North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High

blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high

January 13, 2022

This blog is a preview of our 2022 Crypto Crime Report. Sign up here to reserve your copy and we'll email you the full report when it comes out in February!

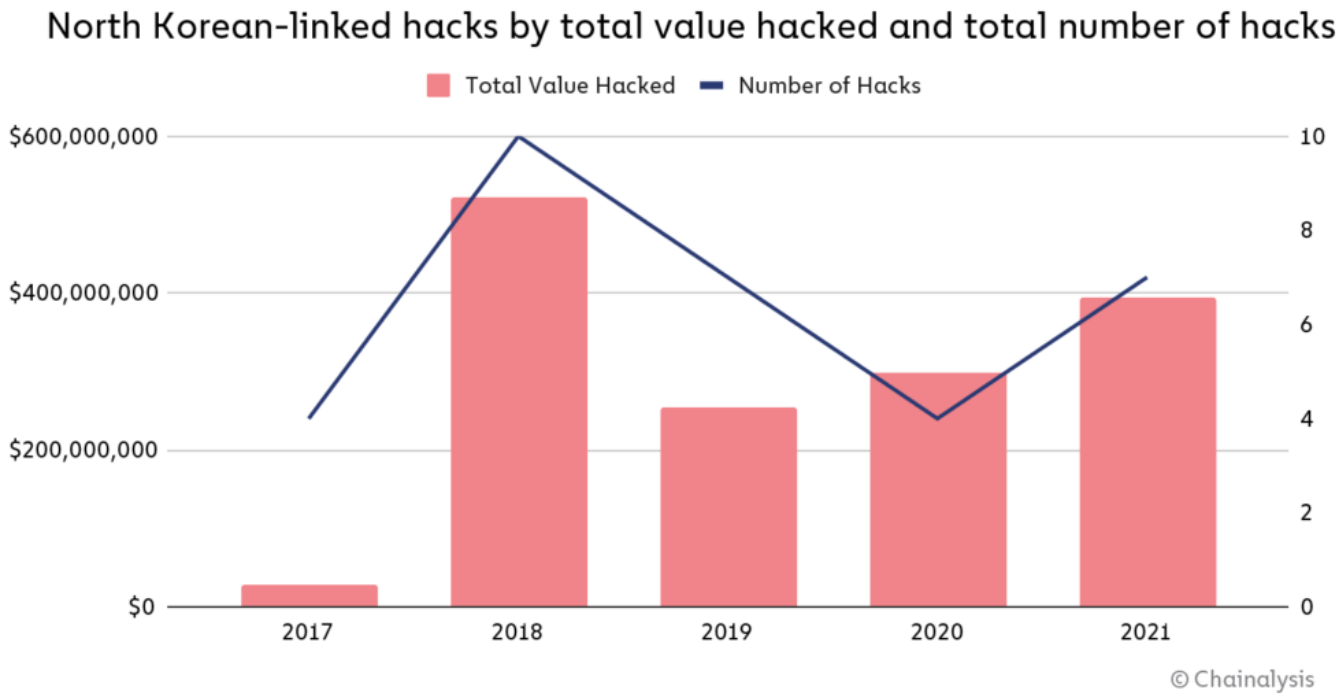
North Korean cybercriminals had a banner year in 2021, launching at least seven attacks on cryptocurrency platforms that extracted nearly $400 million worth of digital assets last year. These attacks targeted primarily investment firms and centralized exchanges, and made use of phishing lures, code exploits, malware, and advanced social engineering to siphon funds out of these organizations' internet-connected "hot" wallets into DPRK-controlled addresses. Once North Korea gained custody of the funds, they began a careful laundering process to cover up and cash out.

