ISSN: 2790-1386

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Cryptocurrency Research

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper

Open Access

The $1.4 Billion Bybit Hack: Cybersecurity Failures and the Risks of Cryptocurrency Deregulation

David S. Krause[1*]

[1]Emeritus Associate Professor of Finance, Marquette University, Milwaukee, WI, USA. E-mail: david.krause@marquette.edu

Article Info

Volume 5, Issue 1, June 2025
Received : 06 March 2025
Accepted : 10 June 2025
Published : 25 June 2025
doi: 10.51483/IJCCR.5.1.2025.52-62

Abstract

Cryptocurrency exchange hacks remain a persistent threat, posing significant financial and security risks. The 2025 Bybit hack, resulting in approximately $1.4 billion in losses, is the largest cryptocurrency heist to date, highlighting the vulnerabilities even among leading exchanges. This paper examines the implications of such breaches on market stability, regulatory policies, and investor confidence, particularly within the context of the Trump administration's deregulatory approach to digital assets. The analysis explores the trade-offs between promoting innovation and ensuring robust security frameworks, emphasizing the potential for policy adjustments in light of escalating cyber threats. Additionally, the study reviews historical exchange hacks, demonstrating a pattern of increasing sophistication among malicious actors. The findings suggest that regulatory clarity and enhanced security measures are essential for the long-term stability of the cryptocurrency ecosystem. Future research directions include evaluating global regulatory responses, the role of decentralized exchanges, and the effectiveness of cybersecurity protocols.

Keywords: *Cryptocurrencies, Exchange hacks, Regulation, Cybersecurity, Investor protection, Market stability*

© 2025 David S. Krause. This is an open access article under the CCBY license (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

1. Introduction

The February 2025 Bybit hack stands as one of the largest cryptocurrency exchange breaches in history, with attackers stealing approximately $1.4 billion worth of Ethereum (ETH) (AP News, 2025; Dhage, 2025). The incident highlights persistent vulnerabilities in centralized crypto exchanges and raises urgent questions about blockchain security, regulatory oversight, and the resilience of digital asset markets. Despite the industry's ongoing efforts to enhance security measures, the sophistication of this attack underscores the evolving threats facing cryptocurrency platforms (Lakshmanan, 2025).

* *Corresponding author: David S. Krause, Emeritus Associate Professor of Finance, Marquette University, Milwaukee, WI, USA. E-mail: david.krause@marquette.edu*

2790-1386/© 2025. David S. Krause. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The attack occurred when hackers exploited vulnerability in Bybit's Ethereum multi-signature cold wallet transfer process. The perpetrators manipulated transaction signing mechanisms to approve unauthorized withdrawals while bypassing security protocols (Bybit Announcement, 2024; Jima, 2025). Forensic investigations suggest that the North Korean state-sponsored Lazarus Group orchestrated the breach, a claim supported by similarities to prior high-profile exchange hacks (Jima, 2025; Lakshmanan, 2025). The aftermath of the Bybit hack saw a rapid decline in Ethereum's price and broader market turmoil, with the total cryptocurrency market capitalization dropping by $75 billion within 24 hours (AP News, 2025; The Economic Times, 2025).

Beyond the financial impact, the Bybit hack has intensified regulatory scrutiny. Authorities and industry experts have renewed calls for stricter compliance with global frameworks, such as the European Union's Markets in Crypto-Assets (MiCA) regulation, to mitigate systemic risks (The Economic Times, 2025). Moreover, the incident underscores the ongoing debate about the security of centralized exchanges versus decentralized alternatives, as traders increasingly seek refuge in self-custodial solutions and privacy-focused assets (AP News, 2025).

This paper provides a comprehensive analysis of the Bybit hack, examining its technical execution, financial consequences, regulatory implications, and broader significance for the cryptocurrency industry. By evaluating the attack's mechanics and industry response, this study seeks to contribute to the ongoing discourse on strengthening security measures and improving investor protection in the digital asset ecosystem.

2. Cryptocurrency Exchange Hacks

Crypto exchange hacks remain a critical and persistent threat within the digital asset ecosystem, leading to the theft of billions of dollars over the past decade. The recent Bybit breach, resulting in the loss of $1.4 billion in Ethereum, now ranks as the largest cryptocurrency exchange hack in history (Zhou, 2025; McGrath, 2025). This incident highlights the continued vulnerabilities of even well-established exchanges to sophisticated cyberattacks, despite ongoing advancements in security protocols.

