10, 2021	Poly Network	Approximately $610M	Private key leak / Multi-chain cross-chain contract vulnerability
March 23, 2022	Ronin Bridge (Axie Infinity sidechain)	$624M (173,600 ETH + 25.5M USDC)	Private key leak (social engineering attack)
February 21, 2025	Bybit ETH cold wallet (centralized exchange, hypothetical case)	$1.4B (ETH and related derivative assets)	Multi-sig system vulnerability + malicious contract phishing

Gate Research

Gate Research

3.2.1 Mt. Gox Exchange Attack (2014)

Mt. Gox was once the world's largest Bitcoin exchange, handling over 70% of global Bitcoin transactions. However, on February 24, 2014, the exchange suffered a catastrophic hack, resulting in the theft of approximately 850,000 Bitcoins (valued at around $450 million then, or roughly $8 billion at current prices). This incident ultimately forced Mt. Gox to file for bankruptcy. However, this was not Mt. Gox's first security breach. As early as 2011, the exchange had already lost 25,000 Bitcoins. In March 2014, Mt. Gox announced that it had recovered about 200,000 Bitcoins, but 650,000 coins remained missing. To this day, the true circumstances behind the Mt. Gox incident remain unresolved. While theories include insider theft, external hacking, and internal collusion, the core issue remains unsolved —most stolen Bitcoins have yet to be fully recovered.

3.2.1.1 Price Drop and Market Panic

Following the incident, BTC dropped 11.72% in a single day. Within two months after the event, BTC hit a low of $340 on April 11, marking a 36% decline. Market sentiment experienced significant volatility in the short term, and some investors chose to sell their holdings to mitigate potential risks. However, the actual impact of this panic-induced sell-off may have been overstated.

Figure 11: BTC Price Movement Before and After the Mt. Gox Attack

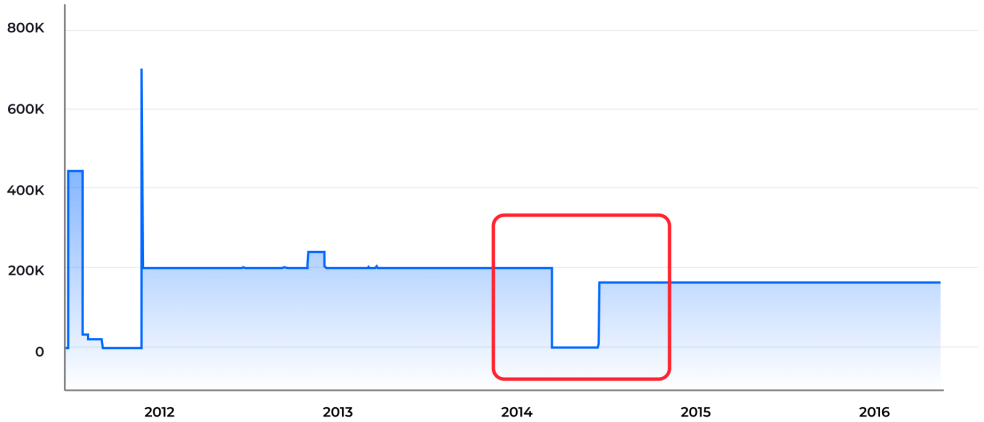
Gate Research, Data from: Gate.io

Gate Research

3.2.1.2 Liquidity Crisis and Fund Movements

At the time of the Mt. Gox incident, the global macroeconomic environment was unstable. The U.S. Federal Reserve's interest rate policies and CPI data had already influenced the cryptocurrency market. During this period, the Fed's quantitative easing measures had led to a weakening U.S. dollar, prompting some investors to turn to cryptocurrencies as a hedge for asset preservation and growth. However, the Mt. Gox attack severely damaged investor confidence in cryptocurrencies. On-chain data analysis revealed abnormal Bitcoin outflows before Mt. Gox halted withdrawals. Some major holders and sensitive investors moved their funds early, further destabilizing the market. Subsequently, the exchange suspended all withdrawals, Bitcoin liquidity plummeted, and the market briefly came to a standstill.

Figure 12: Mt. Gox BTC Holdings from 2012 to 2016



Gate Research, Data from: intel.arkm

Gate Research

3.2.1.3 Collapse of Trust and Industry Image Damage

The impact of this hack was profound, causing not only sharp Bitcoin price fluctuations but also severely weakening trust in the global cryptocurrency community. The incident dealt a long-term blow to investor confidence, driving trust levels within the crypto ecosystem to an all-time low. Many investors began re-evaluating the security and reliability of cryptocurrencies. The Mt. Gox event became one of the most notorious security incidents in the crypto ecosystem, leaving a lasting shadow over the perceived risks of digital asset exchanges.

Mainstream media widely portrayed the Mt. Gox incident as a symbol of the cryptocurrency industry's "immaturity" and "high risk," further delaying institutional investor entry into the space. Some traditional investors developed a hardened perception of cryptocurrencies, associating them with terms like "hacking" and "fraud," damaging the industry's overall image and growth potential.

3.2.1.4 Legal Action and Regulatory Intervention

Following the incident, affected users and investors filed numerous lawsuits seeking compensation. In 2015, former CEO Mark Karpeles was arrested and faced multiple charges. Although some charges were ultimately dropped, the legal actions significantly accelerated regulatory intervention in the crypto market. Japanese authorities and the Financial Services Agency (FSA) conducted an in-depth investigation into the Mt. Gox incident to uncover the reasons behind the lost Bitcoin and identify those responsible. These investigations revealed severe negligence by the platform's management in handling user funds and security measures. The collapse of Mt. Gox became a pivotal moment for regulatory bodies, prompting improvements in cryptocurrency exchange management regulations. This incident played a key role in shaping global crypto regulatory frameworks.