These complex tactics and techniques have led many security researchers to characterize cyber actors for the Democratic People's Republic of Korea (DPRK) as advanced persistent threats (APTs). This is especially true for APT 38, also known as "Lazarus Group," which is led by DPRK's primary intelligence

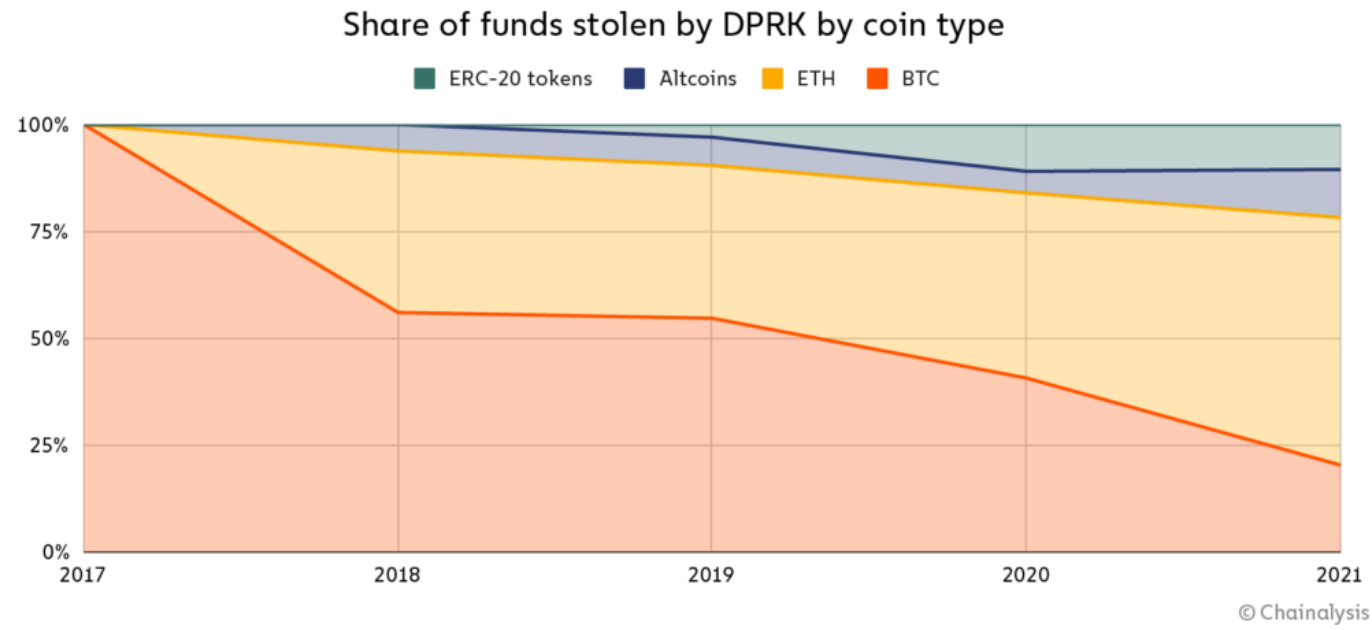
agency, the US- and UN-sanctioned Reconnaissance General Bureau. While we will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were likely carried out by the Lazarus Group in particular.

Lazarus Group first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime—a strategy that has proven immensely profitable. From 2018 on, The group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. The most successful individual hacks, one on KuCoin and another on an unnamed cryptocurrency exchange, each netted more than $250 million alone. And according to the UN security council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs.

In 2021, North Korean hacking activity was on the rise once again. From 2020 to 2021, the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40%.