Table 1 provides a chronological overview of major crypto exchange hacks, illustrating the growing financial losses incurred by the industry. Over time, the scale and frequency of attacks have escalated, underscoring the evolving tactics employed by malicious actors (McGrath, 2025). The table lists the most significant exchange breaches, spanning from 2014 to 2025, revealing an upward trend in the magnitude of losses.

Table 1: Major Cryptocurrency Exchange Hacks

Exchange/Platform	Year	Cryptocurrencies Affected	Amount Lost (USD)
Bybit	2025	Ethereum	$1.4 billion
DMM Bitcoin	2024	Bitcoin	$305 million
Mixin Network	2023	Bitcoin, Ethereum, Tether	$200 million
Ronin Network	2022	Ethereum, USDC	$615 million
FTX	2022	Multiple coins	$477 million
Binance	2022	Binance Coin	$570 million
Wormhole	2022	Multiple coins	$325 million
Poly Network	2021	Multiple coins	$611 million
KuCoin	2020	Multiple coins	$281 million
Coincheck	2018	NEM	$532 million
Mt. Gox	2014	Bitcoin	$450 million

Historically, cryptocurrency exchange hacks have shaped industry security practices and regulatory responses. The 2014 Mt. Gox hack, which resulted in the theft of approximately $450 million in Bitcoin, exposed the vulnerabilities of early exchanges and led to the platform's eventual collapse (Kaspersky, 2024; Elliptic, 2023). Subsequent high-profile attacks, such as the $615 million Ronin Network hack in 2022 and the $611 million Poly Network breach in 2021, demonstrate that both centralized and decentralized platforms remain prime targets for cybercriminals (Kaspersky, 2024).

These breaches have significant consequences beyond immediate financial losses. They contribute to eroded user confidence, increased market volatility, and heightened regulatory scrutiny. For instance, the 2018 Coincheck hack, which resulted in the theft of $532 million in NEM tokens, affected approximately 260,000 users and led to stricter regulatory oversight in Japan (Trend Micro, 2018). Similarly, the Bybit hack immediately triggered widespread investor concerns, causing a temporary drop in Ethereum's price and a surge in withdrawal requests from the platform (Zhou, 2025).

The persistent nature of these hacks underscores the challenges exchanges face in securing user funds and maintaining market trust. From 2011 to 2020 alone, over 50 cryptocurrency exchanges suffered security breaches, with cumulative losses exceeding $15.6 billion (Balaban, 2023). The increasing sophistication of these attacks has raised fundamental questions about the adequacy of existing security measures and the need for improved risk management strategies. Governments and regulatory bodies worldwide have cited these breaches as justification for stricter compliance requirements and the implementation of security standards for cryptocurrency exchanges (Elliptic, 2023). As the cryptocurrency market continues to expand, addressing these security vulnerabilities will be critical for sustaining industry growth and maintaining investor confidence.

3. Attack Mechanism and Exploited Vulnerabilities

The Bybit hack of February 2025 was executed through a sophisticated attack targeting the exchange's Ethereum multi-signature (multisig) cold wallet. The breach occurred during a routine transfer from the cold wallet to a warm wallet, wherein attackers manipulated the transaction interface to display a legitimate destination address while covertly altering the underlying smart contract logic. This manipulation enabled them to bypass Bybit's multi-signature authentication protocols and gain unauthorized control over the wallet (Lakshmanan, 2025; Bybit Announcement, 2024).

Blockchain forensic analysis suggests that the attackers employed advanced phishing and social engineering tactics to compromise internal credentials, thereby facilitating unauthorized access (Jima, 2025). Based on similarities with previous cyberattacks, including the January 2025 Phemex hack, blockchain analysts have attributed the attack to the North Korean state-sponsored Lazarus Group.

The attack exploited vulnerabilities within Bybit's multisig cold wallet system, transaction interface design, and human verification processes. A key weakness lay in the lack of real-time validation within the Safe.global platform's transaction interface. This allowed attackers to mask malicious code while displaying a valid recipient address, a tactic reminiscent of previous breaches such as those involving WazirX and Radiant Capital in 2024 (SecurityWeek, 2025; Faridi, 2025).

