https://doi.org/10.51483/IJCCR.5.1.2025.92-101

ISSN: 2790-1386

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Cryptocurrency Research

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

Research Paper

Open Access

Crypto Security in the Aftermath of the Bybit Hack: Evaluating Risk Management Strategies for Digital Assets

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 : 27 February 2025
Accepted : 23 May 2025
Published : 25 June 2025
doi: 10.51483/IJCCR.5.1.2025.92-101

Abstract

The 2025 Bybit hack highlights the persistent security challenges within the cryptocurrency industry, exposing vulnerabilities in exchange security and user account protection. This paper examines the mechanisms of account takeover attacks, including phishing, credential stuffing, and session hijacking, and analyzes the broader risks they pose to investors and the industry. It evaluates security measures such as multi-factor authentication, self-custody solutions, and transaction monitoring, emphasizing the importance of proactive risk management. Additionally, the paper explores regulatory responses and industry shifts toward decentralized security models. The findings underscore that while exchanges play a critical role in enhancing security, investors must adopt self-custody and rigorous security practices to mitigate account takeover risks. A combination of stronger regulatory frameworks, technological innovations, and user education is essential to safeguarding digital assets and fostering a more resilient cryptocurrency ecosystem.

Keywords: *Cryptocurrencies, Cybersecurity, Account takeover attacks, Crypto hack, Self-custody, Regulation, Decentralized finance, Blockchain*

1. Introduction

The cryptocurrency industry was rocked by the largest hack in its history when Bybit, a major centralized exchange, suffered a staggering $1.4 billion theft on February 21, 2025 (Krause, 2025; Sellers, 2025). The attack, allegedly orchestrated by the North Korean-linked Lazarus Group, exploited vulnerabilities in the exchange's cold wallet security and leveraged sophisticated social engineering tactics to gain unauthorized access to user funds (Page, 2025). This event not only exposed weaknesses in Bybit's security infrastructure but also triggered a secondary crisis—a $4 billion liquidity exodus of funds from the Bybit platform, as panicked users withdrew assets in response to security concerns (Cromley, 2025).

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

Bybit's failure to prevent such an extensive breach has reignited concerns about the safety of centralized exchanges (CEXs) and the broader risks associated with cryptocurrency exchange custody. While CEXs offer liquidity and ease of access to digital assets, they also serve as high-value targets for cybercriminals due to their large asset pools and reliance on custodial wallet systems. The incident raises critical questions about the security of cryptocurrency exchanges, the effectiveness of existing safeguards, and the need for improved investor protection measures.

The Bybit hack underscores the increasing prevalence of account takeover (ATO) attacks, a method frequently used by cybercriminals to bypass security mechanisms and gain unauthorized access to cryptocurrency funds. ATO attacks against cryptocurrency exchanges have surged in recent years, with centralized platforms experiencing 68% of all reported hacks in the first half of 2024 (Elad, 2025). These attacks employ a combination of phishing schemes, malware injections, and SIM-swapping tactics to hijack user accounts and manipulate authentication processes.

In the case of Bybit, the attack extended beyond direct theft from exchange wallets. Investigators suggest that the hackers exploited user interfaces and manipulated transaction confirmation protocols, allowing them to approve unauthorized withdrawals without triggering conventional security alerts (Cromley, 2025). This demonstrates how ATO tactics have evolved to circumvent even cold wallet security—a feature traditionally considered the gold standard for protecting digital assets from online threats.

This paper seeks to examine the implications of the Bybit hack within the broader context of cryptocurrency exchange security. Specifically, it will:

1. Identify key vulnerabilities in centralized exchange security models, focusing on how the Bybit breach exploited weaknesses in cold wallet storage and user authentication mechanisms.
2. Assess the rising threat of ATO attacks, analyzing the methods used by cybercriminals to compromise exchange and user accounts.
3. Propose security strategies that cryptocurrency investors and exchanges can adopt to mitigate risks, including best practices for self-custody, multi-factor authentication improvements, and alternative trading solutions such as decentralized exchanges (DEXs).