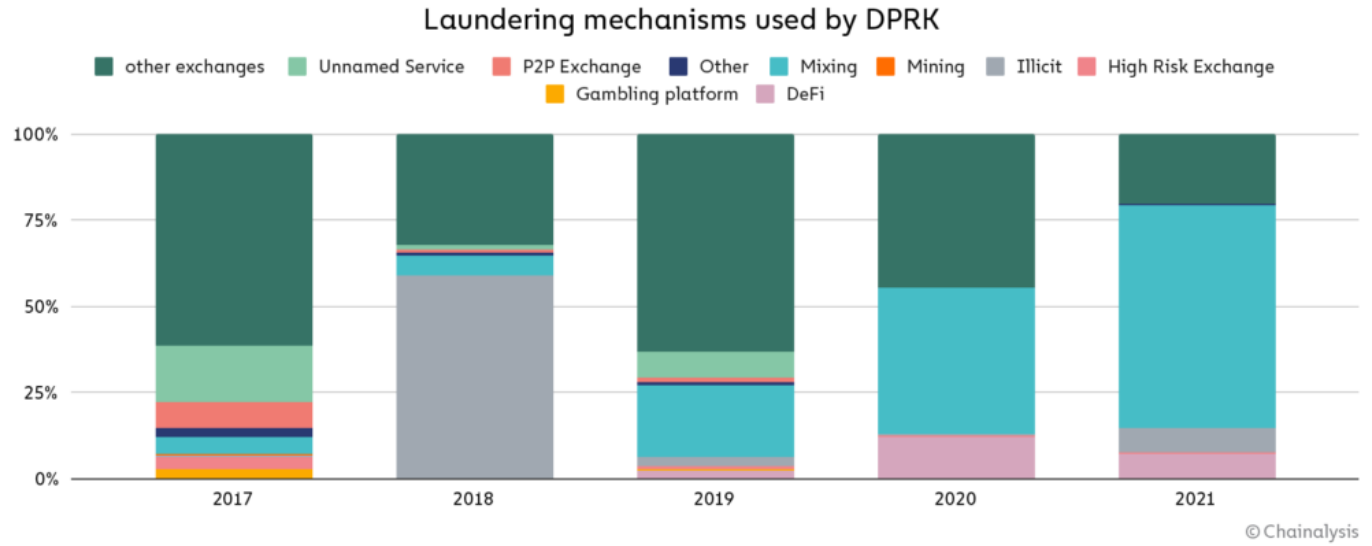
Interestingly, in terms of dollar value, Bitcoin now accounts for less than one fourth of the cryptocurrencies stolen by DPRK. In 2021, only 20% of the stolen funds were Bitcoin, whereas 22% were either ERC-20 tokens or altcoins. And for the first time ever, Ether accounted for a majority of the funds stolen at 58%.



The growing variety of cryptocurrencies stolen has necessarily increased the complexity of DPRK's cryptocurrency laundering operation. Today, DPRK's typical laundering process is as follows:

1. ERC-20 tokens and altcoins are swapped for Ether via decentralized exchange (DEX)
2. Ether is mixed
3. Mixed Ether is swapped for Bitcoin via DEX
4. Bitcoin is mixed
5. Mixed Bitcoin is consolidated into new wallets
6. Bitcoin is sent to deposit addresses at crypto-to-fiat exchanges based in Asia —potential cash-out points

In fact, we observed a massive increase in the use of mixers among DPRK-linked actors in 2021.



