How North Korea's Lazarus Group laundered over $110 million in crypto using cross-chain bridges

How North Korea's Lazarus Group laundered over $110 million in crypto using cross-chain bridges

In 2023, hacker groups affiliated with the North Korean regime significantly increased their attacks on centralized platforms. Interestingly, back in 2022, according to a Chainalysis report, the focus was on decentralized finance.
Reviewing the recent incidents where Lazarus hackers attacked both the CoinEx cryptocurrency exchange and Stake.com casino (causing a total damage of slightly over $110 million), the BitOK team will spotlight the primary tools and techniques employed for cryptocurrency laundering. Moreover, we will investigate the reasons behind hackers' significant interest in cross-chain bridges.

On September 4, 2023, during the attack on the online casino Stake.com, hackers managed to steal cryptocurrency from the Ethereum, MATIC, and BNB Chain (formerly Binance Smart Chain) networks, amounting to over $41 million.
A portion of the funds stolen from the Ethereum network was initially directed to addresses believed to be associated with the Lazarus Group and included in the U.S. Office of Foreign Assets Control (OFAC) sanctions lists. Subsequently, the funds were transferred to two addresses:

1. 0xa4694f58A2445c5BF89405bc20E87fe6D8622356;
2. 0xc8A03DaaB82DB33Af11a48Bdb1E0e2B59C4c62Fb.

Afterward, the funds were **distributed across various addresses** and routed to THORChain, where **'chain-hopping'** occurred - exchanging from the Ethereum (ETH) network to Bitcoin (BTC).

Some of the funds were directed to the decentralized cryptocurrency exchange aggregator, 1inch Network. Using it, ETH was exchanged for the ERC-20 standard USDT stablecoin, which was then transferred to THORChain. Through the cross-chain bridge, USDT was converted into BTC. One of the Bitcoin addresses of the recipients, for example, is the address bc1q6z6y8e335wd3ys5zr0qvqpgztw359w0e9zlpgm (see figure 1).

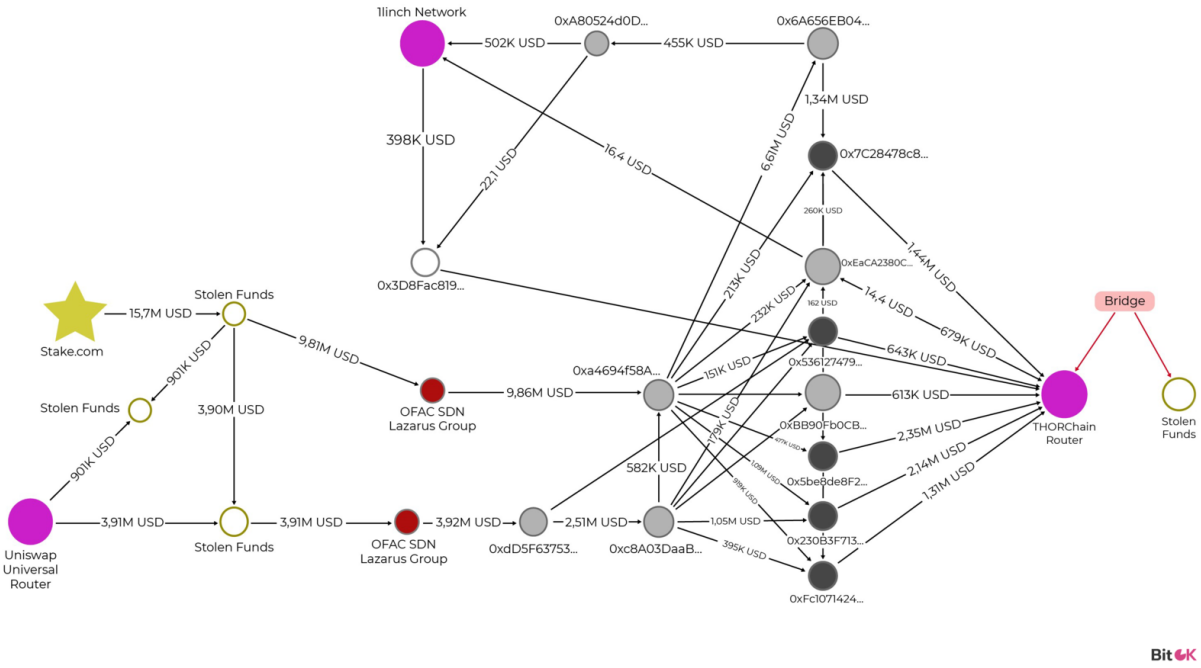


Fig. 1. Transaction list of addresses 0xa46...22356 and 0xc8A...c62Fb

Following this, the funds were sent to the de facto sanctioned mixer Sindbad.io (formerly Blender) (see figure 2).