By addressing these areas, this research seeks to provide a comprehensive framework for understanding and mitigating security risks in the cryptocurrency ecosystem. The Bybit hack serves as a critical case study illustrating the urgent need for enhanced security measures and investor education in an industry that remains highly vulnerable to cyber threats.

2. The Bybit Hack and its Implications

The Bybit hack of February 21, 2025, was the largest cryptocurrency theft in history, with attackers siphoning approximately $1.4 billion in Ethereum (ETH) and ERC-20 tokens from the exchange's cold wallet (Carter, 2025). This unprecedented breach exposed critical vulnerabilities in centralized exchange security protocols and triggered a significant market reaction.

The attack unfolded during a routine transfer from Bybit's ETH multi-signature cold wallet to its warm wallet. Hackers exploited vulnerability in the transaction signing process, manipulating the interface to display a benign transfer while executing malicious code that transferred wallet ownership (Butt, 2025). This sophisticated method allowed the attackers to bypass multi-signature security measures and drain the wallet's contents undetected (Krause, 2025).

In the aftermath of the hack, Bybit experienced a severe liquidity crisis as users rushed to withdraw their assets, resulting in a $4 billion "bank run" within 24 hours of the incident (Rodrigues, 2025). This mass exodus of funds further strained the exchange's operations and highlighted the fragility of user trust in centralized platforms. The scale and speed of these withdrawals paralleled the collapses of FTX and Celsius in 2022, where security breaches or insolvency fears led to cascading liquidity crises (Trautman and Foster, 2023; Cong *et al.*, 2025). Bybit's inability to reassure users swiftly led to significant capital outflows, posing risks of further financial instability within the digital asset market.

Bybit's reliance on periodic transfers between hot, warm, and cold wallets played a pivotal role in exposing the exchange to this attack. While cold wallets are designed to be offline and secure, they must interact with warm wallets for liquidity management. This attack revealed vulnerabilities in that transfer process, particularly in how the multi-signature verification system was manipulated (Lakshmanan, 2025). The exploit also underscores the persistent risks associated with centralized exchanges managing vast amounts of assets within single infrastructure models.

The attack has been attributed to the Lazarus Group, a North Korean state-sponsored hacking collective known for targeting cryptocurrency exchanges (Park, 2021; Lakshmanan, 2025). This attribution underscores the geopolitical implications of such large-scale cyber heists, as they potentially serve as a means for sanctioned nations to circumvent international financial restrictions.

State-sponsored cybercriminals like the Lazarus Group have increasingly leveraged cryptocurrency thefts to fund illicit activities, including weapons development and financial sanctions evasion (Kethineni and Cao, 2020). The Bybit hack aligns with previous high-profile thefts linked to North Korea, such as the 2022 Axie Infinity hack, which resulted in over $600 million in stolen funds (Alam, 2022). The scale of this latest attack raises concerns about the ability of regulatory bodies to track and recover stolen assets when powerful state actors are involved.

The Bybit incident is particularly significant as it demonstrates that even well-established exchanges with substantial security investments remain vulnerable to sophisticated attacks. While centralized exchanges have adopted advanced security measures, including multi-signature wallets, Hardware Security Modules (HSMs), and real-time monitoring, these protections have proven insufficient against highly organized cybercriminals (Shamla Tech, 2025).

The incident raises urgent questions about whether centralized exchanges can effectively secure user assets at scale. It also bolsters arguments for DEX adoption, where users retain full custody of their funds without relying on a third party's security infrastructure. However, DEXs come with their own limitations, including smart contract vulnerabilities and lower liquidity compared to CEXs.

