A $60 million wallet theft. Beosin KYT Reveals the Hackers' Money Laundering Tactics

Beosin · Follow

6 min read · 1 day ago

Listen Share ••• More

Previously, a wallet theft involving tens of millions of dollars shocked the entire industry.

According to Beosin EagleEye, a security risk monitoring, alerting and blocking platform, Atomic Wallet was attacked in early June this year. The attack caused a loss of at least $60 million, based on information reported by known victims on the chain.

According to CoinDesk, Atomic Wallet CEO Konstantin Gladych said that the team is now collecting data from affected users and said that "the attack was definitely organized by a team of professional hackers who are using scripts, fund splitting, coin mixers and other measures".

In this article, we will dive into the details of how the money was laundered in this hacked theft and use Beosin KYT virtual asset AML compliance and analytics platform to track and analyze their schemes.

Incident Overview

According to Beosin team, so far the theft involved a total of 21 chains, including BTC, ETH and TRX. The stolen funds are mainly concentrated in the ethereum chain. Among them:

Ethereum chain

The stolen funds have been identified as 16,262 ETH worth of virtual currency, about $30 million.

Wavefield Chain

Wavefield chain is known to have stolen funds of 251335387.3208 TRX worth of virtual currency, about 17 million USD.

BTC Chain

BTC chain is known to have been stolen 420.882 BTC worth of virtual currency, equivalent to $12.6 million.

BSC Chain

The BSC chain is known to have lost 40.206266 BNB worth of virtual currency.

Other chains

XRP: 1676015 XRP, about $840,000

LTC: 2839.873689 LTC, about $220,000

DOGE: 800575.67369797 DOGE, about $50,000

Ethereum

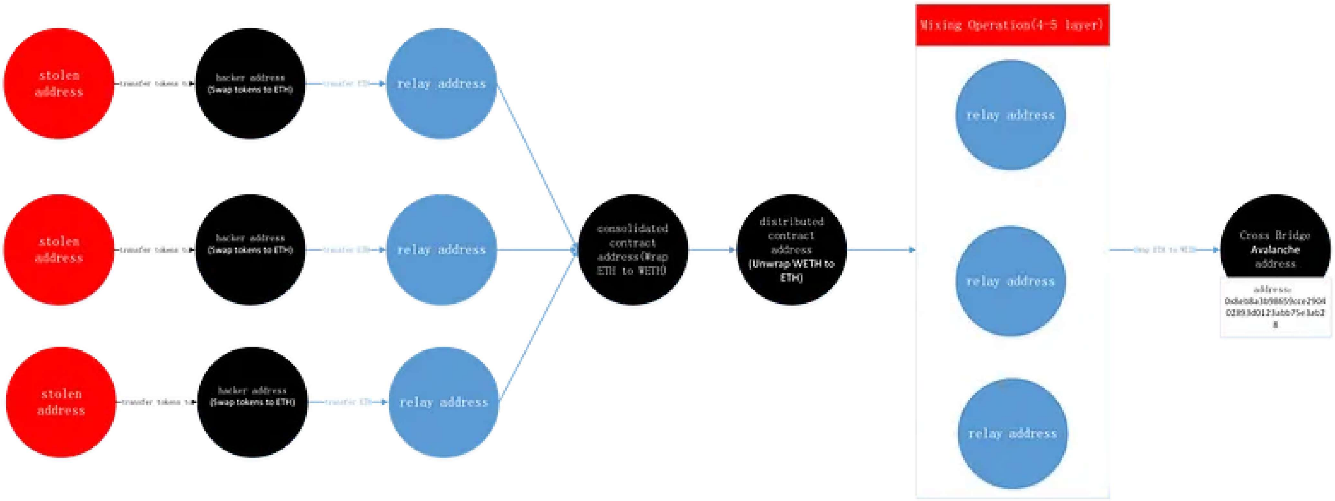
In the operation of hackers on the stolen money, there are two main ways in which ethereum is attacked on the chain:

1. Using Avalanche to launder money across the chain after dispersal through the contract

According to Beosin team, hackers would first exchange the valuable coins in the wallet for the main coins of the public chain, and then pool them through two contracts.

The contract address will pack ETH into WETH through two layers of transit, then transfer the WETH to the contract used to disperse the ETH, and transfer it into the wallet address used by Avalanche for Cross Bridge through up to 5 layers of transit for cross-chain operations. This cross-chain does not use contracts, instead it is an internal book-entry transaction of Avalanche.

