How rogue nations are capitalizing on gaps in crypto regulation to finance weapons programs

Nolan Fahrenkopf, Research Fellow at Project on International Security, Commerce and Economic Statecraft, University at Albany, State University of New York

Published: December 16, 2025 8:46am EDT

Two years after Hamas attacked Israel on Oct. 7, 2023, families of the victims filed suit against Binance, a major cryptocurrency platform that has been plagued by scandals.

In a Nov. 24, 2025, filing by representatives of more than 300 victims and family members, Binance and its former CEO – recently pardoned Changpeng Zhao – were accused of willfully ignoring anti-money-laundering and so-called "know your customer" controls that require financial institutions to identify who is engaging in transactions.

In so doing, the suit alleged that Binance and Zhao – who in 2023 pleaded guilty to money laundering violations – allowed U.S.-designated terrorist entities such as Hamas and Hezbollah to launder US$1 billion. Binance has declined to comment on the case but issued a statement saying it complies "fully with internationally recognized sanctions laws."

The problem the Binance lawsuit touches upon goes beyond U.S.-designated terrorist groups.

As an expert in countering the proliferation of weapons technology, I believe the Binance-Hamas allegations could represent the tip of the iceberg in how cryptocurrency is being leveraged to undermine global security and, in some instances, U.S. national security.

Cryptocurrency is aiding countries such as North Korea, Iran and Russia, and various terror- and drug-related groups in funding and purchasing billions of dollars worth of technology for illicit weapons programs.

Though some enforcement actions continue, I believe the Trump administration's embrace of cryptocurrency might compromise the U.S.'s ability to counter the illicit financing of military technology.

In fact, experts such as professor Yesha Yadav, professor Hilary J. Allen and Graham Steele, anti-corruption advocacy group Transparency International and even the U.S. Treasury itself warn it and other legislative loopholes could further risk American national security.

A tool to evade sanctions

For the past 13 years, the Project on International Security, Commerce, and Economic Statecraft, where I serve as a research fellow, has conducted research and led industry and government outreach to help countries counter the proliferation of dangerous weapons technology, including the use of cryptocurrency in weapons fundraising and money laundering.

Over that time, we have seen an increase in cryptocurrency being used to launder and raise funds for weapons programs and as an innovative tool to evade sanctions.

Efforts by state actors in Iran, North Korea and Russia rely on enforcement gaps, loopholes and the nebulous nature of cryptocurrency to launder and raise money for purchasing weapons technology. For example, in 2024 it was thought that around 50% of North Korea's foreign currency came from crypto raised in cyberattacks.

Modern-day bank robbers?

iStock/Getty Images Plus

A digital bank heist

In February 2025, North Korea stole over $1.5 billion worth of cryptocurrency from Bybit, a cryptocurrency exchange based in the United Arab Emirates. Such attacks can be thought of as a form of digital bank heist. Bybit was executing regular transfers of cryptocurrency from cold offline wallets – like a safe in your home – to "warm wallets" that are online but require human verification for transactions.

North Korean agents duped a developer working at a service used by Bybit to install malware that granted them access to bypass the multifactor authentication. This allowed North Korea to reroute the crypto transfers to itself. The funds were moved to North Korean-controlled wallets but then washed repeatedly through mixers and multiple other crypto currencies and wallets that serve to hide the origin and end location of the funds.

While some funds have been recovered, many have disappeared.

The FBI eventually linked the attack to the North Korean cyber group TraderTraitor, one of many intelligence and cyber units engaging in cyberattacks.

Lagging behind on security

Cryptocurrency is attractive because of the ease with which it can be acquired and transferred between accounts and various digital and government-issued currencies, with little to no requirements to identify oneself.

And as countries such as Russia, Iran and North Korea have become constricted by international sanctions, they have turned to cryptocurrency to both raise funds and purchase materials for weapons programs.

Even stablecoins, promoted by the Trump administration as safer and backed by hard currency such as the U.S. dollar, suffer from extensive misuse linked to funding illicit weapons programs and other activities.

Traditional financial networks, while not immune from money laundering, have well-established safeguards to help prevent money being used to fund illicit weapons programs.

But recent analysis shows that despite enforcement efforts, the cryptocurrency industry continues to lag behind when it comes to enforcing anti-money-laundering safeguards. In at least some cases this is willful, as some crypto firms may attempt to circumvent controls for profit motives, ideological reasons or policy disputes over whether platforms can be held accountable for the actions of individual users.

It isn't only the raising of these funds by rogue nations and terrorist groups that poses a threat, though that is often what makes headlines. A more pressing concern is the ability to quietly launder funds between front companies. This helps actors avoid the scrutiny of traditional financial networks as they seek to move funds from other fundraising efforts or firms they use to purchase equipment and technology.

The incredible number of crypto transactions, the large number of centralized and decentralized exchanges and brokers, and limited regulatory efforts have made crypto incredibly useful for laundering funds for weapons programs.

This process benefits from a lack of safeguards and "know your customer" controls that banks are required to follow to prevent financial crimes. These should, I believe, and often do apply to entities large and small that help move, store or transfer cryptocurrency known as virtual asset service providers, or VASPs. However, enforcement has proven difficult as there are an incredibly large number of VASPs across numerous jurisdictions. And jurisdictions have fluctuating capacity or willingness to implement controls.

The cryptocurrency industry, though supposedly subject to many of these safeguards, often fails to implement the rules, or it evades detection due to its decentralized nature.

Digital funds, real risk

The rewards for rogue nations and organizations such as North Korea can be great.

Ever the savvy sanctions evader, North Korea has benefited the most from its early vision on the promise of crypto. The reclusive country has established an extensive cyber program to evade sanctions that relies heavily on cryptocurrency. It is not known how much money North Korea has raised or laundered in total for its weapons program using crypto, but in the past 21 months it has stolen at least $2.8 billion in crypto.

Iran has also begun relying on cryptocurrency to aid in the sale of oil linked to weapons programs – both for itself and proxy forces such as the Houthis and Hezbollah. These efforts are fueled in part by Iran's own crypto exchange, Nobitex.

Russia has been documented going beyond the use of crypto as a fundraising and laundering tool and has begun using its own crypto to purchase weapons material and technology that fuel its war against Ukraine.

A threat to national security

Despite these serious and escalating risks, the U.S. government is pulling back enforcement.

The controversial pardon of Binance founder Changpeng Zhao raised eyebrows for the signal it sends regarding U.S. commitment to enforcing sanctions related to the cryptocurrency industry. Other actions such as deregulating the banking industry's use of crypto and shuttering the Department of Justice's crypto fraud unit have done serious damage to the U.S.'s ability to interdict and prevent efforts to utilize cryptocurrencies to fund weapons programs.

The U.S. has also committed to ending "regulation by prosecution" and has withdrawn numerous investigations related to failing to enforce regulations meant to prevent tactics used by entities such as North Korea. This includes abandoning an admittedly complicated legal case regarding sanctions against a "mixer" allegedly used by North Korea.

These actions, I believe, send the wrong message. At this very moment, cryptocurrency is being illicitly used to fund weapons programs that threaten American security. It's a real problem that deserves to be taken seriously.

And while some enforcement actions do continue, failing to implement and enforce safeguards up front means that crypto will continue to be used to fund weapons programs. Cryptocurrency has legitimate uses, but ignoring the laundering and sanctions-evasion risks will damage American national interests and global security.

Nolan Fahrenkopf is a research fellow at the Center for Policy Research at the University at Albany, which receives grants related to nonproliferation from the U.S. Department of State and Department of Energy.