Meanwhile, a portion of the stolen funds st s not associated with any services. For instance, at the address bc1qf u22s4zjek0e0umzj7z7k.

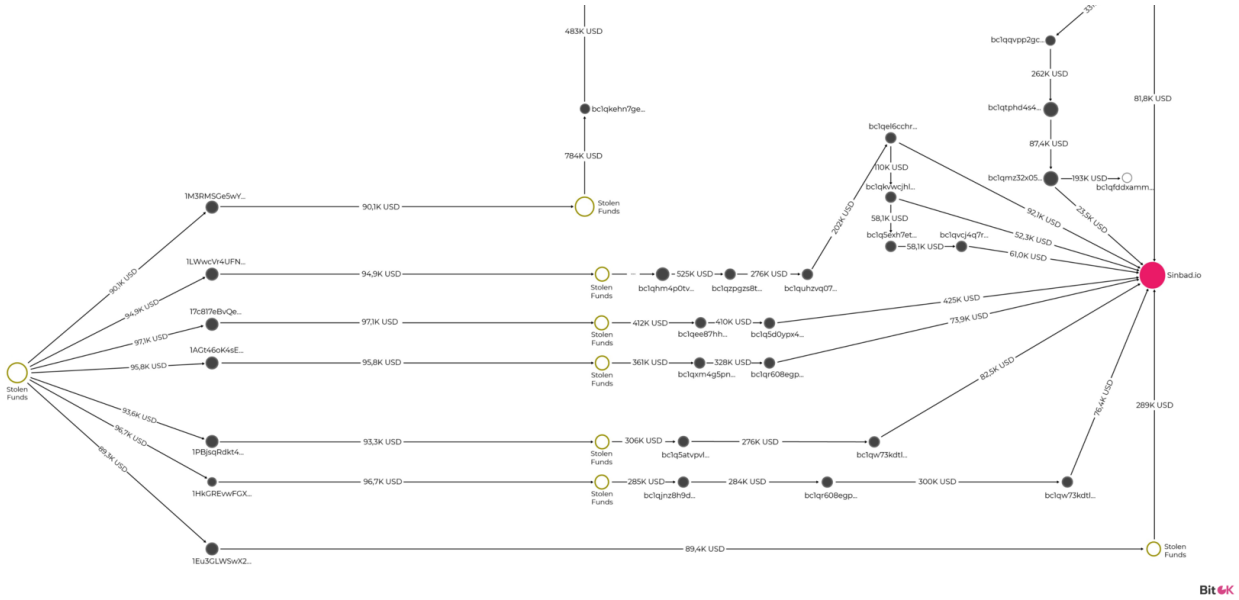


Fig. 2. Scheme for sending funds to Sindbad.io mixer

The stolen USDT_ETH were partially directed to the address 0x1154926C6AC4Be7A6C979D11ca2921D3e77BaaA1. From this address, funds were transferred to the decentralized exchange (DEX) Uniswap (an example transaction is 0x5f043071f40d87ac3d12c07faed80fb96d2048f36eeb19ac697884725fd35846), where the stablecoin was exchanged for ETH. Subsequently, the ETH funds were redirected back to the address 0x115...BaaA1 (see figure 3).

