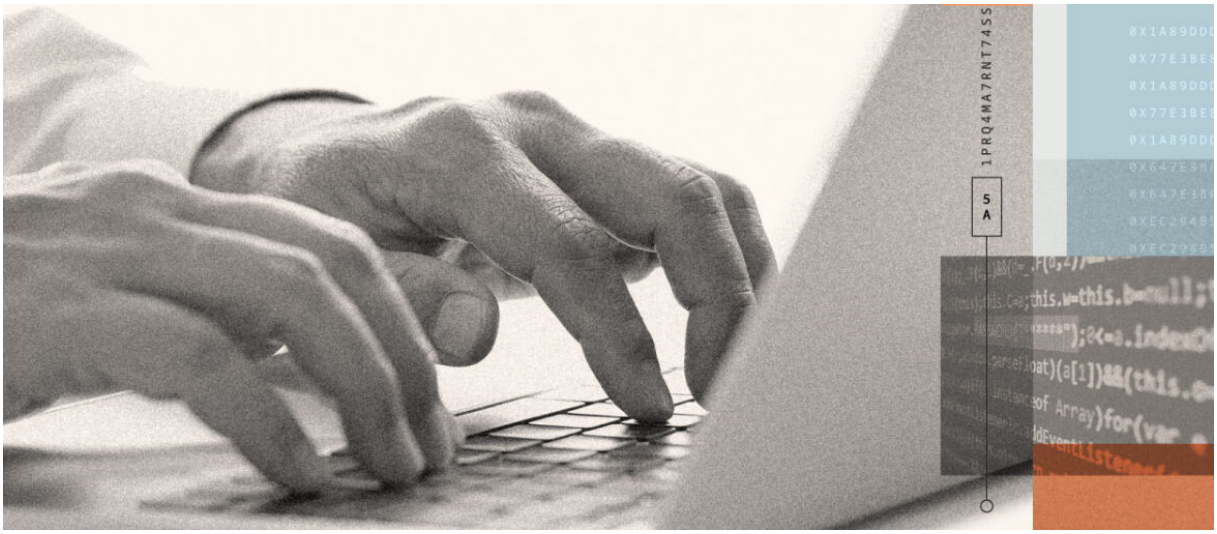
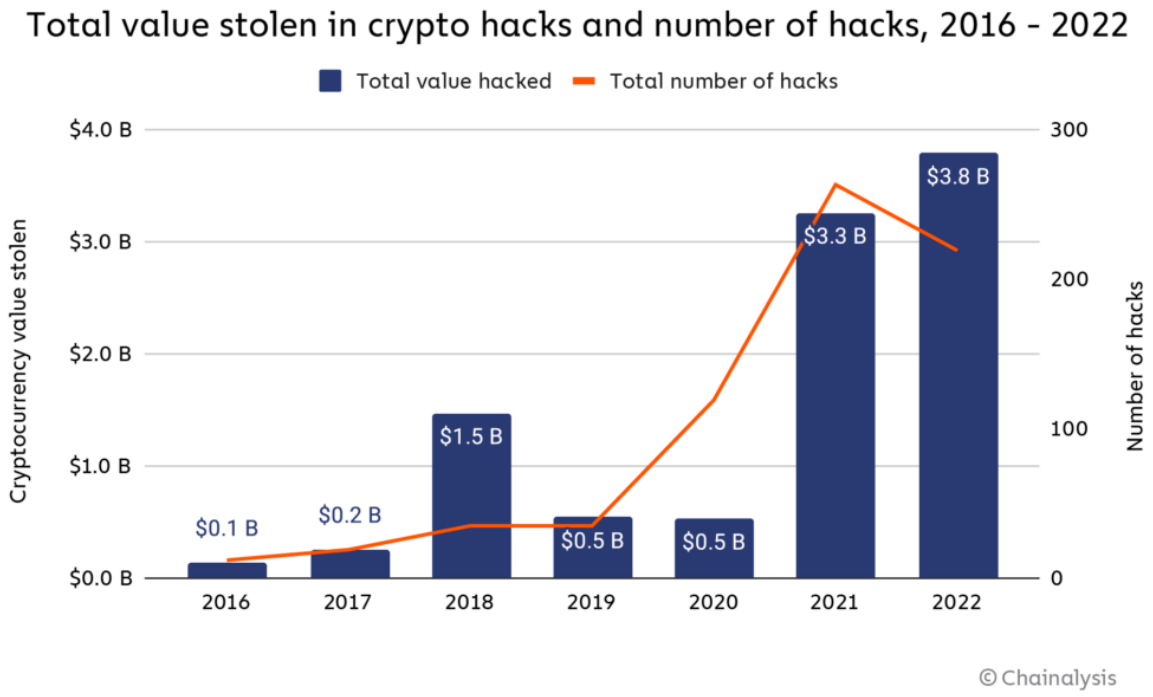
# 2022 Biggest Year Ever For Crypto Hacking