The Bybit hack echoes previous major exchange breaches that reshaped industry security policies:

- **Mt. Gox (2014):** The collapse of Mt. Gox, once the world's largest Bitcoin exchange, resulted in a loss of approximately $460 million due to security breaches and mismanagement. This event marked the first large-scale hack that exposed the dangers of centralized custodianship (Rao and Shaen, 2022).
- **Coincheck (2018):** Japanese exchange Coincheck lost $530 million in NEM tokens after hackers exploited weaknesses in its hot wallet infrastructure (Trend Micro, 2018). This breach emphasized the importance of cold storage solutions but also highlighted the risks of transfer interactions between wallets (Tsuchiya and Hiramoto, 2021; Trend Micro, 2018).
- **FTX (2022):** Although FTX's collapse was primarily due to fraudulent financial practices rather than hacking, the subsequent draining of remaining funds by alleged insiders further demonstrated how centralized control over assets can be abused (Trautman and Foster, 2023).
- **Binance (2019):** A security breach resulted in $40 million in stolen Bitcoin from Binance's hot wallet. Binance, however, managed to reimburse affected users and overhaul security practices, showing how rapid response strategies can mitigate damage (Tiwari *et al.*, 2025).

Bybit's $1.4 billion loss represents a significantly larger scale compared to past hacking incidents. This substantial difference underscores the reality that even the strongest security systems can be compromised by increasingly sophisticated cyber threats. This breach serves as a stark reminder of the need for continuous improvement in security protocols, particularly in the management of hot and cold wallet systems, which remain a critical point of vulnerability (Shamla Tech, 2025). As the crypto industry continues to evolve, exchanges must adapt their security measures to counter increasingly sophisticated attack vectors and maintain user trust in the face of persistent threats.

3. Understanding Cryptocurrency Security and Custody

Cryptocurrency wallets play a fundamental role in securing digital assets, with different types offering varying levels of protection. Cold wallets, such as hardware wallets, are widely regarded as the most secure storage option. These devices store private keys offline, making them immune to online threats like hacking and malware (Aaron, 2024). Industry leaders such as Ledger Flex and Trezor Safe 5 employ advanced security features, including tamper-resistant chips and secure elements designed to withstand both physical and digital attacks.

Warm wallets provide a middle ground between security and usability by integrating additional security layers while maintaining a degree of online accessibility. Multi-signature (multi-sig) and Threshold Signature Schemes (TSS) are often used to distribute key management responsibilities, thereby reducing the risk of a single compromised key leading to an unauthorized transaction (Zimperium, 2025). This architecture enhances protection while allowing controlled access to funds.

Hot wallets, which remain connected to the internet, offer the highest level of accessibility but are also the most vulnerable to cyberattacks. These include software-based wallets such as Metamask, Coinbase Wallet, and Phantom, which facilitate seamless transactions but expose users to phishing, malware, and exchange breaches (QuickNode, 2025). Due to these risks, security best practices emphasize limiting the funds stored in hot wallets and implementing Two-Factor Authentication (2FA) to mitigate unauthorized access.

3.1. CEX vs. DEX: Security Trade-Offs

The security debate between centralized and decentralized exchanges revolves around trade-offs between custody, convenience, and security. CEXs provide an intuitive trading experience with liquidity and customer support but require users to entrust their assets to the platform. This custodial model creates a single point of failure, making exchanges prime targets for hackers (Rhodes, 2024). Despite stringent security investments, incidents like the Bybit hack highlight the risks associated with holding large sums of user funds in centralized custody.

DEXs, on the other hand, operate without a central authority, allowing users to retain control over their private keys. By leveraging smart contracts and blockchain-based order books, DEXs reduce counterparty risk and eliminate the need for intermediaries (Khaliq, 2024). However, security challenges persist, as vulnerabilities in smart contracts and user errors can result in irreversible losses. Protocol exploits, such as reentrancy attacks or flash loan exploits, have demonstrated that while decentralization reduces trust dependency, it does not eliminate all risks.

The choice between self-custody and exchange custody depends on a user's risk tolerance and technical expertise. While self-custody ensures full asset control, it requires rigorous security measures, including private key management and secure backups. Exchange custody offers convenience but exposes users to insolvency risks, withdrawal restrictions, and potential regulatory intervention (HiveNet, 2024).