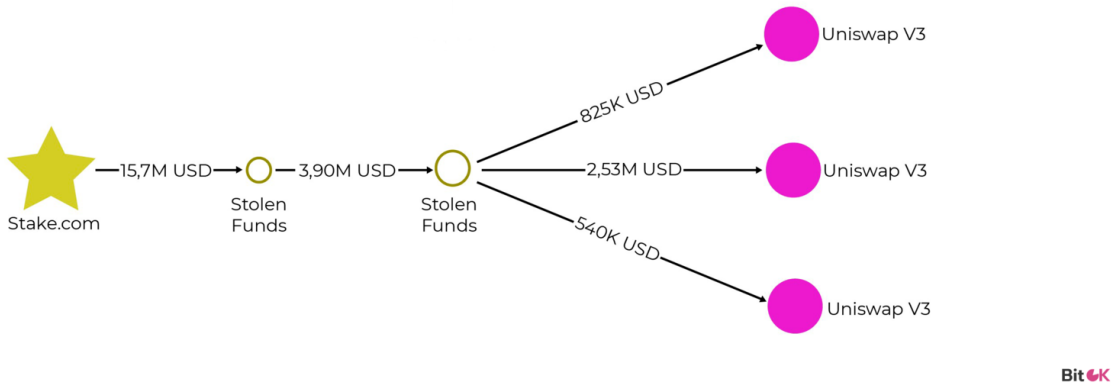


Fig. 3. Swap via Uniswap from address 0x115...BaaA1

Afterward, the funds were directed to the address 0xdD5F63753b578cc801d11572e80C62ee97BB3571. From there, they were once again transferred to the THORChain bridge, with a prior step of dispersing the funds among several intermediary addresses. Using THORChain, the attackers exchanged ETH for BTC through chain-hopping and sent it to addresses like bc1q4k9lreq9thdw9d33xh89nx8n5m9rpm6qr9ejea (see figure 4).

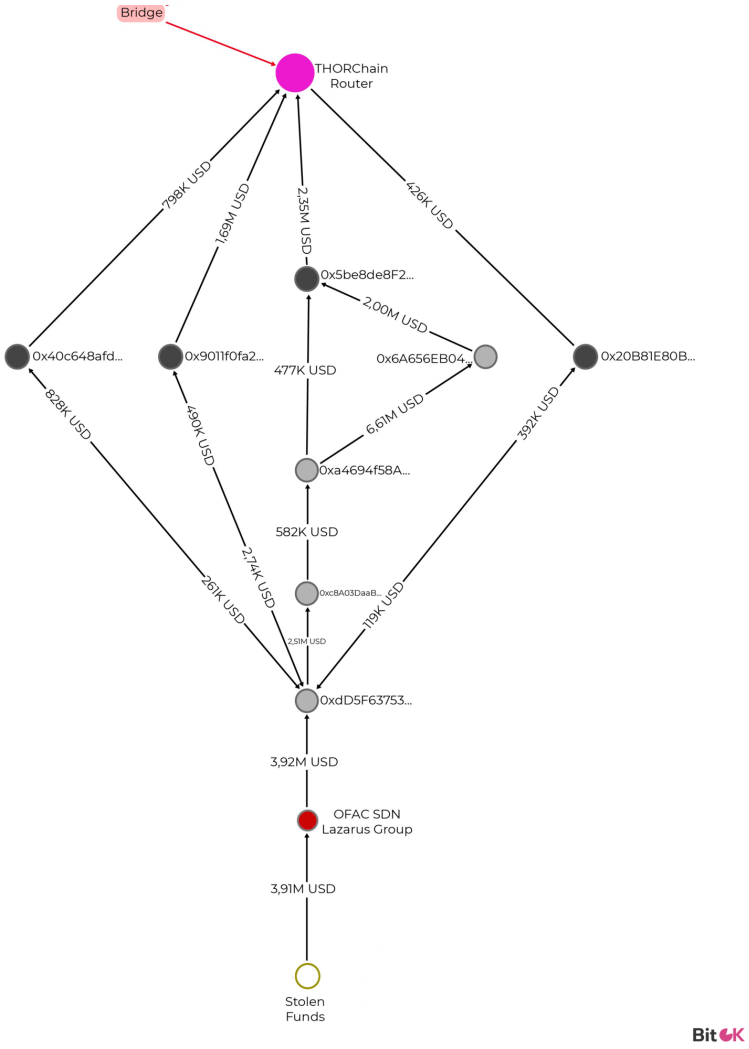


Fig. 4. List of transactions from address 0x115...BaaA1

Later on, the funds from this wallet were distributed in three ways:

1. Some funds went to the Sindbad.io **mixer** (see figure 5);
2. Some funds went to **centralized cryptocurrency exchanges** (HTX, Whitebit, etc.) (see figure 6);
3. The remaining assets are **dormant in wallets without movement** (bc1q9xn3va65wwvmynyxmu6a4cc32tyjw7a0fjm2wj, bc1qyzkpyvxlpyqjca6kjfpdn49rfpzm6t97p2sadn, bc1qrpyx42mmss76d7f5nnq33uv37epuwakgufg0gr, etc.) (see figure 5).