3.2.1.5 Follow-Up Developments and Impact

The Mt. Gox incident not only sounded the alarm on security risks but also accelerated the industry's move toward standardization. On the one hand, it encouraged investors to emphasize exchange security, prompting platforms to strengthen security technologies and management practices. The painful lessons from Mt. Gox led the entire industry to re-evaluate exchange security and asset custody mechanisms, driving the adoption of security technologies such as multi-signature wallets and proof-of-reserve systems.

On the other hand, the event attracted heightened regulatory attention, accelerating the de-

velopment of cryptocurrency regulatory policies. After the incident, the Japanese government quickly enacted the Payment Services Act, requiring all cryptocurrency exchanges to register and comply with financial regulations. Other countries followed suit, strengthening their regulatory frameworks accordingly.

In 2024, Mt. Gox announced that it would begin repaying BTC and BCH to affected investors. Bitcoin prices fluctuated following this announcement, triggering short-term panic selling. Between May 28 and July 5, Bitcoin prices fell from a high of $70,000 to below $54,000, marking a 22% drop. Despite market volatility, the announcement of cash repayments brought renewed hope to affected investors, signifying tangible progress in resolving this long-standing issue.

3.2.2 Poly Network Attack (2021)

Poly Network is a cross-chain organization jointly initiated by the Neo, Ontology, and Switcheo foundations, with Distributed Technology serving as the technical provider. On August 10, 2021, Poly Network experienced an unprecedented hacking attack resulting in approximately $612 million losses. The stolen assets spanned multiple ecosystems, including Ethereum, Binance Smart Chain (BSC), and Polygon. The attacker exploited an invalid transaction on the source chain, which was mistakenly included in the Alliance Chain’ s Merkle tree via a relay system. The hacker then manipulated keeper permissions on the target chain, ultimately unlocking and transferring assets across multiple public blockchains. This incident marked the largest DeFi hack at the time and drew widespread attention to cross-chain interoperability security. Following the attack, the hacker returned approximately $258 million in funds, but roughly $342 million remained unrecovered. The incident sparked speculation that the attacker may have acted with “white hat”intentions, possibly aiming to expose Poly Network’s security vulnerabilities.

3.2.2.1 Market Confidence and User Losses

After the Poly Network attack, Bitcoin experienced a daily decline of 1.47%, while the overall sentiment in the mainstream crypto market remained stable. The Ethereum ecosystem, which was directly affected, recorded a relatively minor 0.66% drop, showing limited volatility.

Figure 13: BTC Price Movement Before and After the Poly Network Attack

Gate Research, Data from: Gate.io

Gate Research

Figure 14: ETH Price Movement Before and After the Poly Network Attack

Gate Research, Data from: Gate.io

Gate Research

However, the users most severely impacted were those involved in yield farming through the cross-chain aggregator O3 Swap. Since O3 Swap’s cross-chain functionality relied on Poly Network, the platform suspended its cross-chain-related services following the attack. Before the incident, O3 Swap’s stablecoin pools on networks such as Polygon offered an annualized yield exceeding 20%, while some short-term single-asset pools delivered annualized returns in the hundreds of percent. These high returns attracted numerous DeFi farmers. Unfortunately, after the attack, these high-yield investors suffered significant losses. According to CoinGecko data, O3 Swap’s token had reached an all-time high of $8.20 on June 20, 2021. However, following the incident, the token’s price plummeted, reflecting the market’s heightened concerns over the security of cross-chain services.

Figure 15: O3 Price Movement Before and After the Poly Network Attack

Gate Research, Data from: CoinGecko

Gate Research

3.2.2.2 Shrinking Cross-Chain Bridge Market and Changes in DeFi Ecosystem Structure

Although the overall DeFi ecosystem's total market cap showed little change throughout 2021, the Poly Network incident led to a significant decline in the market share of cross-chain bridges and related protocols. The attack occurred on August 10, yet the total value locked (TVL) across cross-chain bridges did not decline significantly until August 26. The TVL dropped from $11.53 billion on the day of the attack to a low of $2.87 billion on August 28, representing a 75% decrease —a clear reflection of growing concerns about cross-chain security.

Figure 16: Cross-Chain Bridge TVL Trend (2021-2022)

Gate Research, Data from: DefiLlama

Gate Research

In the fourth quarter of 2021, several DeFi sectors experienced noticeable shifts. Decentralized exchanges, oracles, and lending platforms saw their market caps decrease by approximately 9%, collectively losing about $1.5 billion. Conversely, yield aggregators and the insurance sector emerged as the biggest beneficiaries, as some investors shifted funds away from high-risk cross-chain protocols to safer DeFi products.

Figure 17: DeFi Sector Market Cap Changes in Q4 2021

Share Q4 2021 Market Cap Share	Category	Quarterly Change
	Total DeFi Market Cap	0.0%
49.4%	Decentralized Exchanges	-0.3%
16.9%	Oracles	-8.5%
17.4%	Lending	-4.4%
6.1%	Derivatives	-9.0%
7.5%	Yield Aggregators	64.2%
2.1%	Insurance	31.5%
0.4%	Asset Management	-36.7%
0.3%	Fixed Income	-17.1%

Gate Research, Data from: CoinGecko

Gate Research

3.2.2.3 Industry Warning and Security Reflection

The Poly Network incident exposed numerous vulnerabilities in cross-chain protocols and smart contract security, prompting the entire DeFi sector to accelerate upgrades in security audits and technical defenses. Many cross-chain projects and aggregators (such as O3 Swap) were forced to suspend related services, compelling the industry to deeply reflect and improve security measures. This incident became a significant case study in DeFi security, encouraging many cross-chain projects to enhance smart contract security in its aftermath. Several projects adopted formal verification tools (such as Certora) to prevent similar vulnerabilities. At the same time, governments and regulatory bodies increased their oversight of the DeFi sector, driving stricter enforcement of KYC, AML, and other security standards.