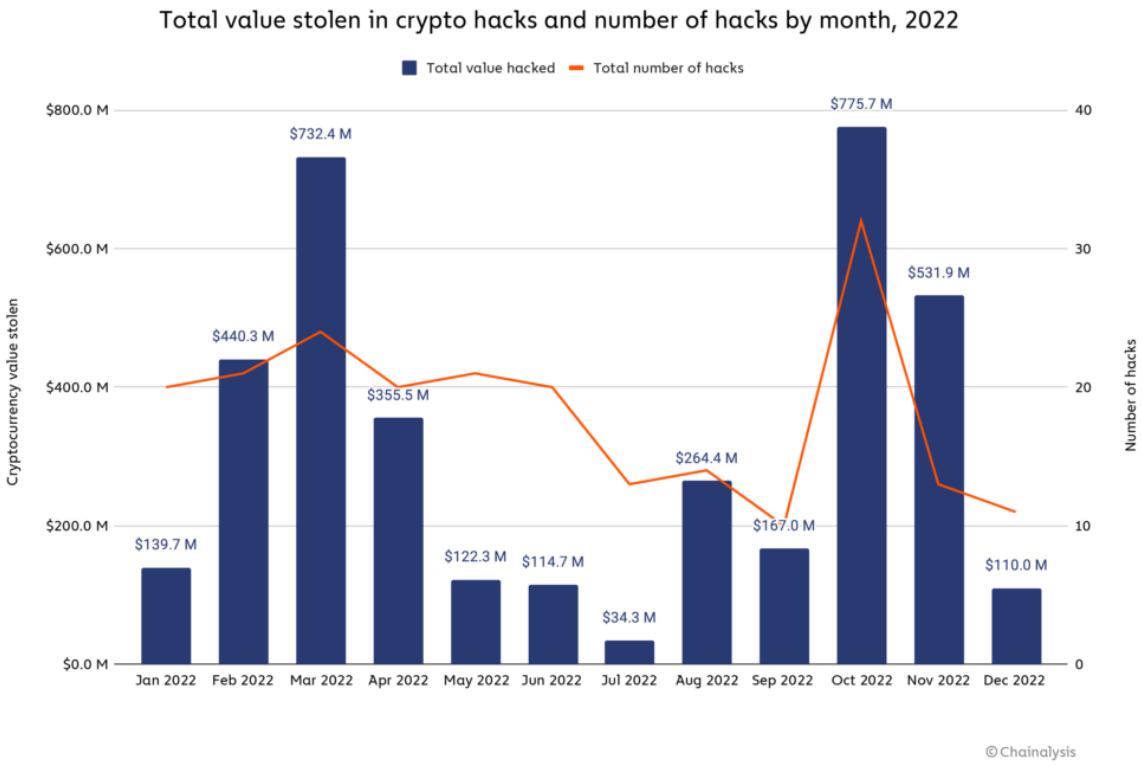


2022 was the biggest year ever for crypto hacking, with $3.8 billion stolen from cryptocurrency businesses.