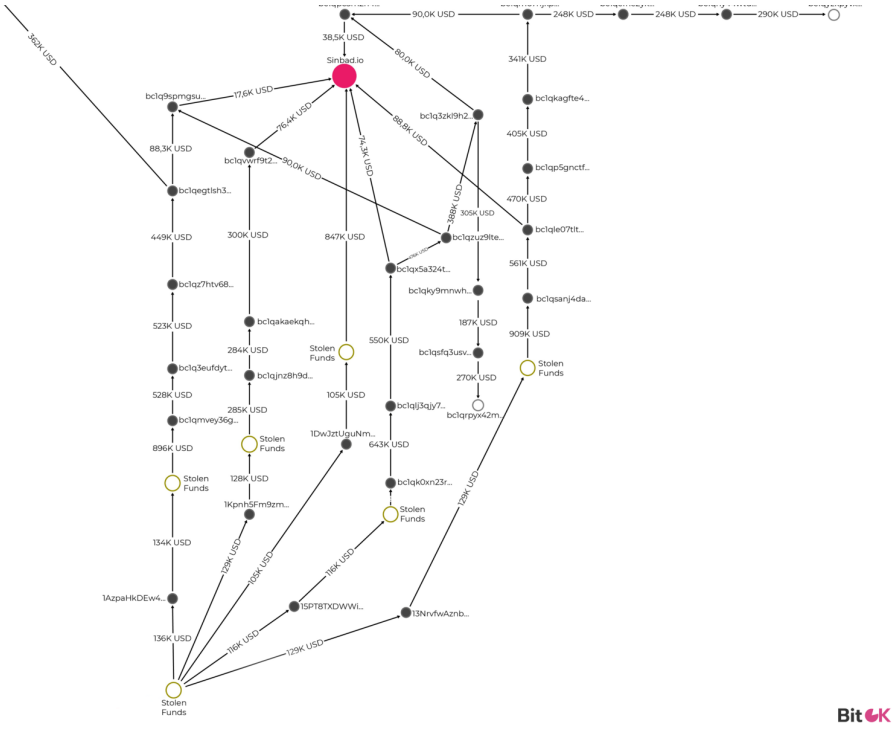


Fig. 5. Scheme for sending funds from address bc1q4...9ejea to Sindbad.io mixer

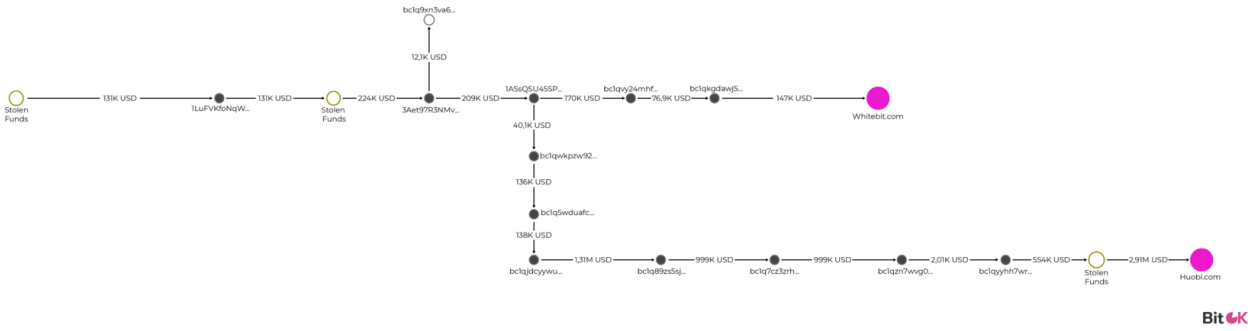
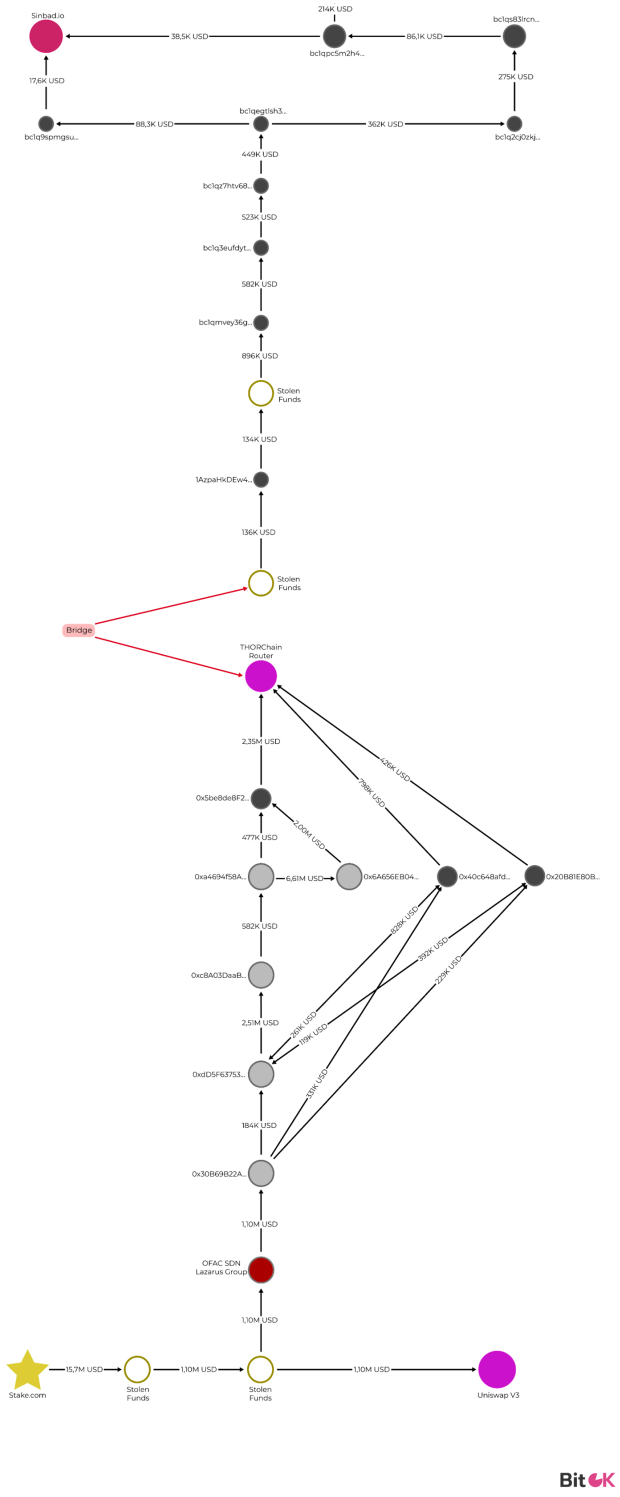