One of the most significant aspects of the breach was the use of the delegatecall function to rewrite the wallet's implementation address, granting attackers full control over the compromised funds (Faridi, 2025). Delegatecall enables a contract to execute external code within its own context, offering code reuse but posing access control risks. Additionally, the attack exploited blind signing practices, where authorized signers approved transactions without thoroughly verifying the underlying code. The interface masked the malicious logic behind legitimate-looking destination addresses, further enabling the breach (Nguyen, 2025; Carter, 2025).

Beyond the technical aspects, social engineering played a crucial role in the attack. The attackers launched a targeted phishing campaign against Bybit employees, distributing malware-laced documents that impersonated internal stakeholders. Once a single signer's credentials were compromised, attackers were able to initiate fraudulent transactions, leveraging procedural complacency to gain approval from additional signers who failed to detect the deception (Nguyen, 2025; Cointelegraph, 2025). This human-layer vulnerability

highlights the persistent challenge of mitigating social engineering risks, even within exchanges that implement robust technical safeguards (Faridi, 2025). The attackers also leveraged a zero-day vulnerability in Safe.global's User Interface (UI), which allowed transaction data to appear legitimate while altering smart contract permissions (Carter, 2025).

The Bybit hack underscores the ongoing security risks associated with centralized exchanges, even those with significant financial reserves and security measures in place. This incident highlights the urgent need for improved cold wallet security, real-time smart contract validation, and enhanced employee cybersecurity training to prevent similar breaches in the future. Moreover, the sophisticated combination of technical exploits and social engineering tactics exemplifies the evolving threat landscape facing cryptocurrency platforms, necessitating a multi-faceted approach to security and regulatory oversight.

4. Financial Impact and Market Reactions

The Bybit hack triggered significant volatility across cryptocurrency markets, with Ethereum experiencing the most substantial immediate impact. ETH prices plummeted by 7% within minutes of the breach, falling from $2,845 to $2,625 before partially recovering to $2,735 (Butt, 2025). This sharp decline contributed to broader market contagion, wiping out $75 billion in global cryptocurrency market capitalization within 24 hours. Bitcoin (BTC) and Solana (SOL) also suffered declines of 2.4% and 3.0%, respectively (AP News, 2025; The Economic Times, 2025).

The initial sell-off was exacerbated by speculative trading, as rumors circulated that Bybit would repurchase ETH to mitigate losses, briefly pushing prices up (Liu, 2025). However, this recovery was short-lived after Bybit CEO Ben Zhou clarified that the exchange had no plans for large-scale ETH purchases, leading to renewed selling pressure (Manoylov, 2025).

4.1. Liquidity and Exchange Stability

In response to the hack, Bybit focused on securing short-term liquidity to maintain operations and reassure users. The exchange swiftly obtained bridge loans from industry partners, covering 80% of the stolen ETH—equivalent to $1.12 billion—thereby preventing the need to sell reserves into a depressed market (Panewslab, 2025; Manoylov, 2025). Additionally, Zhou emphasized Bybit's $20 billion in reserves and its 1:1 asset-backing policy, asserting that user funds remained secure. However, critics noted that the breach reduced Bybit's reserve ratio to 92% of liabilities, raising concerns about the exchange's overall solvency (Masud, 2025; OneSafe, 2025).

Despite these reassurances, the hack reinforced concerns about systemic risks within centralized exchanges. Analysts highlighted that Bybit's pre-hack reserves of $16.2 billion accounted for just 8% of the $200 billion held by the largest cryptocurrency exchanges, underscoring the fragility of centralized platforms in handling large-scale security breaches (OneSafe, 2025).

4.2. Hacker Liquidation and On-Chain Monitoring

The stolen 401,347 ETH—valued at approximately $1.4 billion—was distributed across 53 wallets, all of which were placed under real-time surveillance by blockchain analytics firms (Liu, 2025; Jima, 2025). However, several key risks complicate efforts to recover the stolen assets:

Decentralized Exchange (DEX) Laundering: The use of platforms like Uniswap allows hackers to mix funds, making tracing more difficult.

Cross-Chain Swaps: Moving funds to privacy-focused blockchains, such as Monero, significantly hinders asset recovery efforts.

Over-The-Counter (OTC) Broker Networks: Unregulated brokers facilitate fiat conversion, enabling hackers to cash out without triggering centralized exchange alerts.