Hacking activity ebbed and flowed throughout the year, with huge spikes in March and October, the latter of which became the biggest single month ever

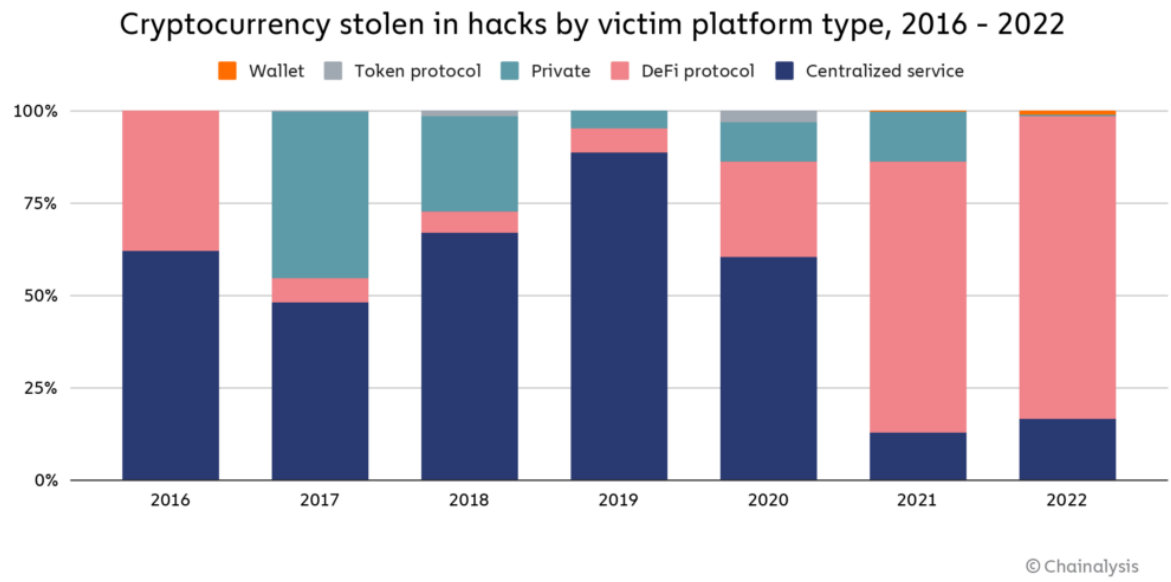
for cryptocurrency hacking, as $775.7 million was stolen in 32 separate attacks.




Below, we'll dive into what kinds of platforms were most affected by hacks, and take a look at the role of North Korea-linked hackers, who drove much of 2022's crypto hacking activity and shattered their own yearly record for most cryptocurrency stolen.

## DeFi protocols by far the biggest victims of cryptocurrency hacks

In last year's Crypto Crime Report, we wrote about how decentralized finance (DeFi) protocols in 2021 became the primary target of crypto hackers. That trend intensified in 2022.




DeFi protocols as victims accounted for 82.1% of all cryptocurrency stolen by hackers — a total of $3.1 billion — up from 73.3% in 2021. And of that $3.1 billion, 64% came from cross-chain bridge protocols specifically. Cross-chain bridges are protocols that let users port their cryptocurrency from one blockchain to another, usually by locking the user's assets into a smart contract on the original chain, and then minting equivalent assets on the second chain. Bridges are an attractive target for hackers because the smart contracts in effect become huge, centralized repositories of funds backing the assets that have been bridged to the new chain — a more desirable honeypot could scarcely be imagined. If a bridge gets big enough, any error in its underlying smart contract code or other potential weak spot is almost sure to eventually be found and exploited by bad actors.