Fig. 6. Scheme for sending funds from address bc1q4...9ejea to centralized exchanges

An examination of the laundering schemes involving USDC and DAI indicates that hackers employed similar methods as described above. Their strategy included the use of:

- Decentralized platforms like Uniswap (see figures 7 and 8).
- Changing blockchain networks using THORChain (see figures 7 and 8).
- Withdrawing funds through the Sindbad.io mixer and various centralized exchanges (see figures 7).
- Leaving a portion of the funds in the hackers' cold wallets (see figures 7).



BitOK

Fig. 7. Scheme of converting funds to USDC and sending them to Sindbad.io mixer

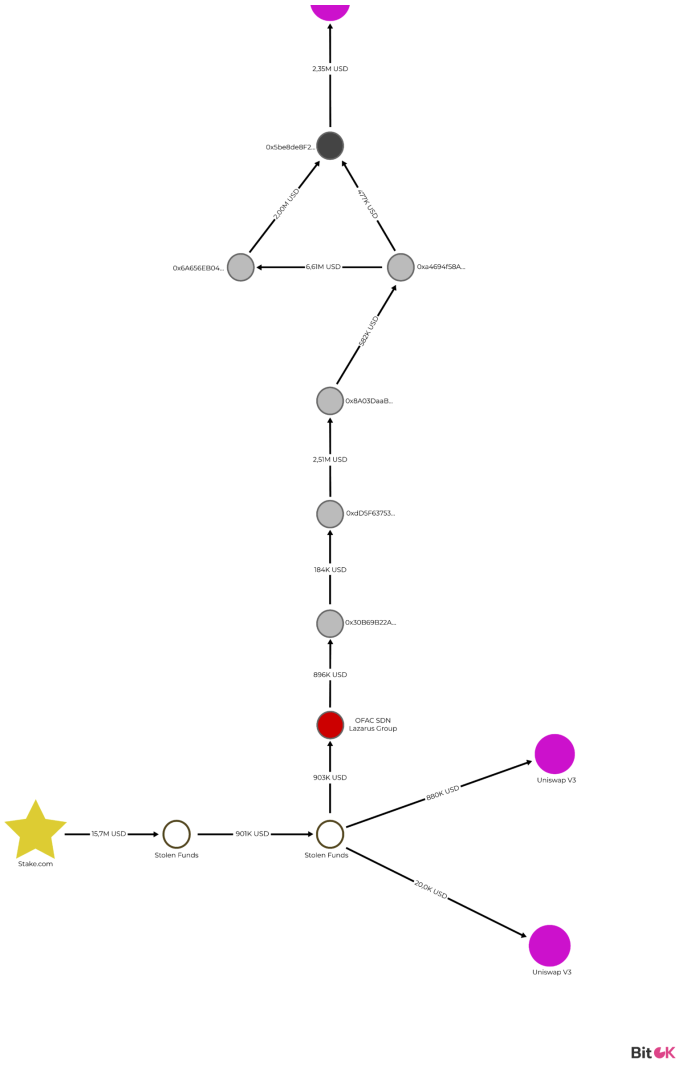


Fig. 8. Scheme for converting funds to DAI and changing the blockchain network

Attack on CoinEx

On September 12, 2023, during the CoinEx incident, the hackers used similar tactics as in the Stake.com casino case. They sent some TRON (TRX) funds directly to a TRON network version of Uniswap, namely SunSwap. There, they **swapped** TRX for USDT.