3.2. The Risks of Keeping Crypto on Exchanges

Storing cryptocurrency on exchanges carries inherent risks, with hacking and unauthorized access being primary concerns. Even with multi-layered security measures, centralized platforms remain susceptible to sophisticated cyberattacks. The history of exchange breaches, including the Mt. Gox collapse and the recent Bybit hack, illustrates the vulnerabilities of custodial platforms (HiveNet, 2024).

Beyond hacking, users face the risk of withdrawal restrictions imposed by exchanges. Regulatory compliance measures, internal policies, and financial instability can lead to sudden limitations on fund withdrawals, preventing users from accessing their assets when needed (Khaliq, 2024). Furthermore, counterparty risk is an ongoing concern, as exchange insolvency can result in substantial financial losses. The failure of platforms like FTX exemplifies how poor risk management and opaque financial practices can erode customer confidence and lead to catastrophic consequences for users.

3.3. "Not Your Keys, Not Your Crypto"

This phrase underscores the critical importance of private key ownership in safeguarding digital assets (Levitin,

2022). Without direct control over private keys, users rely on third parties to secure their funds, leaving them vulnerable to counterparty failures and restrictions. The forced liquidation of user holdings on platforms like Robinhood and various exchange-imposed withdrawal freezes have demonstrated the risks associated with custodial reliance. The SEC investigated whether Robinhood Crypto improperly closed accounts with certain token listings but closed the investigation in 2025 without taking enforcement action (Robinhood, 2025). Despite the favorable ruling for Robinhood, the case highlights the necessity of self-custody for users seeking true financial sovereignty.

Proper private key management is essential to reducing the risk of asset loss (Courtois and Mercer, 2017). Best practices include storing keys in hardware wallets, using strong passwords and multi-factor authentication, and maintaining encrypted backups in secure locations. By prioritizing self-custody and security best practices, users can significantly enhance the protection of their cryptocurrency holdings in an increasingly hostile cyber environment.

4. Comparative Analysis of Crypto Security Strategies

The Bybit hack underscores the need for robust security strategies to mitigate account takeover risks and unauthorized access in digital asset markets. Various security measures—self-custody, two-factor authentication, and multi-signature wallets—offer various levels of protection, each with its own strengths and limitations. A comparative analysis of these methods provides insights into their effectiveness in preventing similar breaches.

4.1. Self-Custody: Maximizing Security at the Cost of Convenience

Self-custody, where users control their private keys without relying on third parties, is widely regarded as the most secure method for asset protection. Cold storage solutions, such as hardware wallets and paper wallets, offer near-impenetrable security against cyber threats (Aaron, 2024). However, the risk of loss due to misplaced seed phrases or hardware failure makes self-custody a double-edged sword. Unlike exchange-based storage, self-custody places the full responsibility of asset security on the user, demanding careful key management practices (The Holy Coins, 2024).

4.2. Two-Factor Authentication: An Essential But Imperfect Layer of Security

2FA enhances account security by requiring an additional authentication step beyond the password. App-based and hardware security keys are generally more secure than SMS-based 2FA, which is vulnerable to SIM-swapping attacks (Cryptopedia, 2020). Hardware security keys, such as YubiKeys, provide superior resistance to phishing attempts, as authentication requires physical possession of the key (Arkose Labs, 2024). Despite these advantages, attackers can still bypass 2FA through social engineering or session hijacking, highlighting the need for complementary security measures.

4.3. Multi-Signature Wallets: Reducing Single Points of Failure

Multi-signature (multisig) wallets enhance security by requiring multiple private key approvals for transactions. This structure mitigates risks associated with a single compromised key and is especially valuable for institutional investors and DeFi applications (Zimperium, 2025). However, multisig wallets introduce usability challenges, including transaction delays and key coordination complexities. Additionally, while they reduce internal fraud risks, multisig solutions remain vulnerable to sophisticated cyberattacks targeting multiple keyholders.

4.4. Comparative Effectiveness of Security Strategies

Each security measure offers trade-offs between security, usability, and risk mitigation. The Table 1 summarizes these strengths and weaknesses.