3.2.3 Ronin Bridge Attack (2022)

Axie Infinity operates on an Ethereum sidechain called Ronin, designed to address Ethereum's scalability issues. To enable efficient and low-cost asset transfers between Ronin and Ethereum, the platform introduced the Ronin Bridge, allowing users to easily transfer assets like Ether (ETH) and USDC between the two blockchains.

On March 23, 2022, attackers exploited a vulnerability in the Ronin Bridge by forging withdrawal transactions using stolen private keys. In just two transactions, the attackers stole 173,600 ETH

and 25.5 million USDC, totaling approximately $624 million. By March 29, some users noticed they could no longer withdraw ETH via the Ronin Bridge, which prompted the team to discover that attackers had drained most of the funds nearly a week earlier. In response, the team suspended the Ronin Bridge and the Katana decentralized exchange (DEX) on the sidechain. They also swiftly migrated the node infrastructure and collaborated closely with law enforcement, major crypto exchanges, and Chainalysis to track and contain the attackers.

3.2.3.1 Price Collapse of Ecosystem Tokens

Following the attack on March 23, 2022, BTC rose by 1.24% that day. However, users only realized the Ronin Bridge attack on March 29, and starting in early April, Bitcoin (BTC) entered a downward trend. However, this decline was not solely due to the Ronin Bridge attack. Several other significant events in 2022 contributed to BTC's sharp decline, such as the Terra (LUNA) collapse, which drove BTC down to $30,000, the bankruptcy of the Celsius lending platform, and the U.S. Federal Reserve's interest rate hike in September. Combined, these factors caused BTC to fall from $47,000 in April to around $18,500 by September —a total decline of nearly 60%.

Figure 18: BTC Price Movement Before and After the Ronin Bridge Attack

Gate Research, Data from: Gate.io

Gate Research

The RON token suffered a sharp decline of over 20% between March 29 and March 30, falling from $2.20 to $1.70. Market panic intensified afterward, and continuous selling pressure drove RON to a low of $1.23 within a month. From its lowest point, this marked a 43% decline. Even when measured by its closing price of $1.36, RON' s one-month post-incident decline was 39%.

Figure 19: RON Price Movement Before and After the Ronin Bridge Attack

Gate Research, Data from: Gate.io

Gate Research

Additionally, Axie Infinity’s ecosystem token AXS was also severely impacted. Following the incident, AXS fell from $52 to $45, a drop of 13%.

Figure 20: AXS Price Movement Before and After the Ronin Bridge Attack

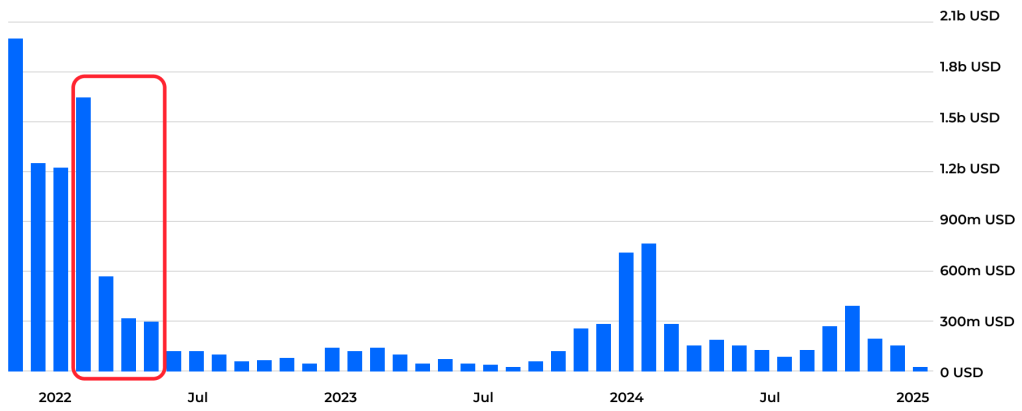
Gate Research, Data from: CoinGecko

Gate Research

3.2.3.2 Ecosystem Collapse and Capital Outflow

The impact of this attack was significant, causing not only massive financial losses but also a sharp decline in user activity and on-chain transaction volume within the Ronin ecosystem. From Ronin’s DEX monthly trading volume data, it is evident that following the March 2022 hack, related metrics dropped drastically. Combined with the crypto winter of 2023, Ronin seemed to enter a prolonged period of stagnation.