## How do we make DeFi safer?

DeFi is one of the fastest-growing, most compelling areas of the cryptocurrency ecosystem, largely due to its transparency. All transactions happen on-chain, and the smart contract code governing DeFi protocols is publicly viewable by default, so users can know exactly what will happen to their funds when they use them. That's especially attractive now in 2023, as many of the crypto market blowups of the past year were due to a lack of transparency into the actions and risk profiles of centralized cryptocurrency businesses. But that same transparency is also what makes DeFi so vulnerable — hackers can scan DeFi code for vulnerabilities and strike at the perfect time to maximize their theft.

DeFi code auditing conducted by third-party providers is one possible remedy to this. Blockchain cybersecurity firm Halborn is one such provider, and is notable for its clean track record — no DeFi protocol to pass a Halborn audit

has subsequently been hacked. We spoke with Halborn COO David Schwed, whose background includes stints in risk and security at large banks like BNY Mellon, about how DeFi protocols can better protect themselves. He emphasized that many of the issues in DeFi come down to a lack of investment in security. “A big protocol should have 10 to 15 people on the security team, each with a specific area of expertise,” he told us. He indicated that the core issue is that DeFi developers prioritize growth over all else, and direct funds that could fund security measures to rewards in order to attract users. “The DeFi community generally isn’t demanding better security — they want to go to protocols with high yields. But those incentives lead to trouble down the road.”

Schwed told us that DeFi developers should look to traditional financial institutions for examples of how to make their platforms more secure. “You don’t need to move as slow as a bank, but you can borrow from what banks do.” Some measures he recommends include:

- **Test protocols with simulated attacks.** DeFi developers can simulate different hacking scenarios on testnets in order to test how their protocol stands up to the most common attack vectors.

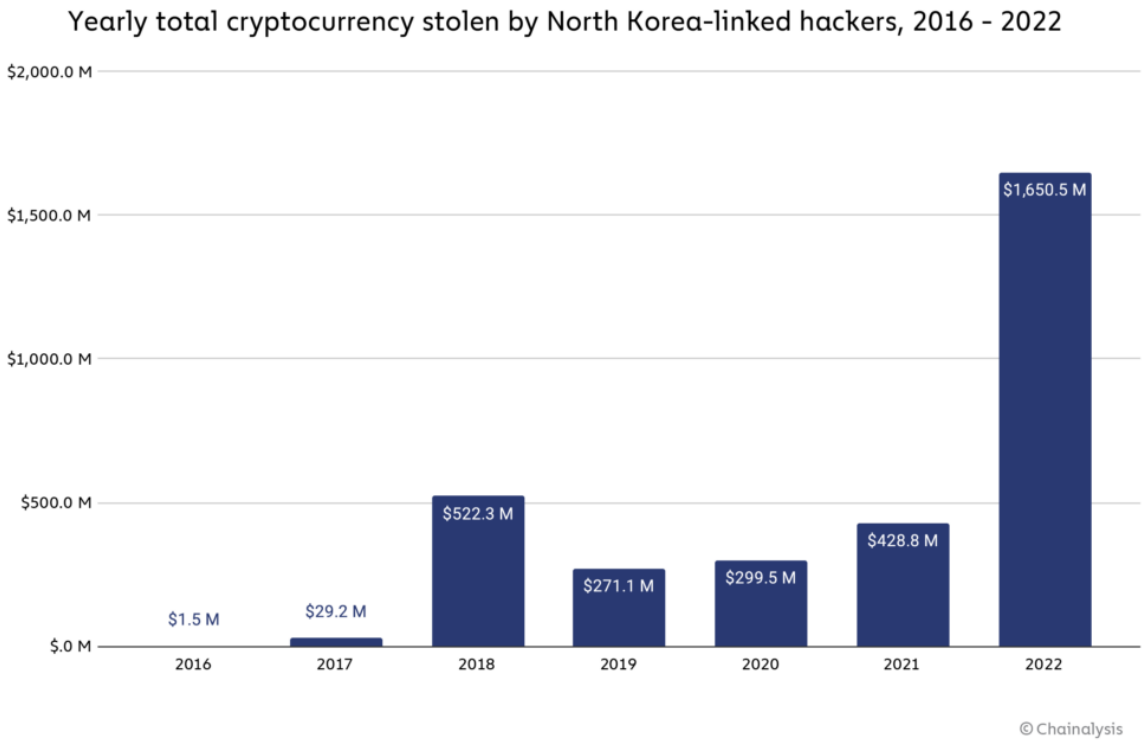
- **Take advantage of crypto’s transparency.** One huge advantage of a blockchain like Ethereum is that transactions are visible in the mempool before they’re confirmed on the blockchain. Schwed recommended that DeFi developers monitor the mempool closely for suspicious activity on their smart contracts to detect possible attacks as early as possible.
- **Circuit breakers.** DeFi protocols should build out automated processes to pause their protocols and halt transactions if suspicious activity is detected. “It’s better to briefly inconvenience users than to have the entire protocol get drained,” said Schwed.