4.5. *A Layered Approach to Security*

No single security measure is sufficient to fully protect against account takeover attacks and exchange breaches. Instead, a layered approach—combining self-custody for long-term holdings, 2FA for exchange accounts, and

Table 1: Sample Size for the Study		
Security Measure	**Strengths**	**Weaknesses**
Self-Custody	Full control over assets; immune to exchange hacks	Risk of lost keys; complex for non-technical users
App-Based 2FA	Adds an extra authentication layer; mitigates password breaches	Vulnerable to phishing, social engineering
Hardware Security Keys	Strong resistance to phishing and remote attacks	Requires physical possession; not widely adopted
Multi-Signature Wallets	Reduces risk of single key compromise; ideal for institutions	Complex setup; potential coordination issues

multisig wallets for institutional use—offers the most effective defense against security threats. As cryptocurrency adoption continues to grow, users and platforms must prioritize security best practices to safeguard digital assets from evolving cyber risks.

5. How to Prevent Account Takeover Attacks

Implementing robust authentication measures is critical in preventing account takeover attacks in cryptocurrency platforms (Doerfler *et al.*, 2019). Hardware security keys and app-based 2FA provide significantly stronger protection compared to SMS-based authentication, which is vulnerable to SIM-swapping attacks and phishing attempts (Cryptopedia, 2020). Security keys such as YubiKey require physical possession to authorize access, reducing the likelihood of unauthorized logins.

Biometric authentication, including fingerprint recognition and facial scanning, adds another layer of security by utilizing unique biological characteristics (Dwivedi *et al.*, 2020). Unlike passwords or one-time passcodes, biometric data cannot be easily intercepted or replicated, making it an effective safeguard against impersonation attempts (Arkose Labs, 2024). Combining multiple authentication methods, such as biometric login with hardware security keys, further enhances security by requiring multiple factors that attackers cannot easily compromise.

5.1. Vigilant Account Monitoring and Risk Management

Proactive monitoring and risk management play a vital role in preventing account takeovers. Rate limiting on login attempts and monitoring access patterns can help detect brute-force attacks and unauthorized login attempts. Security teams should implement geofencing to restrict access from high-risk locations and block suspicious IP addresses (Cryptopedia, 2020).

Using a dedicated device for cryptocurrency transactions and avoiding public Wi-Fi or VPNs when accessing accounts can also mitigate risks. Attackers often leverage compromised networks or VPN services to bypass location-based security checks, making it crucial for users to connect through trusted networks only (Arkose Labs, 2024). Regularly auditing account activity and enabling email or app-based login notifications can alert users to unauthorized access attempts, allowing them to take swift action.

5.2. Enhancing Transaction Visibility and Security

Ensuring transparency in transaction approvals is key to preventing unauthorized fund transfers. Many account takeover attacks succeed because users blindly sign transactions without verifying their details. Avoiding blind signing and thoroughly reviewing transaction requests before approval can prevent fraudulent transfers (Maxwell, 2025).

Multi-signature wallets further enhance security by requiring multiple approvals for transactions. This setup ensures that a single compromised key does not allow attackers to access funds. For example, a 2-of-3 multi-signature wallet requires at least two authorized signers to approve a transaction, reducing the risk of unauthorized transfers due to compromised credentials (Zimperium, 2025).

5.3. Self-Custody as a Security Solution

Self-custody is one of the most effective ways to mitigate account takeover risks. Storing assets in non-custodial wallets, particularly hardware wallets for long-term holdings and warm wallets for frequently accessed funds, prevents third-party exchanges from controlling private keys (Aaron, 2024). This approach eliminates the risk of exchange breaches or insider threats leading to unauthorized withdrawals.

Diversifying asset storage across multiple wallets, including paper wallets and secure digital vaults, reduces the risk of a single point of failure. Users should also implement secure backup management, storing seed phrases in offline, tamper-resistant locations such as safety deposit boxes or encrypted USB drives (The Holy Coins, 2024). This ensures continued access to funds even if a primary device is lost or compromised. By combining strong authentication methods, vigilant account monitoring, transaction verification, and secure self-custody practices, users can significantly reduce their exposure to account takeover attacks and protect their cryptocurrency holdings.