Figure 21: Ronin Chain DEX Monthly Trading Volume (2022-2025)

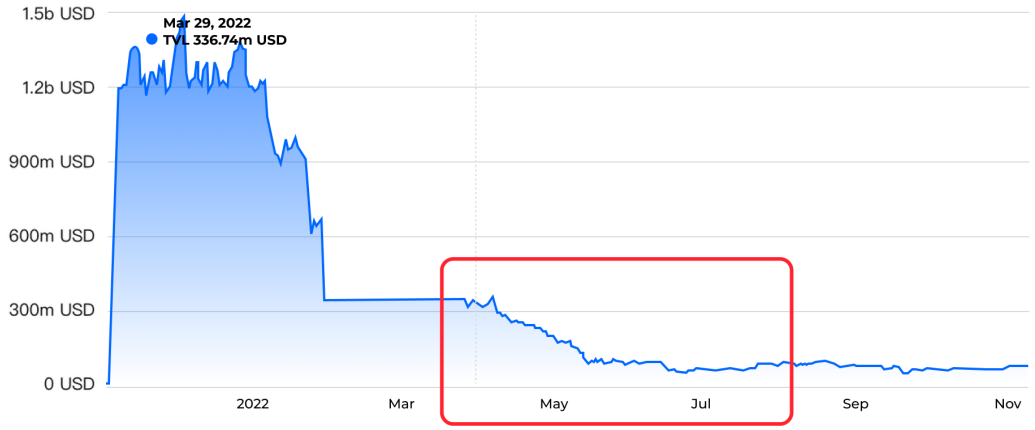


Gate Research, Data from: DefiLlama

Gate Research

The Total Value Locked (TVL) in the Ronin chain had already declined significantly in early 2022 due to the collapse of Axie Infinity's economy, the crypto market downturn, and the failure of the P2E model. However, the Ronin Bridge attack further accelerated capital outflows, causing its TVL to drop from approximately $336 million on March 29, 2022, to $83 million within two months (May 29, 2022), representing a decline of about 75.29%. Notably, since the Ronin ecosystem was primarily built around Axie Infinity with a relatively small DeFi component mainly focused on Katana DEX rather than lending protocols, this attack did not directly trigger large-scale DeFi liquidations.

Figure 22: Ronin Chain TVL Trend (2021-2022)



Gate Research, Data from: DefiLlama

Gate Research

3.2.3.3 Industry Security and Regulatory Response

The Ronin attack posed severe challenges to cross-chain protocols and their security, accelerated capital outflows, shook investor confidence, and triggered profound industry reflections on security and regulatory standards. This incident drove upgrades in Web3 security measures: to reduce single-point control risks, Ronin increased its validator nodes from 9 to 21, while the broader DeFi ecosystem began widely adopting decentralized multi-signature (MPC) and trustless verification mechanisms (such as ZK-Rollups) to enhance security. Additionally, the U.S. government intensified its crackdown on hacking activities; although OFAC's sanctions on Tornado Cash were overturned, U.S. law enforcement agencies still strengthened monitoring of wallet addresses linked to North Korea's Lazarus Group and worked with exchanges to freeze suspicious funds.

3.2.4 Bybit Exchange Attack (2025)

On February 21, 2025, the cryptocurrency exchange Bybit experienced a major hacking incident resulting in approximately $1.4 billion in losses. At 23:44 (UTC+8) that evening, Bybit's CEO confirmed the attack on Twitter, stating that around 401,000 ETH (valued at approximately $1.4 billion at the time) had been transferred to an unknown address. Bybit reported that only one ETH cold wallet was compromised, while all other wallets remained secure, and withdrawal services continued to operate normally.

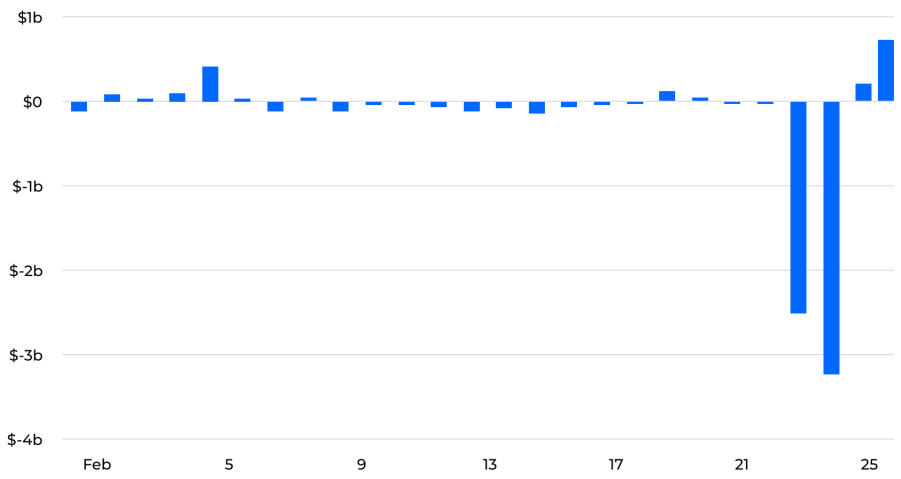
The key aspect of this attack was the hacker's exploitation of the multi-signature system. At the time, Bybit was conducting a routine transfer between its ETH cold wallet and hot wallet. During the Safe transaction signing process, the hacker leveraged a malicious contract previously deployed, successfully upgrading the transaction contract and extracting the funds. Detailed data tracking related to this incident can be found on Gate Research's Dune Analytics Dashboard. This report will focus on analyzing the attack's impact on the market.