Another part of the funds went to SunSwap too, using addresses TB3ixJUBMQsfELigRodctY6kBhZ74G48UX and TMuMk21X6Gzm6ErNoAhGirWxX1aei4ixwo. From TB3ixJUBMQsfELigRodctY6kBhZ74G48UX the funds were dispersed to several intermediary addresses and then deposited on SunSwap, where they were exchanged for USDT.

After the swap:

such as Bitget, Gate.io, etc. (see figure 9).

2. Another portion of the USDT was exchanged for ETH using the cross-chain bridge Allbridge.io. After that, using the THORChain bridge, the perpetrators converted the funds from ETH to BTC and distributed them among numerous wallets, where they continue to remain as of the date of the investigation (bc1qy06xsq9yx93d02n95mv5y09z8fzy6usrj09ndy, bc1qzed4cka5972m3x5uh254msyn3f7sfqvcdkhv2k, bc1qnjsclu7xuarcewcxw85umq4ffrmaegvk0rfnat, bc1qa45rjs5sqz7m78m6jhu74myzcdswzp52f4n44z, etc.) (see figure 10).

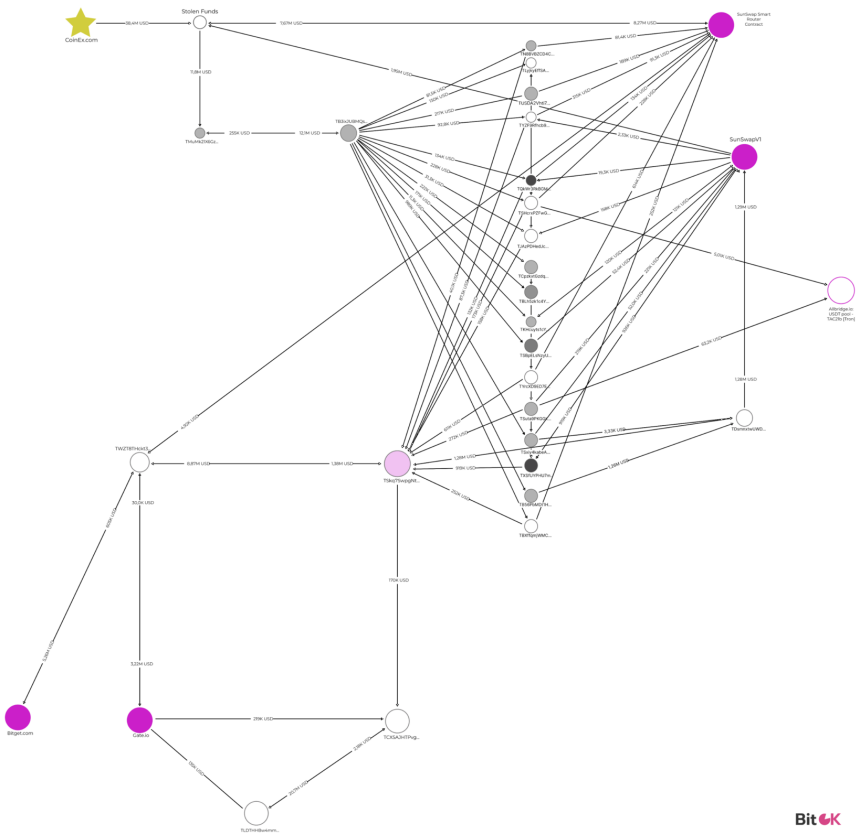


Fig. 9. Scheme of conversion funds to USDT and distribution of funds from address TB3ix...G48UX

