

# North Korea's nuclear program is funded by stolen cryptocurrency. Could it collapse now that FTX has?

December 1 2022, by James Jin Kang



Credit: CC0 Public Domain

Since the world's second-largest crypto exchange, FTX, [declared bankruptcy](#) earlier this month, the [flow-on effects](#) have been felt [far and](#)

[wide](#).

But among the many victims are also some not-so-innocent parties. For the Democratic People's Republic of Korea, a country facing heavy sanctions, cryptocurrency theft has been a (relatively) [simple way](#) to fund the country's expanding [nuclear arsenal](#).

It's well [documented](#) that Kim Jong-un's military operation hackers have been [stealing cryptocurrency](#) to support North Korea's [nuclear and missile program](#) for several years.

But with the general downturn in the crypto market, coupled with the recent FTX collapse and myriad [other pitfalls](#), analysts estimate North Korea has probably lost most of its [crypto haul](#).

Can we expect its nuclear weapons development to come to a halt, or slow down? It seems unlikely.

## **What North Korea's hackers have been up to**

North Korea sponsors several hacker groups, including [Lazarus Group](#) (also called Guardian of Peace and Whois Team) and Advanced Persistent Threat 38 ([APT38](#)).

While nobody knows exactly how many North Korea-backed hackers there are, experts [have estimated](#) Kim Jong-un has between [6,000 and 7,000](#) working both inside and outside the country.

North Korea has invested in its national cybercrime arsenal [for some 15 years](#). It's almost impossible for an organization to defend itself against an army of this size and caliber once it comes charging.

In 2016, Lazarus hackers came close to [stealing US\\$1 billion](#) from

Bangladesh's national bank—but a typo in the computer code meant they only got away with US\$81 million.

Since then, they've refined their methods. Lazarus has been accused of stealing [US\\$571 million](#) from cryptocurrency exchanges between January 2017 and September 2018, [US\\$316 million](#) from 2019 to November 2020, and US\$840 million in [the first five months](#) of 2022.

According to Chainalysis, North Korean hackers have [stolen an estimated](#) total of about US\$1 billion in cryptocurrency this year. A large chunk of this would have come from Lazarus' massively lucrative heist against NFT-based online game Axie Infinity. In April, US authorities held the group responsible for stealing [US\\$620 million](#) in cryptocurrency from the game.

For context, it's [estimated](#) North Korea only earned about US\$142 million from trade exports in 2020.

## Okay, so how much has it now lost?

It's difficult to say exactly how much cryptocurrency has been stolen (and used) by North Korean hackers—and therefore how much might remain.

In June, blockchain analyst and former FBI analyst Nick Carlsen [told Reuters](#) one of North Korea's crypto caches had lost 80% to 85% of its value in a number of weeks, falling to less than US\$10 million.

Losses will have intensified following the FTX collapse. According to a [Chainalysis report](#), in January North Korea held about US\$170 million in stolen unlaundersed cryptocurrency, taken from 49 hacks conducted from 2017 to 2021. It also claims Ether was the most common cryptocurrency stolen by North Korea in 2021, making up 58% of the total theft.

[Ether's value](#) fell by more than 20% following the FTX crash, and remains low. It's reasonable to expect North Korea will wait before cashing out. When it does, experts looking on will be in a better place to figure out how much it has.

## **Why steal crypto to fund nuclear weapons tests?**

The United States, South Korea and Japan [have been warning](#) North Korea against conducting a seventh nuclear test. But Kim Jong-un doesn't seem to be letting up. On Saturday, at the launch of North Korea's largest ballistic missile yet, he [told state media](#) the "ultimate goal is to possess the world's most powerful strategic force, the absolute force unprecedented in the century."

International sanctions and border closures due to COVID-19 have made it difficult for North Korea to trade and generate funds through other means—which makes the cryptocurrency market an attractive target.

Cryptocurrency remains unregulated by most countries' governments. At the same time, transactions can be made quickly, and allow more anonymity than transactions made through traditional banking systems.

It's also easier to hack a cryptocurrency exchange than it is to hack a bank. The latter are almost always bolstered by advanced security barriers and sometimes require in-person appearances.

## **No more missile tests, for now?**

The rapid drop in crypto's value, compounded by the FTX crash, will have certainly left a dent in North Korea's nuclear military expansion funds. Nonetheless, Kim Jong-un's cybercriminal army will likely find new sources of illicit income (and will probably keep stealing crypto

too).

North Korea [has](#) also [had financial support](#) from supporters in South Korea who follow the "Juche" ideology—the same Marxist-Leninist-adjacent political philosophy imposed in North Korea.

And in April American crypto expert Virgil Griffith [pleaded guilty](#) to helping North Korea evade US sanctions through using [cryptocurrency](#).

Then there's China—a key player in deciding whether sanctions against North Korea will actually work. In May, China joined Russia [in vetoing](#) a draft proposal from the US to tighten sanctions against North Korea, and continues to [trade with it](#).

As long as North Korea can glean [financial benefit](#) from China, and other avenues as mentioned above, it's unlikely to stop its plans.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: North Korea's nuclear program is funded by stolen cryptocurrency. Could it collapse now that FTX has? (2022, December 1) retrieved 23 April 2024 from <https://techxplore.com/news/2022-12-north-korea-nuclear-funded-stolen.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.