3.2.4.1 Market Panic and Liquidity Crisis

Following the hack, market volatility surged as panic withdrawals significantly reduced Bybit's asset reserves, with investors rushing to secure their funds. Data shows that on February 22 and 23, Bybit experienced net crypto outflows of $2.5 billion and $3.2 billion, respectively. By February 24, 2025, Bybit's reserves of BTC, USDT, and USDe had dropped by 21,248 BTC, $1.76 billion in USDT, and $217.47 million in USDe. Consequently, Bybit's total asset reserves decreased from $10.8 billion before the attack to $6.5 billion, marking a total outflow of $4.3 billion. These figures highlight the severe strain on Bybit's liquidity, further intensifying concerns

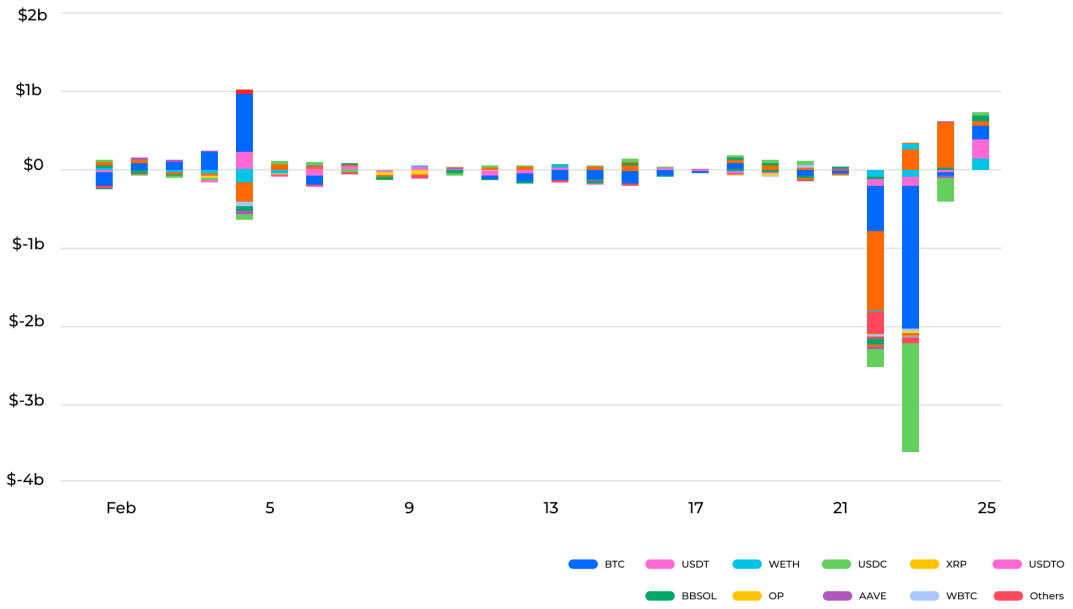
over the security of centralized exchanges.

Figure 23: Bybit USD Inflow in February 2025



Gate Research, Data from: DefiLlama

Figure 24: Bybit Token Inflows in February 2025



Gate Research, Data from: DefiLlama

3.2.4.2 Market Weakness and Accelerated Decline

On the day of the incident, Bitcoin (BTC) experienced a maximum drop of 3%, reaching a low of $94,924.1. By February 26, Bitcoin's price had fallen further to around $86,000, marking a total

decline of nearly 13% for the month. Ethereum (ETH) saw a sharper decline, with a maximum intraday drop of 6% to a low of $2,617.03. Its downward trend continued, with ETH falling from its early February closing price of $3,117 to $2,237 by February 28, resulting in a cumulative monthly decline of approximately 28%. This significant price drop not only reversed several months of gains but also underscored the market's fragile confidence.

Figure 25: BTC Price Trend Before and After the Bybit Attack

Gate Research, Data from: Gate.io

Gate Research

Figure 26: ETH Price Trend Before and After the Bybit Attack

Gate Research, Data from: Gate.io

Gate Research

Compared to mainstream cryptocurrencies like BTC and ETH, Bybit's platform token MNT suffered a more pronounced impact following the incident, with its price plunging by as much as 22.05% to a low of $0.8231.

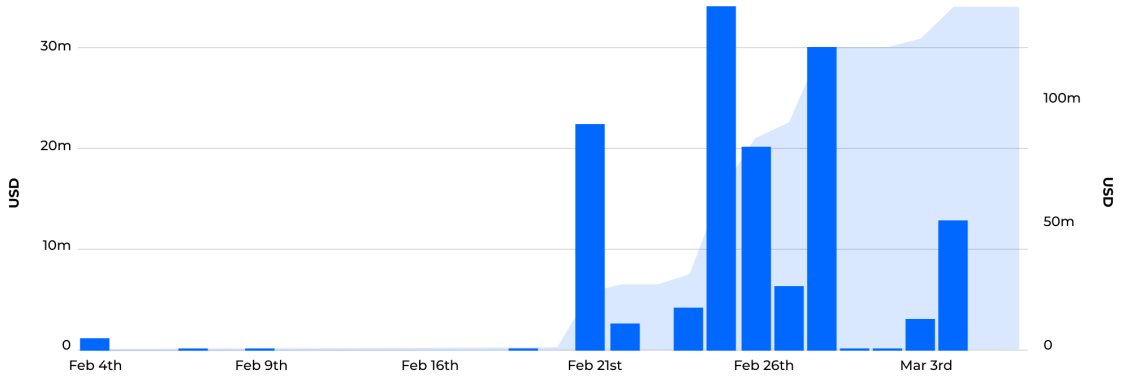
In addition, the incident had broader repercussions for Ethena, which held substantial assets on Bybit. According to Chaos Labs' founder and CEO @omeragoldberg, Bybit accounted for 21% of Ethena's asset distribution, second only to Binance's 36%. Consequently, the Bybit incident triggered a chain reaction affecting Aave, Ethena Labs, and the USDe stablecoin. Amid panic-driven sell-offs, the USDe/USDT pair on Bybit temporarily dropped to $0.96. Chainlink's USDe/USD oracle price also deviated due to heightened secondary market volatility, reaching a low of $0.977. This price deviation directly triggered the liquidation of approximately $22 million in assets on the Aave platform, exacerbating market turbulence. Overall, declining market liquidity, reduced spot demand, and intensified selling pressure contributed to broader market adjustments.