6. Broader Implications for the Cryptocurrency Industry

The recent Bybit hack has far-reaching consequences for the cryptocurrency industry, underscoring the urgent need for improved security measures, regulatory oversight, and technological innovation. The industry's response to such security breaches will play a critical role in shaping its future resilience.

6.1. Strengthening Exchange Security Post-Hacks

Cryptocurrency exchanges have a responsibility to enhance security measures in response to major hacks. Following the Bybit breach, exchanges hopefully are implementing more robust monitoring systems, advanced authentication methods, and real-time fraud detection tools to mitigate similar risks in the future (Okwatch, 2025). Safe Wallet, for example, has introduced additional security layers, such as enhanced transaction verification and stricter withdrawal controls, to prevent unauthorized access. These improvements reflect a growing recognition that centralized exchanges must prioritize user protection through proactive security enhancements.

6.2. Regulatory Evolution and Compliance Requirements

The regulatory landscape for cryptocurrency is evolving rapidly following the election of Donald Trump with efforts to deregulate the industry (Krause, 2025). Conversely, there are increasing consumer protection security concerns. In the United States, both the Senate Banking Committee and the House Financial Services Committee have advanced bills to establish a comprehensive regulatory framework for digital assets (Tran and Matthews, 2025). These initiatives emphasize compliance with the Bank Secrecy Act, investor protections, and transparency requirements. Additionally, the SEC's newly formed task force, spearheaded by Commissioner Hester Peirce, seeks to shift from an enforcement-driven approach to a more structured regulatory framework (Carroll *et al.*, 2025). If properly implemented, balanced regulations could reduce vulnerabilities in centralized platforms and enhance consumer confidence.

6.3. The Future of Crypto Security: Self-Custody and Decentralized Identity

Beyond regulatory measures, technological advancements in self-custody and decentralized identity solutions are gaining traction as alternative security strategies. Self-custody wallets, which provide users with full control over their assets without reliance on third-party custodians, are increasingly favored for their enhanced privacy and security benefits (Withum, 2023). The shift toward self-custody aligns with the broader decentralization movement, allowing users to mitigate CEX counterparty risks.

In parallel, decentralized identity (DID) projects, such as those led by Worldcoin, are exploring the integration of biometric authentication to establish unique digital identities, thereby preventing identity fraud and unauthorized access (KuCoin, 2024). These innovations have the potential to revolutionize account security by providing cryptographic proof of identity without exposing sensitive personal information.

6.4. Multichain Security Solutions and the Path Forward

The industry is also witnessing a shift toward multichain self-custody solutions, which enable users to manage

digital assets across multiple blockchains securely (Nessi, 2025). This approach reduces reliance on single-platform security measures and enhances resilience against systemic vulnerabilities. As the cryptocurrency ecosystem continues to evolve, maintaining a balance between security, decentralization, and regulatory compliance will be essential in fostering long-term industry stability.

Ultimately, the response to major security incidents like the Bybit hack will shape the trajectory of cryptocurrency security. Exchanges, regulators, and users must collaborate to implement more robust safeguards, promote responsible innovation, and strengthen industry-wide resilience against future threats.

7. Conclusion

The Bybit hack serves as a stark reminder of the persistent security threats facing the cryptocurrency industry. This incident underscores the critical vulnerabilities that exchanges and users must address to prevent account takeovers and unauthorized asset transfers. The key lessons from this breach highlight the necessity of robust authentication mechanisms, vigilant account monitoring, and enhanced transaction security.

For investors, adopting proactive security strategies is essential in safeguarding digital assets. Relying solely on exchange-provided security measures is insufficient, as CEXs remain prime targets for cyberattacks. Instead, users should implement multi-layered defenses, including hardware security keys, biometric authentication, and transaction verification protocols, to reduce exposure to malicious actors.