Analysts warn that liquidating even 10% of the stolen ETH could depress prices by 12–15%, comparable to the impact seen when Ethereum co-founder Vitalik Buterin has made large transactions in the past (Liu, 2025). There is speculation that the hackers, likely the North Korean Lazarus Group, may delay selling until

market conditions improve, leveraging decentralized financial tools to obscure transactions further (Jima, 2025).

5. Security Implications for the Crypto Industry

The Bybit hack exposed critical weaknesses in widely adopted security measures, challenging assumptions about the invulnerability of cold wallets and multi-sig protocols. While these mechanisms are designed to enhance asset protection, the attack demonstrated how vulnerabilities in transaction interfaces and human oversight can undermine even the most secure infrastructure.

5.1. Evaluating the Effectiveness of Current Security Measures

Multi-signature cold wallets, which require multiple private keys for transaction authorization, failed to prevent the breach due to:

Transaction Interface Vulnerabilities: Attackers exploited a flaw in the Safe.global UI that masked malicious smart contract logic during multi-sig approvals, bypassing validation checks (SecurityWeek, 2025).

Social Engineering Attacks: Phishing tactics compromised at least one key signer, enabling attackers to manipulate subsequent approvals from unwitting stakeholders (Yue, 2025).

While multi-sig systems reduce single points of failure (Etugbo, 2025), the incident revealed their dependency on secure user interfaces and robust human verification processes. Bybit's $20 billion in reserves proved insufficient to prevent systemic risks, as centralized exchanges collectively hold over $200 billion in assets, many of which rely on similar security frameworks (Yue, 2025).

5.2. Lessons for Centralized Exchanges

To mitigate risks highlighted by the Bybit hack, centralized exchanges should adopt:

Enhanced Interface Security: Implement real-time smart contract validation to detect discrepancies between displayed and actual transaction logic (Patairya, 2025).

Decentralized Key Management: Distribute signing authority across geographically separated teams to reduce insider threats (Etugbo, 2025).

Phishing-Resistant Protocols: Mandate the use of Hardware Security Modules (HSMs) for key storage and enforce Multi-Factor Authentication (MFA) for transaction approvals.

5.3. Blind Signing and Smart Contract Vulnerabilities

The attack underscored how UI manipulation and blind signing—approving transactions without full visibility into contract terms—can compromise even robust cryptographic safeguards. Bybit's interface failed to alert signers to malicious delegatecall functions that redirected funds. Attackers exploited this by:

Masking Contract Logic: Displaying legitimate destination addresses while embedding malicious code to transfer wallet ownership (SecurityWeek, 2025).

Exploiting Simulation Delays: Manipulating the gap between transaction simulation and execution to alter contract states, a technique commonly used in fake transaction scams (Patairya, 2025).

This trend reflects broader industry risks, with blind signing vulnerabilities accounting for 34% of the $2.2 billion stolen in crypto-related thefts in 2024 (Chainalysis, 2025).

5.4. Recommendations for Improved Verification Protocols

Table 2 outlines proposed improvements to exchange practices, focusing on enhancing security and user experience. The table contrasts current, less secure, and informative practices with suggested upgrades.

Additionally, integrating Chaintech Network's cryptographic integrity frameworks—such as real-time authentication and tamper-evident logs—could enhance auditability. Regulatory mandates for transaction transparency tools, akin to Central Bank Digital Currency (CBDC) verification protocols, may further mitigate blind signing risks.

Table 2: Suggested Exchange Improvements	
Current Practice	**Proposed Improvement**
Static transaction previews	Real-time simulation refreshes post-blockchain updates (Patairya, 2025)
Manual contract reviews	Automated blocklisting of phishing contracts via APIs (Chaintech Network, 2025)
Generic approval prompts	Contextual warnings for high-risk functions (e.g., ownership transfers)

The Bybit hack necessitates a paradigm shift in cryptocurrency security, moving beyond reliance on multi-signature mechanisms toward holistic systems that incorporate real-time analytics, decentralized governance, and enhanced user education. As Bybit CEO Ben Zhou emphasized, "Security isn't a feature—it's the product" (SecurityWeek, 2025), underscoring the need for verifiable transaction ecosystems that prioritize security over convenience.

6. Broader Implications for the Future of Crypto Investing

The Bybit hack has raised significant concerns for investors, regulators, and policymakers (Carter, 2025). As the largest cryptocurrency theft in history, the incident underscores persistent security vulnerabilities in the digital asset industry and highlights several critical issues that could shape the future of crypto investing.