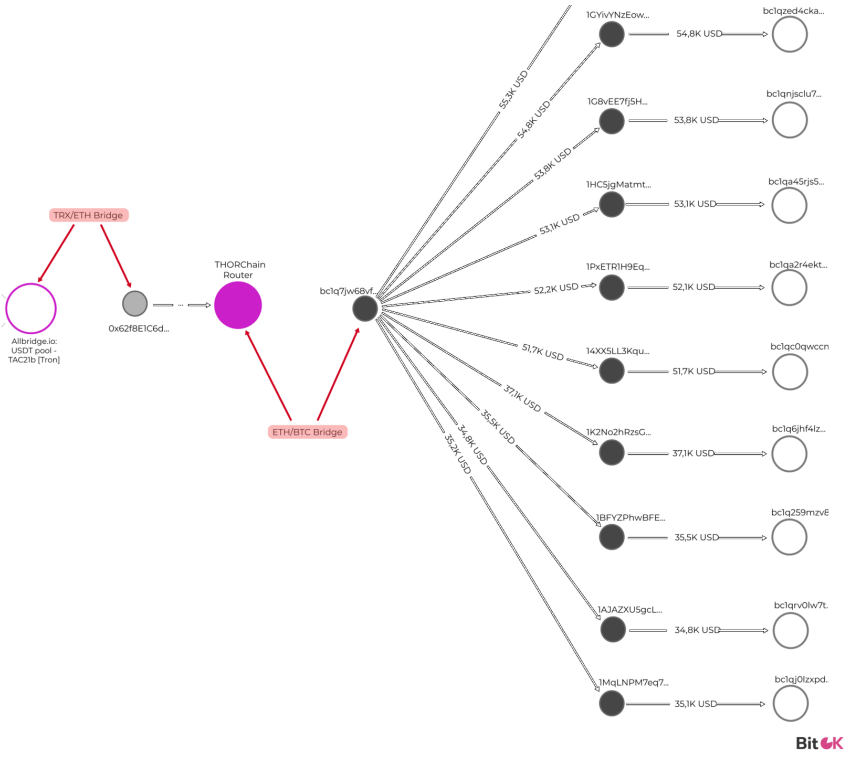
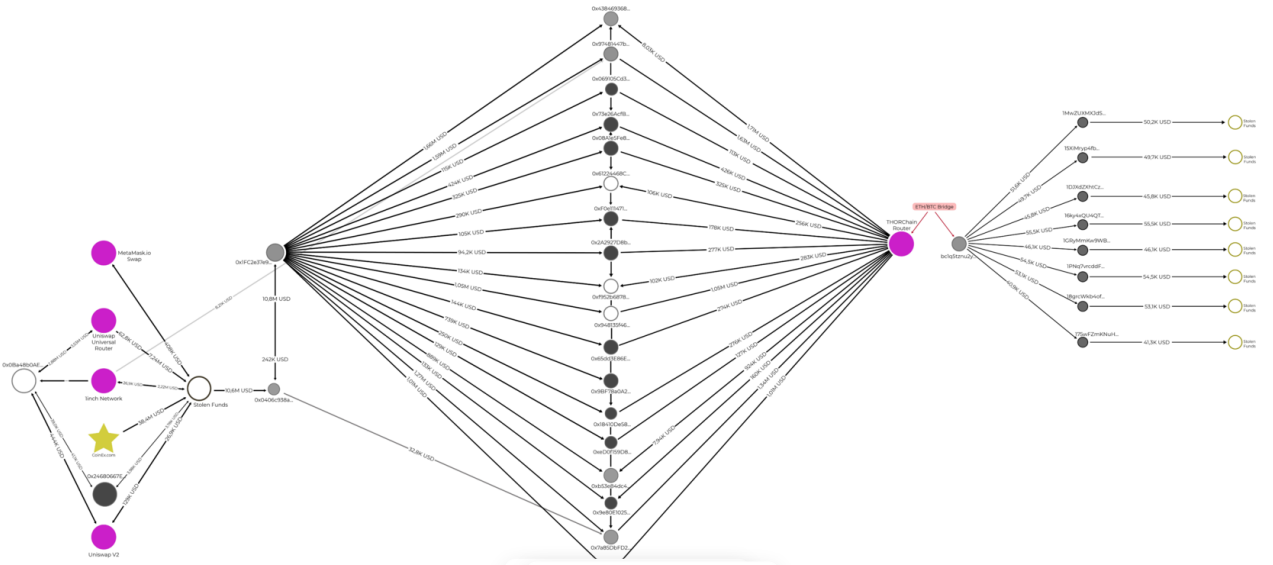