Self-custody remains the most effective approach to mitigating account takeover risks. Moving assets to personal wallets, particularly cold storage solutions for long-term holdings, ensures greater control and security. Diversifying across multiple security layers—such as hardware wallets, multi-signature setups, and decentralized identity solutions—further strengthens protection against breaches. Additionally, users must adopt vigilant account management practices, including monitoring transactions, avoiding blind signing, and maintaining secure backups of private keys. As the cryptocurrency landscape evolves, the balance between innovation, security, and regulation will be pivotal in shaping a safer ecosystem.

References

Aaron, S. (2024). Understanding the Different Types of Crypto Wallets. *BitDegree*, December 9. https://www.bitdegree.org/crypto/tutorials/types-of-crypto-wallets

Alam, O. (2022). Understanding the Economies of Blockchain Games: An Empirical Analysis of Axie Infinity. Distributed Computing Group Computer Engineering and Networks Laboratory ETH Zürich. URL. https://pub. tik. ee. ethz. ch/students/2.

Arkose Labs. (2024). Cryptocurrency Account Takeover (ATO). October 6. https://www.arkoselabs.com/blog/cryptocurrency-account-takeover-ato/

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/2

Carroll, B., Maitra, N. and Perlow, M. (2025). U.S. Crypto Regulation: Key Developments in Trump's First Week. *Dechert*, January 30. https://www.dechert.com/knowledge/onpoint/2025/1/three-significant-u-s—crypto-regulatory-developments-in-the-fir.html

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/2

Cong, W., Harvey, C., Rabetti, D. and Wu, Z.Y. (2025). An Anatomy of Crypto-Enabled Cybercrimes. *Management Science*. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2023.03691

Courtois, N.T. and Mercer, R. (2017). Stealth Address and Key Management Techniques in Blockchain Systems. In *ICISSP 2017-Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, January, 559-566.

Cromley, K. (2025). $1.5 billion Crypto Heist Exposes New Security Vulnerabilities. *Cointrust*, February 24. https://www.cointrust.com/market-news/1-5-billion-crypto-heist-exposes-new-security-vulnerabilities

Cryptopedia. (2020). Account Takeover Attacks (ATO) Explained. *Gemini*, December 8. https://www.gemini.com/cryptopedia/account-takeover-attack-meaning-and-protection

Doerfler, P., Thomas, K., Marincenko, M., Ranieri, J., Jiang, Y., Moscicki, A. and McCoy, D. (2019). Evaluating Login Challenges as a Defense against Account Takeover. *In The World Wide Web Conference*, May, 372-382.

Dwivedi, R., Dey, S., Sharma, M.A. and Goel, A. (2020). A Fingerprint Based Crypto-Biometric System for Secure Communication. *Journal of Ambient Intelligence and Humanized Computing*, 11, 1495-1509.

Elad, B. (2025). Crypto Exchange Hacks and Security Statistics 2025. *CoinLaw*, February 19. https://coinlaw.io/crypto-exchange-hacks-and-security-statistics/

HiveNet. (2024). Centralized vs Decentralized Blockchain: Choosing the Best System for You. December 10. https://www.hivenet.com/post/centralized-vs-decentralized-blockchain-choosing-the-best-system-for-you

Kethineni, S. and Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, 30(3), 325-344.

Khaliq, W. (2024). Centralized vs Decentralized Crypto Exchanges. *Coin Bureau*, November 22. https://coinbureau.com/education/centralized-vs-decentralized-crypto-exchanges/

Krause, D. (2025). The $1.4 billion Bybit Hack: Cybersecurity Failures and the Risks of Cryptocurrency Deregulation. February 23, SSRN. https://ssrn.com/abstract=5150171

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

KuCoin. (2024). Best Decentralized Identity (DID) Projects to Watch in 2024. June 26. https://www.kucoin.com/learn/web3/five-best-decentralized-identity-did-projects

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.html8

Levitin, A.J. (2022). Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency. *Tex. L. Rev.*, 101, 877.