Schwed also told us that regulators have a role to play here, and can help make DeFi safer by setting minimum security standards that protocol developers must follow. The data on DeFi hacks makes one thing clear: Whether achieved through regulation or voluntary adoption, DeFi protocols will greatly benefit from adopting better security in order for the ecosystem to grow, thrive, and eventually penetrate the mainstream.

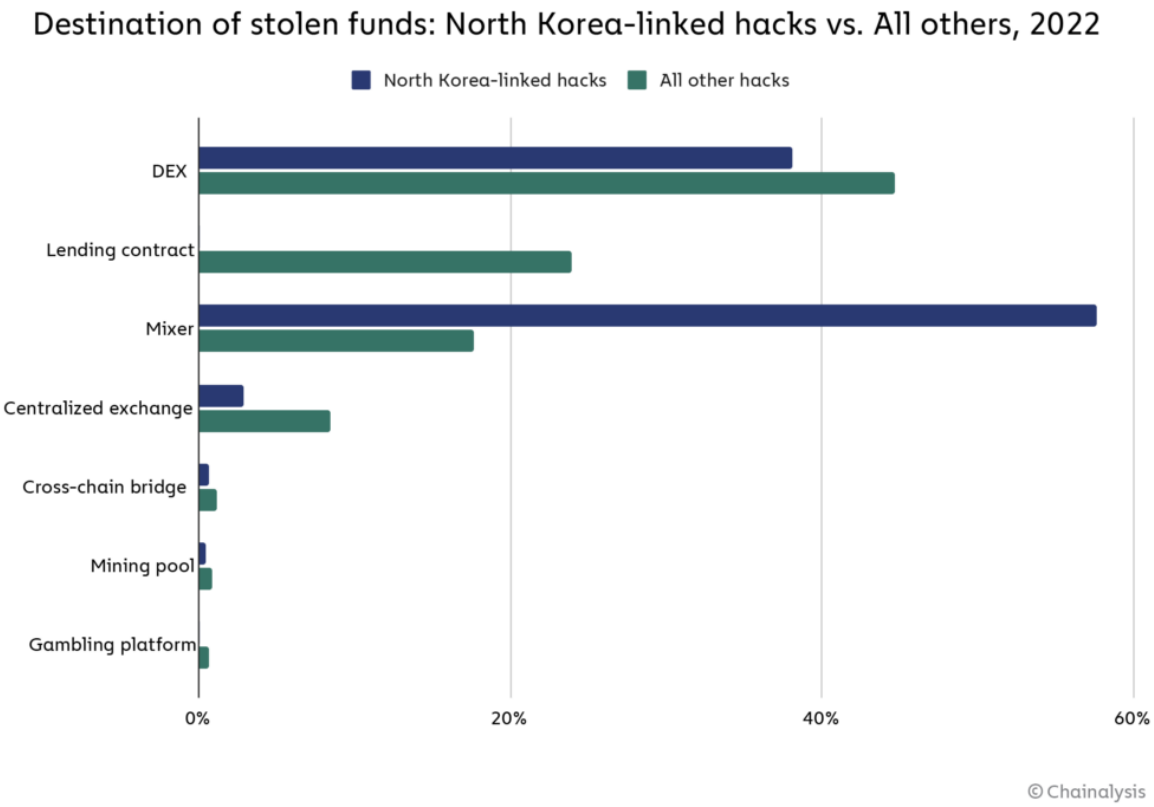
## North Korea-linked hackers break theft records yet again: $1.7 billion stolen