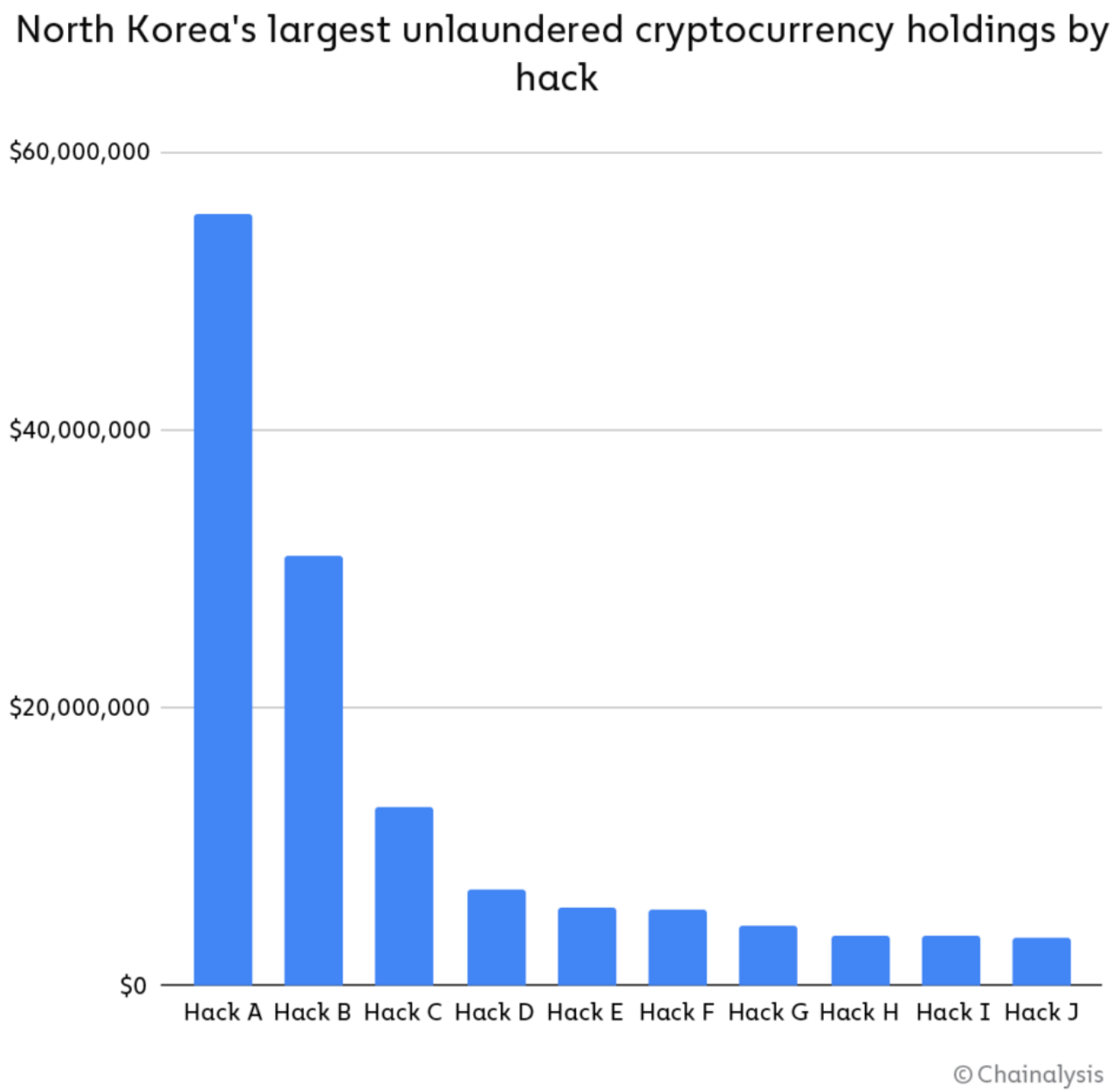
More than 65% of DPRK's stolen funds were laundered through mixers this year, up from 42% in 2020 and 21% in 2019, suggesting that these threat actors have taken a more cautious approach with each passing year.

Why mixers? DPRK is a systematic money launderer, and their use of multiple mixers —software tools that pool and scramble cryptocurrencies from thousands of addresses—is a calculated attempt to obscure the origins of their ill-gotten cryptocurrencies while offramping into fiat.