Maxwell, G. (2025). Confidential Transactions. *Elements Project*. https://elementsproject.org/features/confidential-transactions

Nessi, L. (2025). Multichain Self-Custody: What it is and Why it's Crucial for Crypto Security. January 13, CCN. https://www.ccn.com/education/crypto/multichain-self-custody-crypto-security/

Okwatch, L. (2025). Safe Wallet Enhances Security Features After Bybit Hack. *Crypto News*, February 24. https://crypto.news/safe-wallet-security-features-bybit-hack-2025/

Page, C. (2025). How Hackers Stole $1.5 billion in Crypto from Bybit's Cold Wallet. *American Banker*, February 24. https://www.americanbanker.com/news/how-north-korean-hackers-stole-1-5b-in-ethereum-from-bybit

Park, J. (2021). The Lazarus Group. *Harvard International Review*, 42(2), 34-39.

QuickNode. (2025). An Introduction to Crypto Wallets and How to Keep them Secure. January 30. https://www.quicknode.com/guides/web3-fundamentals-security/security/an-introduction-to-crypto-wallets-and-how-to-keep-them-secure

Rao, S. and Shaen, C. (2022). Mt. Gox-The Fall of a Giant. *Understanding Cryptocurrency Fraud*, 71.

Rhodes, D. (2024). Centralized Exchanges vs. Decentralized Exchanges. *Komodo Platform*, July 22. https://komodoplatform.com/en/academy/centralized-vs-decentralized-exchanges/

Robinhood. (2025). SEC Closes Investigation into Robinhood Crypto with No Action. February 24. Retrieved from https://newsroom.aboutrobinhood.com/sec-closes-investigation-into-robinhood-crypto-with-no-action/

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.html12

Sellers, M. (2025). Crypto Sent Reeling by World's Biggest Ever Heist. *InvestmentNews*, February 21. https://www.investmentnews.com/industry-news/crypto-sent-reeling-by-worlds-biggest-ever-heist/259418

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/12

The Holy Coins. (2024). Cryptocurrency Wallet Guide: Types, Setup and Best Practices. January 1. https://theholycoins.com/blog/what-is-a-cryptocurrency-wallet-a-guide-to-everything-you-need-to-know

Tiwari, M., Zhou, Y., Ferrill, J. and Smith, M. (2025). Crypto Crashes: An Examination of the Binance and FTX Scandals and Associated Accounting Challenges. *The British Accounting Review*, 101584.

Tran, H. and Matthews, B. (2025). The 2025 Crypto Policy Landscape: Looming EU and US Divergences?. *Atlantic Council*, January 29. https://www.atlanticcouncil.org/blogs/econographics/the-2025-crypto-policy-landscape-looming-eu-and-us-divergences/

Trautman, L.J. and Foster, L.D. (2023). The FTX Crypto Debacle: Largest Fraud Since Madoff?. *U. Mem. L. Rev.*, 54, 289, Trend Micro (2018, January 29).

Trend Micro. (2018). Coincheck Suffers Biggest Hack in Cryptocurrency History: Expert Users Tricked into Buying False ICO. *Trend Micro*. https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coincheck-suffers-biggest-hack-in-cryptocurrency-experty-users-buy-false-ico13

Tsuchiya, Y. and Hiramoto, N. (2021). How Cryptocurrency is Laundered: Case Study of Coincheck Hacking Incident. Forensic Science International: Reports, 4, 100241. doi: https://doi.org/10.1016/j.fsir.2021.100241

Withum. (2023). The Future of Self-Custody Wallets: How to Stay Secure in a Connected World. September 12. https://www.withum.com/resources/the-future-of-self-custody-wallets-how-to-stay-secure-in-a-connected-world/

Zimperium. (2025). Top Crypto Wallet Security Tips Every Developer Should Know. https://www.zimperium.com/glossary/crypto-wallet-security/

Cite this article as: David S. Krause (2025). Crypto Security in the Aftermath of the Bybit Hack: Evaluating Risk Management Strategies for Digital Assets. *International Journal of Cryptocurrency Research*, 5(1), 92-101. doi: 10.51483/IJCCR.5.1.2025.92-101.