Fig. 10. Scheme of converting funds to ETH and further distribution

Speaking of ETH, a significant portion of the funds was sent to the address 0x0406c938a8A77F41C360b5304f6811078E42dA3b. After that, the assets were dispersed across various intermediary addresses.

Subsequently, they were sent to THORChain, where they were exchanged for BTC and once again spread across various addresses. (bc1qphh2mnrdwe7p5jxjxnzwsjsxhzyxzy0emzq0e5, bc1qrxv4mx56x0aus73f65asfgd99gp8hll3aeej9l, bc1qf5papnvu23hsm6mz5hvgcgwmd7te80yza4emay, etc.) (see figure.11). As of the investigation date, the funds still reside at these addresses.



As for the stolen Binance Coin (BNB), the funds were also converted to USDT, but this time using several platforms: PancakeSwap, 1inch Network, and Uniswap. After a series of conversions, the assets were sent to the Stargate Finance cross-chain bridge and exchanged for ETH.

Some of the assets were directly exchanged for ETH on decentralized exchanges and then withdrawn to THORChain, where they were again converted into BTC. After the BTC exchange, the funds were distributed across numerous addresses, where they remain as of the report writing (bc1q52y7ktl0h7x3sjy94zv8je753fweprh454tg6n, 3BhLKKb2ePaswCAsD8diyupYSMX5PeSvV5, bc1qu2rhaua3q7xqj8gfqgt92xher9qg5093mm689p, etc.) (see figure 12).

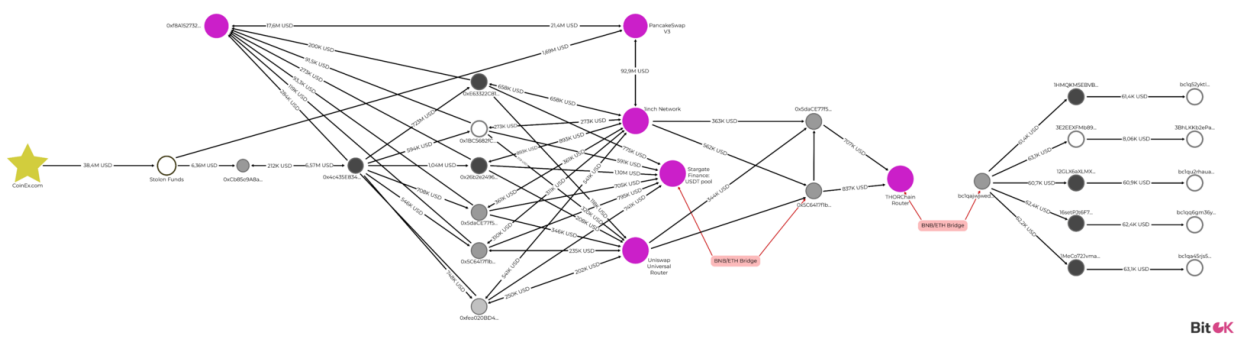


Fig. 12. Chain-hopping scheme from BNB to BTC

Conclusions

All the actions described above can be examined and countered through the use of blockchain investigation tools.

Public responses to cybercrimes, notably from the American regulator OFAC, are evident. Since 2018, OFAC has collaborated with analytical blockchain companies and law enforcement to pinpoint crypto addresses linked to suspected unlawful activities, adding them to sanction lists. As of November 2023, 601 addresses have been included in OFAC's lists.

However, these measures may not always be sufficient. OFAC adds addresses at a slow pace, and only a portion of identified addresses becomes public. Other regulators generally lack a practice of adding addresses to any blacklists.

Nonetheless, the overall well-being of the crypto market heavily relies on the actions of its participants: major crypto exchanges, platforms, bridges, mixers (not all of which are 'bad guys'), and so forth.

Most participants in the crypto industry already operate out of goodwill and primarily focus on protecting customer funds and future karma (regulation will soon be optimally tailored to the market). They are assisted by professional b vices and independent AML investigators.