North Korea-linked hackers such as those in cybercriminal syndicate Lazarus Group have been by far the most prolific cryptocurrency hackers over the last few years. In 2022, they shattered their own records for theft, stealing an

estimated $1.7 billion worth of cryptocurrency across several hacks we've attributed to them. For context, North Korea's total exports in 2020 totalled $142 million worth of goods, so it isn't a stretch to say that cryptocurrency hacking is a sizable chunk of the nation's economy. Most experts agree the North Korean government is using these stolen to fund its nuclear weapons programs.



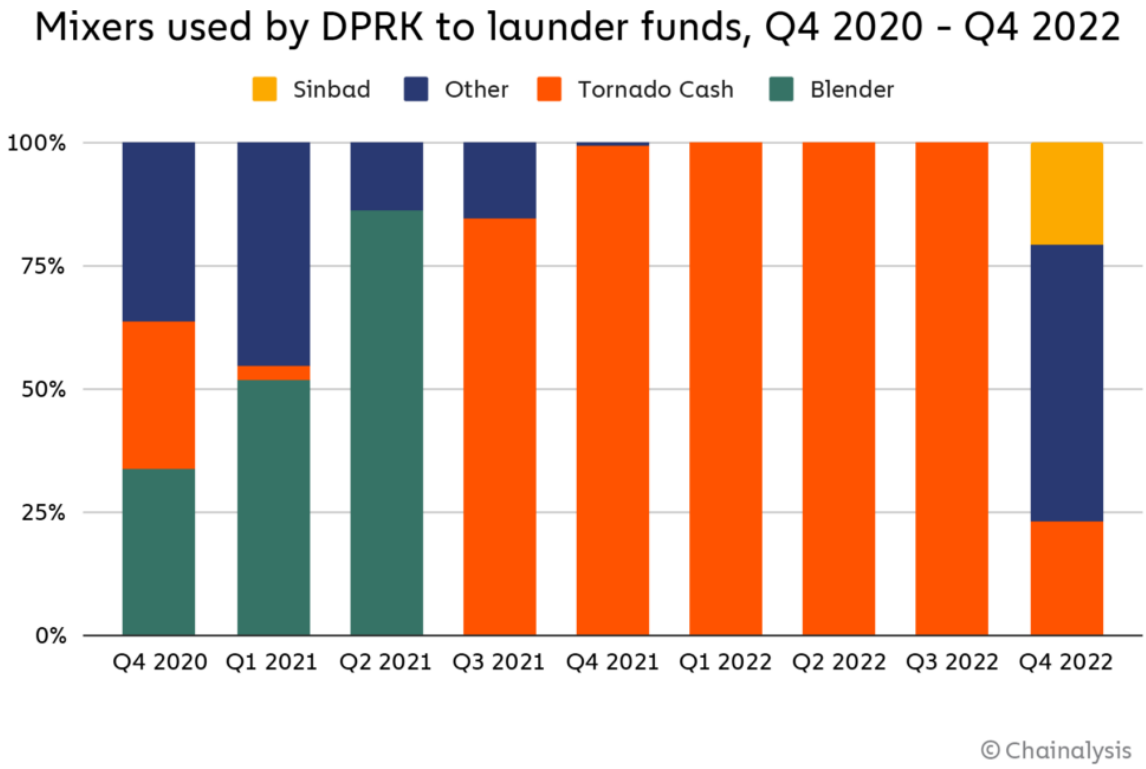

$1.1 billion of that total was stolen in hacks of DeFi protocols, making North Korea one of the driving forces behind the DeFi hacking trend that intensified in 2022. North Korea-linked hackers tend to send much of what they steal to other DeFi protocols, not because these protocols are effective for money laundering — they're actually quite bad for money laundering given their increased transparency compared to centralized services — but rather because DeFi hacks often result in cybercriminals acquiring large quantities of illiquid tokens that aren't listed at centralized exchanges. The hackers therefore must turn to other DeFi protocols, usually DEXes, to swap for more liquid assets.




Besides DeFi protocols, North Korea-linked hackers also tend to send large sums to mixers, which have typically been the cornerstone of their money laundering process. In fact, funds from hacks carried out by North Korea-linked hackers move to mixers at a much higher rate than funds stolen by other individuals or groups. But which mixers do they use? We'll dig in below.

## Meet the new mixer North Korean hackers have turned to following Tornado Cash's OFAC designation

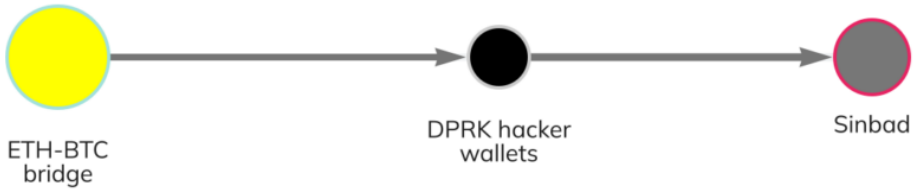
For much of 2021 and 2022, North Korea-linked hackers almost exclusively used Tornado Cash to launder cryptocurrency stolen in hacks. It's not hard to see why — Tornado Cash was for a time the biggest mixer operating, and its unique technical attributes made the funds it mixed relatively difficult to trace.