Figure 27: USDe/USD Oracle Price Before and After the Bybit Attack

Gate Research, Data from: Chainlink

Gate Research

Figure 28: AAVE V3 Ethereum Liquidations Before and After the Bybit Attack



Gate Research, Data from: Dune, @KARTOD

Gate Research

3.2.3.3 Acceleration of Decentralization Trends and Regulatory Reinforcement

Despite Bybit's assurances of its solvency, the stolen funds represented approximately 8.64%–9.28% of its total reserves, raising serious concerns about the security of centralized exchanges (CEX). This incident shattered the belief that "cold storage is absolutely secure," prompting investors to accelerate their shift toward decentralized wallets and decentralized exchanges (DEX) to mitigate risks associated with centralized fund management.

At the same time, regulatory authorities worldwide may tighten asset management requirements for CEX platforms. Countries like Japan and South Korea have already implemented stringent measures such as multi-signature wallet protocols, cold storage ratio disclosures, and third-party audits. This attack may encourage more nations to adopt similar regulations, further strengthening security standards for cryptocurrency exchanges. Additionally, shaken investor confidence may prompt the industry to deepen discussions on reserve transparency, smart contract security, and asset insurance mechanisms.

3.3 Summary

The most immediate impact of a hacking incident is the substantial financial loss. However, beyond monetary damage, such incidents have far-reaching effects on market sentiment and investor confidence. This often leads to a collapse in market trust, changes in investor behavior, and ultimately drives industry ecosystem reshaping and regulatory enhancements. From the cases discussed above, the impacts of hacking incidents on the crypto market can be summarized as follows:

3.3.1 Intense Market Volatility

- Hacking incidents frequently trigger severe market volatility. For instance, the Mt. Gox incident resulted in an 11.72% single-day drop in Bitcoin prices. After the Bybit attack, BTC and ETH experienced maximum intraday losses of 4.44% and 7.84%, respectively.
- While mainstream cryptocurrency prices are influenced by multiple factors (e.g., Terra's collapse, U.S. Federal Reserve rate hikes), hacking incidents undeniably amplify market fragility.

3.3.2 Altered Investor Behavior

- **Panic Selling:** Following hacking incidents, BTC, ETH, and related project tokens often experience rapid short-term declines, alongside deteriorating market sentiment. For example, after the Ronin attack, the RON token's price plummeted by 20% within 24 hours and fell to as low as $1.23 within a month —a 43% decrease from its pre-incident value.
- **Liquidity Risk:** Hacking incidents may force exchanges to temporarily suspend withdrawals, triggering market panic and accelerating capital outflows. Exchanges or affected DeFi platforms often face significant asset losses as users withdraw funds to mitigate risks. For example, Bybit experienced net outflows of $5.7 billion within two days. Similarly, Ronin Bridge's TVL dropped from approximately $336 million on March 29, 2022, to $83 million by May 29, 2022 —a 75.29% decline.
- **Ecosystem Chain Reactions:** The Bybit attack triggered panic selling, causing USDe to depeg to $0.96. Chainlink' s oracle price deviation subsequently led to $22 million in liquidations on Aave. After the Ronin Bridge attack, the resulting asset outflows significantly reduced DeFi activities within the Ronin ecosystem.
- **Erosion of Industry Trust:** Historical incidents —including Mt. Gox, Poly Network, and the Ronin Bridge hack —have repeatedly damaged trust in the crypto industry, causing institutional investors to adopt a more cautious stance.

3.3.3 Industry Ecosystem Reshaping and Regulatory Enhancement

- **Upgraded Security Standards:** The Poly Network incident prompted DeFi projects to enhance contract security audits. Ronin Bridge increased its number of validators to reduce single-point-of-failure risks. Following the Mt. Gox incident, exchanges widely adopted multi-signature wallets and Proof of Reserves (PoR) protocols. The Bybit incident exposed potential vulnerabilities in multi-signature systems, which may prompt the industry to upgrade to MPC wallets, hardware signatures, and other advanced security solutions.
- **Stricter Regulations:** Major hacking incidents often attract regulatory intervention, compelling exchanges and DeFi projects to implement stricter security protocols such as multi-signature wallets and asset reserve verification. Enhanced KYC/AML requirements are also common regulatory responses. For instance, the Mt. Gox incident prompted Japan to introduce the Payment Services Act, regulating crypto exchanges. Following the Ronin Bridge attack in 2022, the U.S. government intensified its surveillance of wallets linked to the North Korean Lazarus Group. Additionally, in 2022, the U.S. OFAC sanctioned Tornado Cash to prevent hackers from laundering funds through the platform —a decision that was overturned by court ruling in 2025.

In essence, hacking incidents act as a mirror —exposing the vulnerabilities of the crypto industry while simultaneously reflecting its potential for growth and evolution. In the short term, these events destabilize market confidence and trigger turmoil. However, in the long term, they serve as catalysts for technological advancements and improved regulatory frameworks.

4 Industry Insights and Recommendations

The crypto industry faces multiple security challenges stemming from technological complexity, human factors, and regulatory compliance issues. First, the complexity and potential vulnerabilities at the technical level are significant concerns. Due to the rapid development of blockchain technology, undiscovered vulnerabilities are inevitable, and insufficient smart contract auditing makes projects susceptible to attacks. Even the underlying blockchain technology itself may have security risks. Second, human factors present another crucial challenge, including users' weak passwords and poor security habits, lack of education on security best practices, and internal management vulnerabilities that could lead to malicious employee activities threatening platform security. Finally, there are numerous regulatory and compliance issues, including inadequate regulatory oversight and challenges in anti-money laundering mechanisms. The complexity of cross-chain transfers, address dispersion, and anonymity of DeFi protocols, combined with the abuse of non-KYC exchanges, create opportunities for hacking attacks and money laundering activities. To address these challenges, the crypto industry must build a multi-layered security protection system that encompasses technology, risk diversification, user education, and regulatory measures.