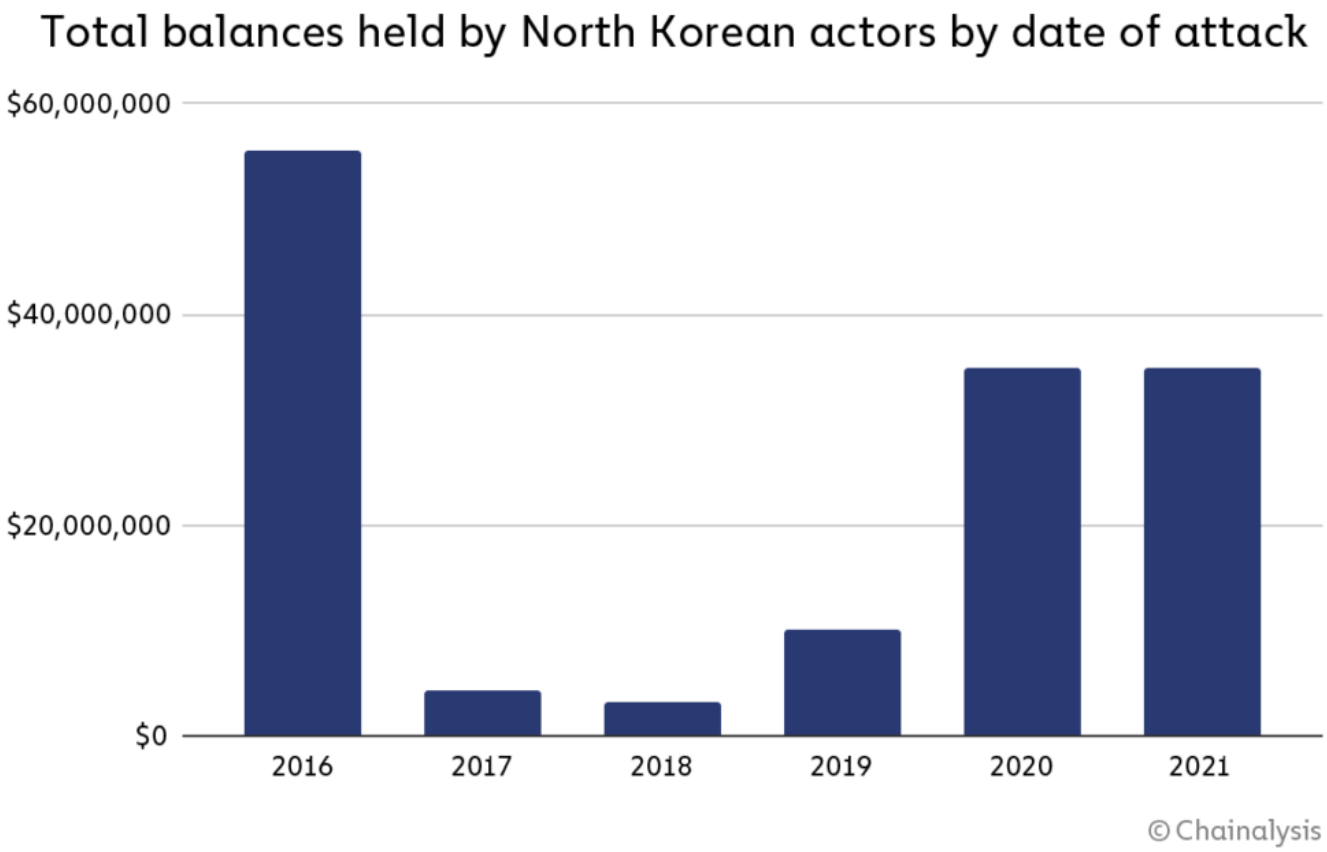
Why DeFi? DeFi platforms like DEXs provide liquidity for a wide range of ERC-20 tokens and altcoins that may not otherwise be convertible into cash. When DPRK swaps these coins for ETH or BTC they become much more liquid, and a larger variety of mixers and exchanges become usable. What's more, DeFi platforms don't take custody of user funds and many do not collect know-your-customer (KYC) information, meaning that cybercriminals can use these platforms without having their assets frozen or their identities exposed.

DPRK's stolen fund stockpile: $170 million worth of old, unlaundered cryptocurrency holdings

Chainalysis has identified $170 million in current balances—representing the stolen funds of 49 separate hacks spanning from 2017 to 2021—that are controlled by North Korea but have yet to be laundered through services. The ten largest balances by dollar value are listed below.



Of DPRK's total holdings, roughly $35 million came from attacks in 2020 and 2021. By contrast, more than $55 million came from attacks carried out in 2016—meaning that DPRK has massive unlaundered balances as much as six years old.



This suggests that DPRK-linked hackers aren't always quick to move stolen cryptocurrencies through the laundering process. It's unclear why the hackers would still be sitting on these funds, but it could be that they are hoping law enforcement interest in the cases will die down, so they can cash out without being watched.

Whatever the reason may be, the length of time that DPRK is willing to hold on to these funds is illuminating, because it suggests a careful plan, not a desperate and hasty one.