6.1. Investor Confidence

The magnitude of this breach may erode investor confidence in centralized cryptocurrency exchanges and the broader digital asset ecosystem. Despite Bybit's assurances that customer funds remain secure and that the platform remains solvent, the hack reinforces the risks associated with storing large sums of cryptocurrency on centralized platforms (Cointelegraph, 2025). This could drive increased migration toward decentralized exchanges and self-custody solutions, as users seek alternatives that mitigate custodial risk. Following hack, the exchange saw over $5.7 billion in total outflows from investors in the following 24 hours. Consequently, Bybit's tracked assets dropped from roughly $16.9 billion to $11.2 billion, prompting an ongoing investigation into the incident (Rodrigues, 2025).

6.2. Regulatory Scrutiny

The Bybit hack is expected to intensify regulatory scrutiny of the cryptocurrency sector, with policymakers and regulatory agencies considering new measures to enhance security and protect investors:

- **Calls for Increased Oversight** – Regulators may push for stricter oversight of cryptocurrency exchanges, particularly regarding security measures, operational risk management, greater reserves, and the handling of customer funds.
- **Compliance Requirements** – Exchanges could face heightened pressure to adopt compliance standards akin to those imposed on traditional financial institutions, including mandatory security audits, enhanced Know Your Customer (KYC) requirements, and capital reserve obligations.

6.3. Policy Implications

This security breach may influence policy discussions in several key areas:

- **Security Standards** – Policymakers may advocate for mandatory multi-signature authentication, real-time security monitoring, and regular third-party security audits to mitigate the risk of future breaches (Upadhyay, 2025).
- **Consumer Protection** – Renewed discussions around investor protection could lead to insurance mandates for cryptocurrency exchanges, like deposit insurance for traditional banks, ensuring users are compensated in the event of security breaches.
- **International Cooperation** – Given the suspected involvement of state-sponsored actors, such as North Korean hackers, this incident may accelerate global collaboration on cybersecurity measures and financial

crime prevention, with regulators working across jurisdictions to enhance compliance and enforcement efforts.

6.4. Industry Response

The possibility of an Ethereum blockchain rollback, aimed at recovering stolen funds from the Bybit hack, was explored, with Bybit engaging the Ethereum Foundation and Vitalik Buterin for potential recommendations. While some industry leaders have advocated for this drastic measure, Bybit's CEO acknowledged it would require community consensus since it is not a unilateral decision (Rodrigues, 2025). Implementing such a rollback, a complex state change, would likely result in a contentious hard fork, potentially splitting the Ethereum network into two distinct chains, given its intricate smart contract ecosystem and the need for broad agreement.

6.5. The Cryptocurrency Industry must Respond Proactively to Restore Trust and Demonstrate Resilience

- **Security Enhancements** – Cryptocurrency exchanges and related platforms may need to significantly upgrade security infrastructures, including adopting AI-driven fraud detection, implementing geographically distributed private key storage, and enhancing cold wallet protections (Shamla Tech, 2025).
- **Transparency Initiatives** – There may be increased adoption of proof-of-reserves audits and real-time asset verification measures to reassure stakeholders about the solvency and security of exchanges (Cointelegraph, 2025).

The Bybit hack serves as a stark reminder of the ongoing security challenges in the rapidly evolving cryptocurrency landscape. Beyond its immediate financial impact, the breach is likely to reshape regulatory approaches, industry best practices, and investor sentiment. Moving forward, crypto exchanges and regulatory bodies must work together to establish more robust security measures, improve transparency, and create a more resilient digital asset ecosystem (Kharif *et al.*, 2025).

7. Bybit Hack and Trump's Crypto Deregulation

The recent Bybit hack, which resulted in the largest cryptocurrency theft in history, presents a significant challenge to the Trump administration's deregulatory approach to the crypto sector (Krause, 2025). While the administration has positioned itself as a strong proponent of digital asset innovation and minimal regulation, this incident underscores the persistent vulnerabilities in the industry and may necessitate a reassessment of current policy priorities.