4.1 Technical Defense Upgrades

To enhance the security of crypto assets, the industry must strengthen protective measures on multiple fronts. Firstly, in terms of private key management and verification mechanisms, decentralized key management solutions such as Multi-Party Computation (MPC) wallets should be adopted. This approach can effectively eliminate the risk of single-point private key leaks and ensure that transactions require multi-party authorization. Meanwhile, using Hardware Security Modules (HSM) or hardware wallets (e.g., Ledger) to store private keys can isolate them from network attacks. Additionally, increasing the number of validator nodes (for instance, Ronin expanded its validators from 9 to 21) can establish a dynamic verification mechanism, further reducing the risk of single-point control.

In terms of smart contract and protocol security, adopting formal verification tools (such as Certora and OpenZeppelin) for mathematical proof-level auditing of smart contracts can help

ensure code logic is secure, fundamentally reducing security risks. Additionally, deploying zero-knowledge proof technologies (e.g., ZK-Rollups) for cross-chain transaction verification can replace traditional multi-signature mechanisms, enhancing both anonymity and security. Modular architecture designs (e.g., Celestia) that separate data availability from the execution layer can also effectively reduce systemic risks.

Lastly, in terms of real-time monitoring and emergency response, deploying on-chain analysis platforms (such as Chainalysis and TRM Labs) is recommended to track suspicious transactions and large fund movements in real-time, enabling prompt detection of potential threats. Moreover, establishing risk thresholds to trigger automatic circuit breaker mechanisms (e.g., pausing cross-chain bridge withdrawals or trading functions after the Ronin attack) can help cut off the attack path before risks escalate, thereby safeguarding user asset security.

4.2 Compliance and Regulatory Coordination

In terms of building a global regulatory framework, Japan's Payment Services Act offers valuable insights. This legislation mandates that exchanges disclose the proportion of assets held in hot and cold wallets, implement multi-signature mechanisms, and undergo third-party security audits to ensure platform security. Additionally, establishing a cross-border on-chain data sharing network can enhance anti-money laundering (AML) efforts by tracking the movement of hacker funds. For example, the United States' monitoring of North Korean Lazarus Group wallets has strengthened overall industry security oversight. To promote DeFi compliance, protocols should be encouraged to integrate KYC/AML modules to rigorously verify user identities and prevent the misuse of anonymous accounts. Furthermore, adopting regulatory sandbox pilots can provide innovative projects with controlled environments for testing, striking a balance between security and efficiency. This model can reference the regulatory framework established by Singapore's MAS (Monetary Authority of Singapore).

4.3 Operational Transparency and Risk Diversification

To build user trust and mitigate systemic risks, the crypto industry must adopt effective measures for asset transparency and insurance coverage. Firstly, to enhance asset transparency, exchanges should regularly publish Proof of Reserves (PoR) reports (e.g., Gate.io periodically releases PoR reports). DeFi platforms can disclose on-chain reserve addresses and audit reports to demonstrate that their assets are fully backed, addressing user concerns about fund security. Additionally, using decentralized oracles for multi-source data verification can effec-

tively prevent price manipulation and liquidation vulnerabilities (e.g., the USDe price deviation during the Bybit incident), ensuring fairness and accuracy in trading and liquidation processes.

Secondly, insurance mechanisms can play a crucial role in risk mitigation. Exchanges and DeFi platforms can establish protocol insurance funds to cover potential losses from hacking incidents. Collaborating with third-party insurance providers to offer user asset insurance can further diversify systemic risks, ensuring that users' funds are protected even in extreme scenarios. These measures not only improve platform security but also reinforce user trust in the crypto ecosystem.

4.4 User Education and Community Collaboration

To improve security across the cryptocurrency industry, raising security awareness and incentivizing white-hat hackers are essential steps. Firstly, security awareness education is fundamental to preventing security incidents. By providing users with security operation guidelines that cover topics such as cold wallet usage, phishing attack identification, and smart contract authorization risks, users can better protect their assets. Additionally, conducting simulated attack exercises (such as "Red Team drills") on a regular basis can test platform defense capabilities, helping to identify and address security vulnerabilities in a timely manner. Meanwhile, establishing bug bounty programs (e.g., Immunefi's high-reward initiatives) encourages white-hat hackers to actively report vulnerabilities, accelerating the resolution of potential issues. Finally, leveraging DAO-based community governance mechanisms allows community members to participate in security upgrade decisions through voting, fostering consensus and trust while collectively driving platform security improvements.

4.5 Industry Ecosystem Collaboration

To enhance cross-chain security and the stability of the broader crypto ecosystem, establishing a cross-chain security alliance is crucial. Forming industry-wide security alliances, such as the Blockchain Security Alliance (BSA), enables the sharing of threat intelligence, real-time updates on hacker attack methods, and defense strategies, ultimately strengthening the industry's overall security posture. Promoting the standardization of cross-chain communication protocols (e.g., IBC) can reduce compatibility vulnerabilities, ensuring secure interoperability between different blockchain networks. Moreover, open-source technology and ecosystem interoperability are also key components. Encouraging projects to publicly share their core module code, such as Ethereum clients, allows for community auditing, enhancing code transparency and security.