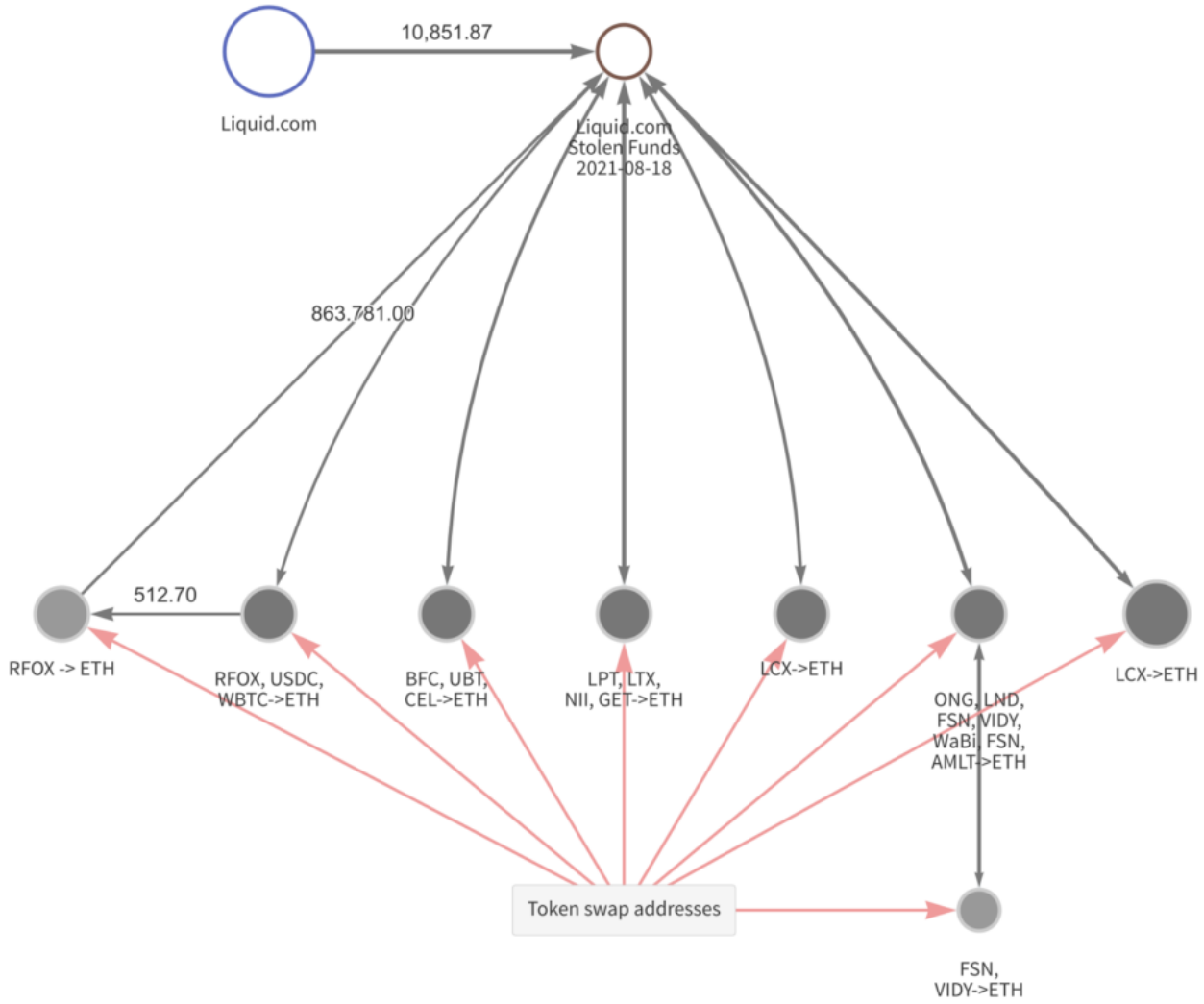
Coinswap, mix, consolidate, cash out: How North Korea-linked hackers laundered $91 million after the Liquid.com hack

On August 19th, 2021, cryptocurrency exchange Liquid.com announced that an unauthorized user had gained access to some of the cryptocurrency wallets managed by Liquid. The night before, **67 different ERC-20 tokens**, along with large quantities of Ether and Bitcoin, had been moved from these wallets to addresses controlled by a party working on behalf of DPRK.

The attacker then used decentralized protocols to swap the various ERC-20 tokens for Ether. From there, they mixed the Ether, swapped the mixed Ether for Bitcoin, mixed the Bitcoin, consolidated the mixed Bitcoin into new wallets, and then deposited the funds into crypto-to-fiat exchanges based in Asia. As a result, approximately $91.35M in cryptoassets was laundered.