7.1. Regulatory Reconsideration?

The scale and impact of the Bybit hack may force the administration to reconsider elements of its deregulatory stance (Krause, 2025). Although the White House remains committed to making the U.S. "the crypto capital of the planet" (Ness, 2025), security concerns raised by such high-profile breaches could lead to a more nuanced regulatory framework:

- **Balancing Deregulation and Security** – The administration may need to strike a balance between promoting innovation and ensuring adequate safeguards to protect investors and institutions from cyber threats.
- **Targeted Regulations** – Rather than imposing broad and burdensome regulations, policymakers might adopt targeted measures that specifically enhance exchange security, such as stricter cybersecurity requirements and risk management protocols.

7.2. Security-Focused Initiatives

Given the severity of the Bybit hack, the administration may shift its focus toward improving security within the digital asset ecosystem. Several potential initiatives could emerge:

- **Prioritization by the Working Group on Digital Asset Markets** – The recently established Working Group on Digital Asset Markets, a key advisory body under the Trump administration, may prioritize cybersecurity recommendations to enhance exchange security and mitigate future breaches (Bosch, 2025).

- **Acceleration of Federal Crypto Framework Development –** While the administration has resisted overly restrictive crypto regulations, it may expedite the development of a comprehensive framework that includes minimum security standards for exchanges and wallet providers.

7.3. Impact on Public Perception

The Bybit hack may also shape public sentiment toward cryptocurrency investments, influencing both investor behavior and government policy:

- **Trust and Adoption Challenges –** Major security breaches can erode trust in cryptocurrency exchanges, potentially slowing down mainstream adoption and complicating efforts to position the U.S. as a leader in digital finance.
- **Increased Investor Protection Demands –** Even within a deregulatory framework, there may be growing pressure from the public and industry stakeholders to implement investor protection measures, such as requiring exchanges to maintain sufficient insurance coverage for hacked funds or mandating real-time security audits.

7.4. International Considerations

Given the global nature of cryptocurrency markets, the Bybit hack may also have broader geopolitical implications:

- **Strengthening International Cybersecurity Cooperation –** The attack, suspected to involve state-sponsored hackers, may prompt the U.S. to seek closer cooperation with international partners on cybersecurity and financial crime prevention efforts.
- **Maintaining a Competitive Edge –** The administration's vision for U.S. crypto dominance could be undermined if security concerns lead to capital flight toward more heavily regulated jurisdictions that are perceived as safer for investors and institutions.

In response to the Bybit hack, the Trump administration may consider several policy modifications to address security vulnerabilities while maintaining its commitment to crypto innovation:

- **Enhanced Disclosure Requirements –** Exchanges could be required to disclose detailed information about their security infrastructure, risk management policies, and prior breaches to ensure greater transparency and accountability.
- **Cybersecurity Standards for Exchanges –** The government may push for the establishment of minimum cybersecurity benchmarks for cryptocurrency exchanges operating within U.S. jurisdictions, possibly incorporating multi-factor authentication mandates, penetration testing, and mandatory third-party security audits.

While the Trump administration remains committed to supporting a favorable environment for crypto innovation and economic growth, the Bybit hack serves as a stark reminder of the sector's persistent security risks. In the coming months, the Trump administration may need to adopt a more measured approach to deregulation—one that integrates necessary security enhancements to safeguard investors while preserving the core principles of innovation and market competitiveness.

8. Conclusion

The Bybit hack of 2025 underscores the persistent vulnerabilities in the cryptocurrency ecosystem and highlights the challenges of balancing innovation with investor protection. While the Trump administration's deregulatory stance seeks to position the U.S. as a leader in digital assets, security breaches of this magnitude raise concerns about the adequacy of existing regulatory frameworks. This incident may prompt a reassessment of cryptocurrency oversight, with potential policy adjustments focusing on enhanced cybersecurity standards, investor protection measures, and international cooperation.

Future research should explore the evolving regulatory landscape in response to major exchange hacks. Key areas include the effectiveness of self-regulation versus government-imposed security mandates, the role

of decentralized exchanges in mitigating hacking risks, and the impact of security breaches on market stability and investor behavior. Additionally, comparative studies analyzing global regulatory responses to exchange hacks could provide valuable insights into best practices for enhancing crypto market resilience.