Implementing protocols like LayerZero for multi-chain asset interoperability can reduce reliance on a single chain, effectively diversifying potential risks and strengthening the ecosystem’s resilience.

Through these measures, the crypto industry can establish a three-in-one security system integrating “technology, regulation, and users.” Technology upgrades serve as the foundation, with advanced tools like zero-knowledge proofs (ZK) and multi-party computation (MPC) defending against increasingly sophisticated attacks. Regulatory collaboration creates an essential framework that enables effective global oversight and anti-money laundering networks, fostering powerful synergy. At the system’s core lies user trust, which grows through transparent operations and ongoing user education, ultimately strengthening community resilience.

5 Conclusion

The cryptocurrency market, in its pursuit of innovation and efficiency, has always been accompanied by security risks. In 2025, the crypto market faced unprecedented security challenges. The large-scale hacking attack on the Bybit exchange not only exposed vulnerabilities in centralized exchange security defenses but also highlighted broader weaknesses across the industry in areas such as technology, regulation, and user education. The continuous evolution of hacking techniques, increasingly complex money laundering tactics, and the resulting market panic and altered investor behavior pose serious threats to the stability and sustainable growth of the crypto market.

However, every crisis also presents an opportunity for progress. From the collapse of trust following the Mt. Gox incident, to the Poly Network cross-chain crisis, and the compromise of Bybit's cold wallet, each attack has forced the industry to evolve. By deeply analyzing these major hacking incidents, we can better understand the vulnerabilities within the industry and extract valuable lessons. To address these challenges, the cryptocurrency industry must build a multi-layered, comprehensive security framework that includes:

- **Technical Defense Upgrades:** Adopting advanced technologies such as decentralized key management, formal verification, and zero-knowledge proofs to improve the security of smart contracts and protocols fundamentally.
- **Compliance and Regulatory Coordination:** Establishing a globally unified regulatory framework, strengthening AML collaboration, promoting DeFi compliance, and balancing innovation with security.
- **Operational Transparency and Risk Diversification:** Enhancing asset transparency, implementing comprehensive insurance mechanisms, and improving user trust.
- **User Education and Community Collaboration:** Promoting security awareness, encouraging white-hat hacker participation, and building a robust community-driven security defense.
- **Industry Ecosystem Collaboration:** Forming cross-chain security alliances, promoting open-source technology, and enhancing ecosystem interoperability to improve the industry' s overall resilience.

The cryptocurrency industry is now at a critical turning point. A safer, more transparent, and sustainable future can be achieved only through the combined efforts of technology, regulation, and community engagement. Each hacking incident serves as a wake-up call, reminding the

industry to continually reflect and improve. By doing so, the crypto market can grow stronger through challenges, advance amid change, and ultimately unlock its true potential.

Author: Ember

6 References

1. https://defillama.com/hacks
2. https://dune.com/legionx/tornadocashstats
3. https://www.footprint.network/@Beosin/Footprint-Beosin-2024-Web3-Security-Report#type=dashboard
4. https://www.footprint.network/@Beosin/Footprint-Beosin-2023-Web3-Security-Report#type=dashboard
5. https://peckshield.com/static/pdf/2020_2.pdf
6. https://www.slowmist.com/report/2024-Blockchain-Security-and-AML-Annual-Report%28CN%29.pdf
7. https://sussblockchain.com/review-of-the-anti-money-laundering-analysis-of-the-web3-blockchain-security-situation-in-the-first-half-of-2023/
8. https://news.qq.com/rain/a/20250225A05C7R00?suid=&media_id=
9. https://www.theblockbeats.info/news/56981
10. https://arxiv.org/abs/2305.14748
11. https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/67a66929a076faf602d64b4c_TRM%202025%20Crypto%20Crime%20Report.pdf
12. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/
13. https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/67a66929a076faf602d64b4c_TRM%202025%20Crypto%20Crime%20Report.pdf
14. https://zh.wikipedia.org/wiki/Mt._Gox
15. https://www.gate.io/trade/BTC_USDT
16. https://intel.arkm.com/explorer/entity/mt-gox
17. https://cn.cointelegraph.com/news/poly-network-hacker-returns-258m-conducts-ama-on-how-it-went-down
18. https://www.odaily.news/post/5171470
19. https://www.gate.io/trade/ETH_USDT
20. https://www.coingecko.com/en/coins/o3-swap
21. https://defillama.com/protocols/Bridge
22. https://www.aicoin.com/zh-Hans/article/289899
23. https://foresightnews.pro/article/detail/1683
24. https://defillama.com/chain/Ronin
25. https://abmedia.io/us-court-overturns-tornado-cash-sanctions
26. https://dune.com/gate_research/bybit-security-breach-tracker#according-to-on-chain-analysis-the-stolen-assets-primarily-include
27. https://defillama.com/cex/bybit?usdInflows=true&tvl=true&twitter=false#tvl-charts

28. https://data.chain.link/feeds/ethereum/mainnet/usde-usd
29. https://dune.com/KARTOD/AAVE-Liquidations
30. https://x.com/omeragoldberg/status/1893440510682964012

Links

Gate Research Official Website

Previous Research Reports

About Gate Research

Gate Research is a professional institute dedicated to blockchain industry analysis. We are committed to providing deep insights into the development trends of the blockchain sector. We aim to equip professionals and enthusiasts with forward-looking and expert industry insights. With a foundational commitment to democratizing blockchain knowledge, we strive to simplify complex technical concepts into understandable language. We present a comprehensive view of the blockchain industry by analyzing vast amounts of data and observing market trends, helping a wider audience understand and engage with this dynamic field.

research@gate.me