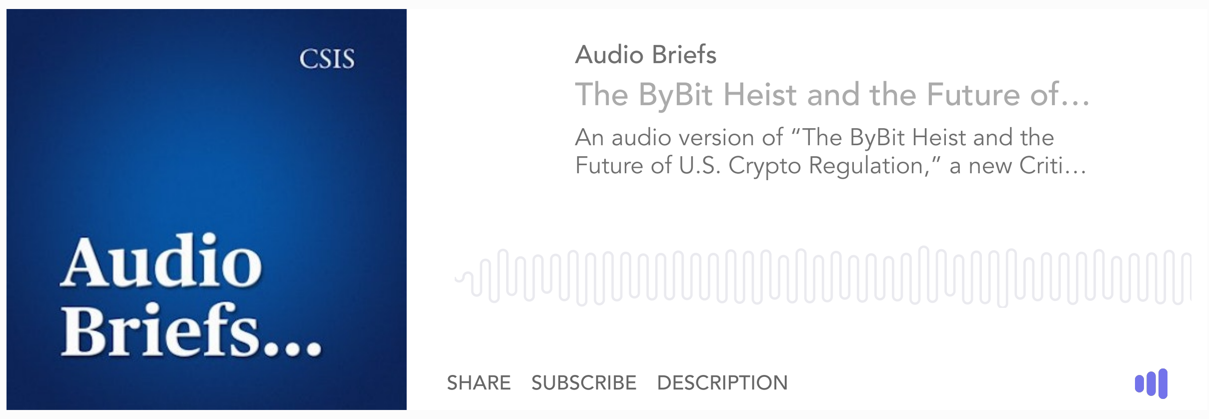
The ByBit Heist and the Future of U.S. Crypto Regulation

Photo: DANIEL DUARTE/AFP via Getty Images

Critical Questions by **Taylar Rajic** and **Julia Brock**

Published March 18, 2025



CSIS

Audio Briefs...

Audio Briefs

The ByBit Heist and the Future of...

An audio version of "The ByBit Heist and the Future of U.S. Crypto Regulation," a new Criti...

On February 21, 2025, a group of hackers from North Korea pulled off the largest cryptocurrency heist in history after stealing $1.5 billion in Ethereum tokens from the Dubai-based cryptocurrency exchange ByBit. The hackers exploited a free storage software product that ByBit used to move Ethereum to another location, most likely coupled with phishing attacks to access control and download malware. It is estimated that at least $160 million of the funds stolen from ByBit were laundered within the first 48 hours of the attack. Although ByBit does not offer services or products in the United States, the hack's ripple effects hurt the global crypto market. The price of Bitcoin experienced a 20 percent drop from its all-time high in January and renewed concerns about the security of these decentralized transactions.

The Trump administration is making cryptocurrency a bellwether of its technology policy portfolio. It has implemented a series of executive orders and meetings to achieve its goal of making the United States the "crypto capital of the planet." However, the ByBit attack highlights the concerns with crypto exchanges and their prevalence amongst North Korean criminal hacking groups.

Q1: Who is responsible for the ByBit cryptocurrency heist?

A1: The theft has been attributed to Lazarus Group, an infamous North Korean criminal hacking group that was also responsible for the 2014 attack on Sony Pictures that released emails and personal employee information and destroyed 70 percent of Sony's laptops and computers. The North Korean government routinely uses Lazarus Group, most likely under its Reconnaissance General Bureau, to commit large-scale ransomware attacks to generate funds for the country's nuclear and ballistic missile program. North Korean hackers have become prolific in stealing cryptocurrency; in 2024 more than a dozen crypto companies were infiltrated by North Korean hackers who posed as legitimate information technology (IT) workers to gain access to internal information and systems. It is estimated that

Taylar Rajic
Associate Fellow, Strategic Technologies Program

Julia Brock
Program Manager and Research Associate, Strategic Technologies Program

PROGRAMS & PROJECTS

Strategic Technologies Program

Emerging Technologies

Economic Security and Technology

Lazarus Group has stolen at least $3.4 billion in cryptocurrencies since its emergence in 2007, creating a significant source of revenue for the North Korean government.

The hackers use a variety of techniques in their operations ranging from more sophisticated cyberattacks through identifying zero-day vulnerabilities and deploying malware to steal funds, and through social-engineering techniques that prey on human vulnerabilities to deceive people into handing over sensitive information. A common technique includes hackers posing as recruiters on LinkedIn and targeting security researchers, creating rapport with them before luring them into phishing attacks. This level of sophistication has evolved from traditional email phishing attacks since increased cybersecurity measures and awareness have made these cyberattacks harder to successfully pull off. North Korea has increased its campaigns against the crypto industry after heavy sanctions continue to cripple their already isolated economy. Crypto theft provides an opportunity for funding that has a low barrier of entry with extremely high-profit opportunity. It's also harder for law enforcement to track, charge, and arrest perpetrators of these hacks than traditional modes of espionage and human intelligence.

Q2: How did the hack happen?

A2: When ByBit CEO Ben Zhou went to sign off on what appeared to be a routine transaction, the hackers intercepted the request, changed the code to make the transaction appear legitimate, and redirected the funds to their wallet instead of the intended recipient. Lazarus Group hackers obtained the stolen currency when it was moving between a cold wallet, which stores digital assets by keeping the private keys identifying a user's ownership of their digital assets offline, and a hot wallet, which stores private keys on an internet-connected server. During a routine transfer of funds, hackers exploited a vulnerability in the user interface source code of Safe Wallet, a free software platform that ByBit used in its transaction and multi-signature (multisig) process. ByBit's use of multisig was intended to protect users from a single point of failure and required several individuals, including Zhou, to sign off on every transaction. Hackers embedded malicious code into the frontend software to make the transaction appear legitimate.