References

AP News. (2025). Cryptocurrency Exchange Says it was Victim of $1.5 billion Hack. February 21. https://apnews.com/article/bybit-exchange-crypto-hack-88256366c723a9de8327ef3d4071057e

Balaban, D. (2023). Inside the World of Crypto Exchange Hacks. *Forbes*. https://www.forbes.com/sites/davidbalaban/2023/05/20/inside-the-world-of-crypto-exchange-hacks/

Bosch, C. (2025). President Trump Issues Executive Order on Crypto as SEC Signals Enforcement Shift. *SheppardMullin*, January 27. https://www.corporatesecuritieslawblog.com/2025/01/president-trump-issues-executive-order-on-crypto-as-sec-signals-enforcement-shift/

Butt, A. (2025). Ethereum Faces 7% Drop After Bybit Hack: Can Recovery Hold?. *Cryptonews*, February 22. https://cryptonews.com/news/ethereum-faces-7-drop-after-bybit-hack-can-recovery-hold/

Bybit Announcement. (2024). Incident Update: Unauthorized Activity Involving ETH Cold Wallet. https://announcements.bybit.com/en/article/incident-update—eth-cold-wallet-incident-blt292c0454d26e9140/

Carter, S. (2025). Latest on the Bybit Record-Breaking $1.4 billion Crypto Hack. *Forbes*, February 21. https://www.forbes.com/sites/digital-assets/2025/02/21/latest-on-the-bybit-record-breaking-14-billion-dollar-crypto-hack/

Chainalysis. (2025). Crypto Crime Report: Blind Signing Risks and Smart Contract Fraud. https://www.chainalysis.com/reports/crypto-crime-2025

Chaintech Network. (2025). Transaction Verification Protocols: Ensuring Robust CBDC Security. https://www.chaintech.network/cbdc-compliance-and-regulatory/transaction-verification-protocols-ensuring-robust-cbdc-security

Cointelegraph. (2025). Bybit Exploit Exposes Security Flaws in Centralized Crypto Exchanges. February 22. https://www.tradingview.com/news/cointelegraph:9a4269573094b:0-bybit-exploit-exposes-security-flaws-in-centralized-crypto-exchanges

Dhage, S. (2025). Crypto Exchange Bybit Confirms Hack as Over $1.4 billion Worth of ETH Leaves Wallets. *The Block*, February 21. https://www.theblock.co/post/342667/crypto-exchange-bybit-hacked-as-over-1-billion-worth-of-eth-leaves-wallets

Elliptic. (2023). Elliptic 10-Year Anniversary: The Biggest Crypto Hacks of the Last Decade. https://www.elliptic.co/blog/analysis/elliptic-10-year-anniversary-the-biggest-crypto-hacks-of-the-last-decade

Etugbo, J. (2025). Why Multi-Signature Crypto Wallets are Crucial for Blockchain Security. *BuiltIn*, January 27. https://builtin.com/articles/multi-signature-crypto-wallets

Faridi, O. (2025). Crypto Exchange Hack Analysis: Preventing the Next $1.5B Bybit Security Breach. *Crowdfund Insider*, February 22. https://www.crowdfundinsider.com/2025/02/236613-crypto-exchange-hack-analysis-preventing-the-next-1-5b-bybit-security-breach/

Jima, L. (2025). North Korean Hackers Drain $1.46B in Ethereum from Bybit; Here's How they Might Cash Out. *The Crypto Basic*, February 22. https://thecryptobasic.com/2025/02/22/north-korean-hackers-drain-1-46b-in-ethereum-from-bybit-heres-how-they-might-cash-out/

Kaspersky. (2024). 8 Crypto Exchange Hacks to Know about. December 18. https://www.kaspersky.com/resource-center/threats/crypto-exchange-hacks

Kharif, O., Shen, M. and Nicolle, E. (2025). Bybit Hack, Crypto's Biggest Ever, Spoils Coinbase's SEC Victory Party. *Yahoo Finance*, February 21. https://finance.yahoo.com/news/bybit-hack-crypto-biggest-ever-000252787.html

Krause, D. (2025). Crypto Debanking and Deregulation: The Trump Administration's Policy Shift. February 10, SSRN. https://ssrn.com/abstract=5131024

Krause, D. (2025). The Dangers of Cryptocurrency Hype and Deregulation: Why Oversight Matters in the Digital Asset Economy. February 13, SSRN. https://ssrn.com/abstract=5136389

Lakshmanan, R. (2025). Bybit Confirms Record-Breaking $1.46 billion Crypto Heist in Sophisticated Cold Wallet Attack. *The Hacker News*, February 22. https://thehackernews.com/2025/02/bybit-confirms-record-breaking-146.html