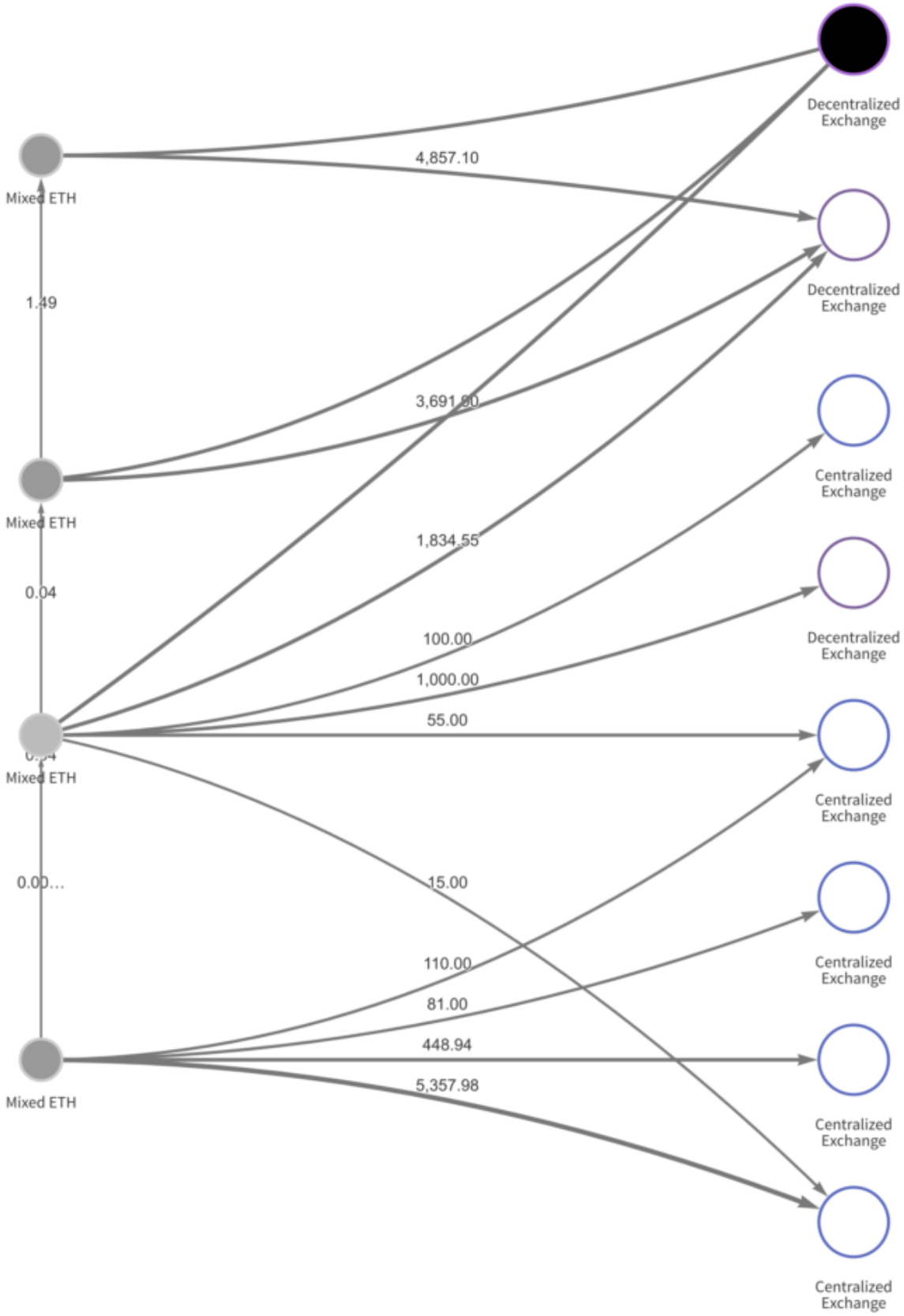
Below, we've visualized each stage of the laundering process in Chainalysis Reactor.