However, the hackers adapted when Tornado Cash was sanctioned in August 2022. While North Korea-linked hackers have still sent some funds to Tornado Cash since then, we can see above that they diversified their mixer usage in Q4 2022, soon after the mixer's designation. This may be due to the fact that, while still operational, Tornado Cash's overall transaction volume has fallen since its designations, and mixers generally become less effective when fewer people are using them. Since then, the hackers have turned to another mixer, Sinbad, which we'll look at in more detail below.

## Sinbad

Sinbad is a relatively new custodial Bitcoin mixer that began advertising its services on the BitcoinTalk forum in October 2022. Chainalysis investigators first observed wallets belonging to North Korea-linked hackers sending funds to the service in December 2022, which we can see on the Chainalysis Reactor graph below.




As we've seen in many North Korea-directed hacks, the hackers bridge the stolen funds from the Ethereum blockchain — including a portion of the funds stolen in the Axie Infinity hack — to Bitcoin, then sending that Bitcoin to Sinbad. During December 2022 and January 2023, North Korea-linked hackers have sent a total of 1,429.6 Bitcoin worth approximately $24.2 million to the mixer.

While North Korea-linked hackers are undoubtedly sophisticated and represent a significant threat to the cryptocurrency ecosystem, law enforcement and national security agencies' ability to fight back is growing. Last year, for example, we saw the first ever seizure of funds stolen by North Korea-linked hackers, when agents recovered $30 million worth of cryptocurrency stolen in the Axie Infinity Ronin Bridge hack. We expect more such stories in the coming years, largely due to the transparency of the blockchain. When every transaction is recorded in a public ledger, it means that law enforcement always has a trail to follow, even years after the fact, which is invaluable as investigative techniques improve over time. Their growing capabilities, combined with the efforts of agencies like OFAC to cut off hackers' preferred money laundering services from the rest of the crypto ecosystem, means that these hacks will get harder and less fruitful with each passing year.