Liu, A. (2025). Bybit's $1.4 billion ETH Hack: Market Impact and Future Implications. *Forbes*, February 21. https://www.forbes.com/sites/aliceliu/2025/02/21/bybits-14-billion-eth-hack-market-impact-and-future-implications/

Manoylov, M. (2025). Bybit CEO Says Firm Secured almost 80% of Lost ETH as Bridge Loan. *The Block*, February 21. https://www.theblock.co/post/342739/bybit-secures-80-lost-eth-bridge-loan-partners-liquidity-crunch-following-hack

Masud, F. (2025). Cryptocurrency Theft of £1.1 bn Could be Biggest Ever. *BBC*, February 22. https://www.bbc.com/news/articles/cx2844nvwx8o

McGrath, C. (2025). Bybit Just Suffered the Biggest Attack in Crypto History, Suffering $1.4 billion in Losses. *Fortune*, February 22. https://fortune.com/crypto/2025/02/21/bybit-largest-hack-crypto-history-1-4-billion-losses/

Ness, L. (2025). How Crypto Regulation could Change Under Trump and the New SEC. *Bloomberg Law*, January 14. https://www.bloomberglaw.com

Nguyen, V. (2025). Bybit Hit with $1.4 billion Hack Targeting its Ethereum Cold Wallet. *Crypto Briefing*, February 21. https://cryptobriefing.com/bybit-phishing-attack/

OneSafe. (2025). Crypto Reserve Transparency: Bybit's Liquidity Dilemma Post-Hack. *OneSafe Research*, February 21.

Panewslab. (2025). Bybit Secures Emergency Funding After Major Security Breach. *Panewslab Crypto Insights*. February 21.

Patairya, D. (2025). How Scammers Use Fake Transaction Simulation Sites to Steal Crypto. *Cointelegraph*, February 13. https://cointelegraph.com/explained/how-do-scammers-use-fake-transaction-simulation-sites-to-steal-crypto

Rodrigues, F. (2025). Bybit Sees Over $4 billion 'Bank Run' After Crypto's Biggest Hack. *Yahoo Finance*, February 22. https://finance.yahoo.com/news/bybit-sees-over-4-billion-195609586.html

SecurityWeek. (2025). Bybit Hack Drains $1.5 billion from Cryptocurrency Exchange. February 22. https://www.securityweek.com/bybit-hack-drains-1-5-billion-from-cryptocurrency-exchange/

Shamla Tech. (2025). Importance of Security in Cryptocurrency Exchanges: 5 Key Ways on the Importance of Security in Cryptocurrency Exchanges. *Shamla Tech*. https://shamlatech.com/importance-of-security-in-cryptocurrency-exchanges/

The Economic Times. (2025). Crypto Exchange Bybit's $1.5 billion Breach: All You Need to Know. February 22. https://economictimes.indiatimes.com/tech/technology/bybits-1-5-billion-breach-all-you-need-to-know/articleshow/118472384.cms

Trend Micro. (2018). Coincheck Suffers Biggest Hack in Cryptocurrency History: Expert Users Tricked into Buying False ICO. January 29. https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coincheck-suffers-biggest-hack-in-cryptocurrency-experty-users-buy-false-ico

Upadhyay, A. (2025). Bybit Suffers Major Crypto Heist: What Happened and What it Means for Users. *CNBC*. February 22. https://www.cnbctv18.com/technology/bybit-suffers-major-crypto-heist-what-happened-and-what-it-means-for-users-19563208.htm

Yue, F. (2025). Crypto Exchange Bybit Suffers $1.4 billion Hack. *Morningstar*, February 21. https://www.morningstar.com/news/marketwatch/20250221267/crypto-exchange-bybit-suffers-14-billion-hack-heres-why-its-troubling-for-the-industry

Zhou, B. (2025). What We Know about the $1.5 billion Bybit Crypto Hack. *Business Insider*. https://www.businessinsider.com/what-we-know-bybit-crypto-ethereum-hack-2025-2

Cite this article as: David S. Krause (2025). The $1.4 Billion Bybit Hack: Cybersecurity Failures and the Risks of Cryptocurrency Deregulation. *International Journal of Cryptocurrency Research,* 5(1), 52-62. doi: 10.51483/IJCCR.5.1.2025.52-62.