This sophisticated social engineering attack has rattled members of the crypto industry, who have long-held beliefs that cold wallets and multisig are some of the most secure methods for protecting digital assets. While industry experts acknowledged that both hot and cold wallets had security risks, many believed cold wallets were more secure from online attacks given that they are, by design, not connected to the internet. Some firms even dubbed them "the best crypto wallet." ByBit had also continued using Safe Wallet despite prior knowledge that the software was not compatible with another of ByBit's security services, according to reporting from the *New York Times*. The ByBit hack has reaffirmed the importance of assessing third parties for security flaws and providing transparency at all stages of the transaction process to catch any signals that a transaction may be malicious in nature.

Q3: How can law enforcement respond to these hacks?

A3: Cryptocurrencies present a unique challenge to law enforcement, with the sheer volume of global cryptocurrency markets growing, the ability to track, catch, and convict criminal activity is becoming more difficult. In the wake of the ByBit attack, the Federal Bureau of Investigation attributed the attack to the Lazarus Group and identified Ethereum addresses linked to the stolen money, urging platforms to prevent moving funds, and therefore allowing the money to be laundered. Despite being able to identify the group and these addresses, hundreds of millions of dollars were laundered in the days following the attack, highlighting the trouble law enforcement has with effectively stopping these activities. One of the biggest issues in combating crimes that use cryptocurrency is the volume and scale that overwhelms the resources of both domestic and international law enforcement agencies. There could be solutions, however, with its underlying technology—blockchain—that could allow for investigations to follow and track stolen money.

Blockchain provides investigators with a wealth of data to analyze transactions and track where illicit funds are being moved. Transactions on blockchain are typically public, providing investigators with evidence to follow the perpetrators of stolen funds. This is particularly true of transactions that take place on U.S.-based cryptocurrency exchanges that must abide by "know your customer" laws that require financial institutions to verify customer identities and reduce the risk of fraud through anonymity. However, the global scale of cryptocurrencies makes it difficult to coordinate amongst jurisdictions when these crimes take place, particularly those that don't have similar verification requirements as the United States. Several needs have been identified that hinder effective law enforcement operations in these crimes, and some of the highest priorities include a lack of information-sharing opportunities across jurisdictions once a crime has been identified. These issues reiterate how the decentralized nature of cryptocurrencies provides unique challenges that both domestic and international law enforcement agencies need to overcome to mitigate the challenges associated with this growing technology.

Q4: Why do malicious actors use cryptocurrencies for money laundering?

A4: The decentralized nature of cryptocurrencies makes them appealing for criminal activity. The current absence of a coordinated, global regulatory framework overseeing crypto transactions makes it easier for criminals to evade law enforcement when moving large amounts of illicit transactions.

The crypto industry's current structure also allows malicious actors like the Lazarus Group to easily launder money, and there are few current incentives in place to encourage crypto trading platforms to prevent a swap or exchange of suspected laundered funds when the platform could benefit financially. Take the ByBit hack: After successfully stealing the funds, Lazarus Group hackers laundered the money by exchanging the stolen tokens for Ether through a decentralized exchange, then sending the funds to over 50 different wallets to complicate the ability for investigators to use the transparent nature of blockchains to trace the money. They then used anonymous trading platforms, such as eXch and THORChain, to swap the funds. Despite ByBit's requests to block the activity, eXch permitted the swaps, generating hundreds of thousands of dollars from the process.

Q5: What effect will this have on the future of crypto policy in the United States?

A5: President Trump has expressed interest in building a strong U.S. crypto market. Within his first few weeks in office, the Trump administration held a crypto summit at the White House and issued an executive order establishing a strategic Bitcoin reserve and a stockpile for other digital currencies. Despite these initiatives, Bitcoin has fallen into a bear market just weeks after it hit a record high of $109,071 in January. This market decline is not solely due to fears stoked by the ByBit hack: Factors such as Trump refusing to commit to a U.S. federal Bitcoin purchasing strategy as well as tariffs, recession concerns, and fears of a tech selloff have sapped risk appetite in crypto and broader financial markets.

A combination of stronger crypto regulations and improved security measures at crypto companies could spark greater consumer confidence in digital assets. The volatility in the stock market in the immediate aftermath of the attack raised questions about investor appetite for increased use of digital assets. Despite the Trump administration's actions to bring crypto into mainstream U.S. markets and financial arenas, the hack could delay increased investment given the security concerns that this attack displayed. Increased crypto activity will depend on how much investors trust these digital assets. The best avenue to increase that trust is by regulating the downsides of crypto so investors can benefit from the upsides.

Taylar Rajic is an associate fellow with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. Julia Brock is a program manager and research associate with the Strategic Technologies Program at CSIS.

Critical Questions is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).
© 2025 by the Center for Strategic and International Studies. All rights reserved.

Tags

Cybersecurity

Center for Strategic and International Studies

1616 Rhode Island Avenue, NW

Washington, DC 20036

Tel: 202.887.0200

Fax: 202.775.3199

MEDIA INQUIRIES

H. Andrew Schwartz

Chief Communications Officer

☎ 202.775.3242

✉ aschwartz@csis.org

Samuel Cestari

Media Relations Coordinator, External Relations

☎ 202.775.7317

✉ scestari@csis.org

See Media Page for more interview, contact, and citation details.

©2025 Center for Strategic & International Studies. All Rights Reserved.