Stage 1: Stolen ERC-20 tokens swapped for Ether at DEXs:

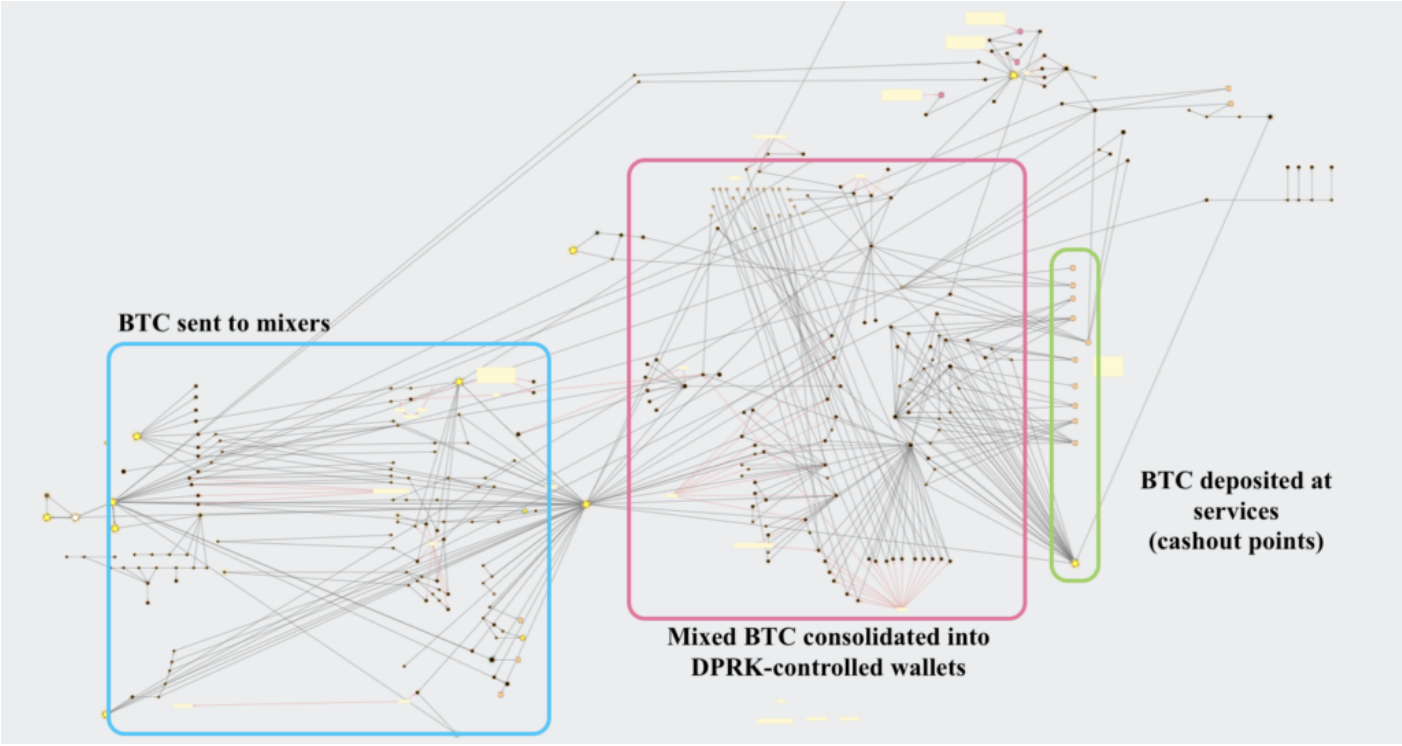


Next, the newly acquired Ether was mixed, and then swapped again.

Stage 2: Mixed Ether deposited at DEXs and CEXs to swap for Bitcoin



Stage 3: Movement of stolen funds after being swapped for BTC



At the end of this process, the attackers move the Bitcoin to centralized, primarily Asia-based exchanges, where it's likely swapped for a fiat currency like China's Renminbi, allowing them to finally access the cash gained from the hack.

DPRK: An advanced persistent threat to the cryptocurrency industry

These behaviors, put together, paint a portrait of a nation that supports cryptocurrency-enabled crime on a massive scale. Systematic and sophisticated, North Korea's government—be it through the Lazarus Group or its other criminal syndicates—has cemented itself as an advanced persistent threat to the cryptocurrency industry in 2021.

Nonetheless, the inherent transparency of many cryptocurrencies presents a way forward. With blockchain analysis tools, compliance teams, criminal investigators, and hack victims can follow the movement of stolen funds, jump on opportunities to freeze or seize assets, and hold bad actors accountable for their crimes.

This blog is a preview of our 2022 Crypto Crime Report. Sign up here to reserve your copy and we'll email you the full report when it comes out in February!