A sketch of the Etherchain link is shown below:


stolen address
transfer tokens to
hacker address (Swap tokens to ETH)
transfer ETH
relay address
stolen address
transfer tokens to
hacker address (Swap tokens to ETH)
transfer ETH
relay address
stolen address
transfer tokens to
hacker address (Swap tokens to ETH)
transfer ETH
relay address
consolidated contract address(Wrap ETH to WETH)
distributed contract address (Unwrap WETH to ETH)
Mixing Operation(4-5 layer)
relay address
relay address
relay address
Swap ETH to WETH
Cross Bridge Avalanche address
address:
0xdef8a3b98659cce2904 02893d0123abb75e3ab2 8

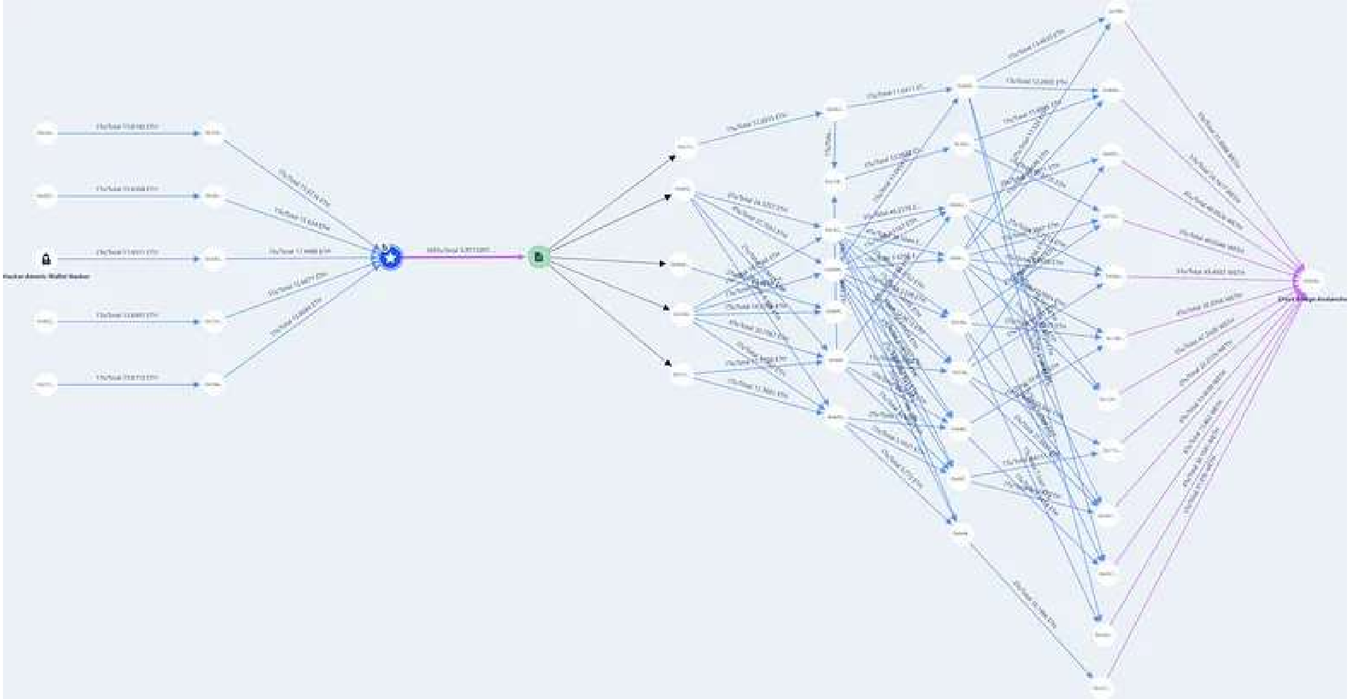
Collateralized Contract 1:

0xe07e2153542eb4b768b4d73081143c90d25f1d58

Total 3357.0201 ETH involved

Collateralized to WETH and transferred to contract 0x3c3ed2597b140f312412815239 52e936037cbed3

The detailed diagram of the sale route is shown below:



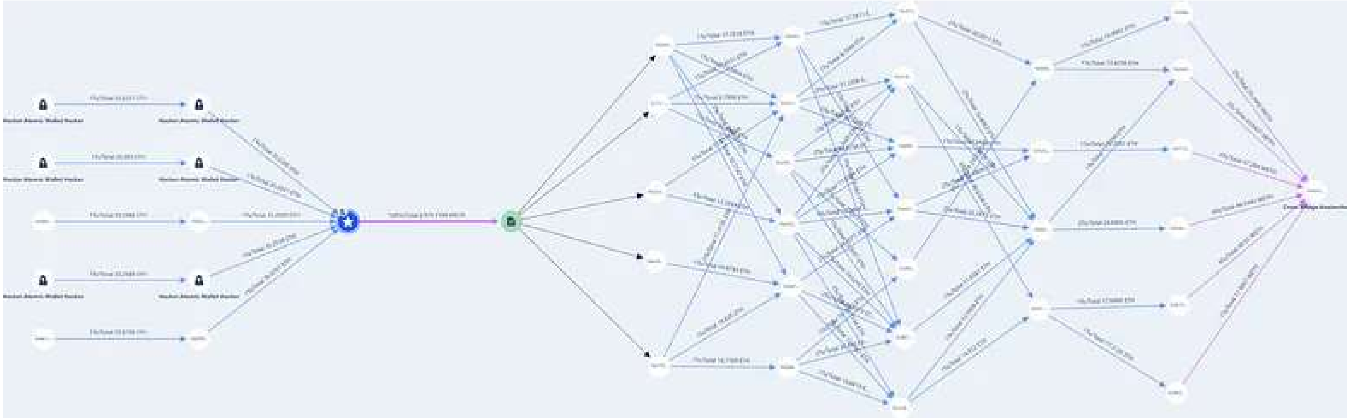
Collateralized contract 2:

0x7417b428f597648d1472945ff434c395cca73245

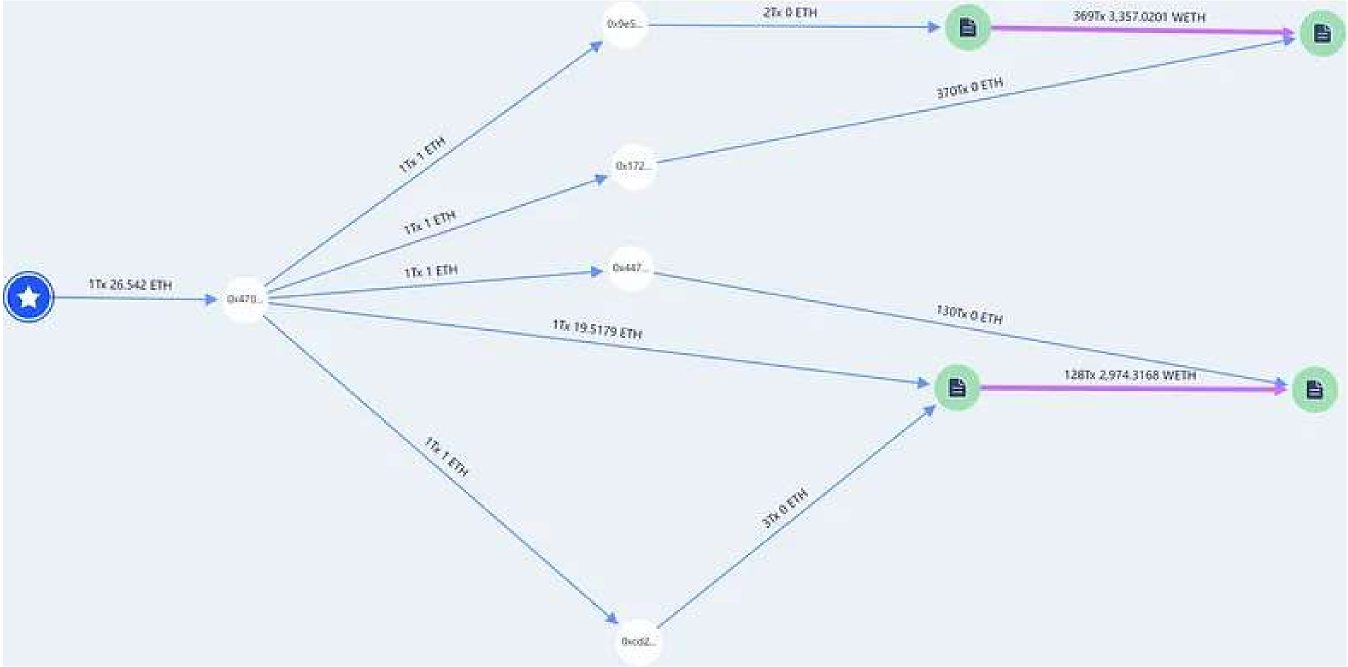
Total 3009.8874 ETH involved

Hackers exchanged to WETH and transferred to the contract 0x20deb1f8e842fb42e7af4c1e8e6ebfa9d6fde5a0

The detailed diagram of the pinning route is shown below:



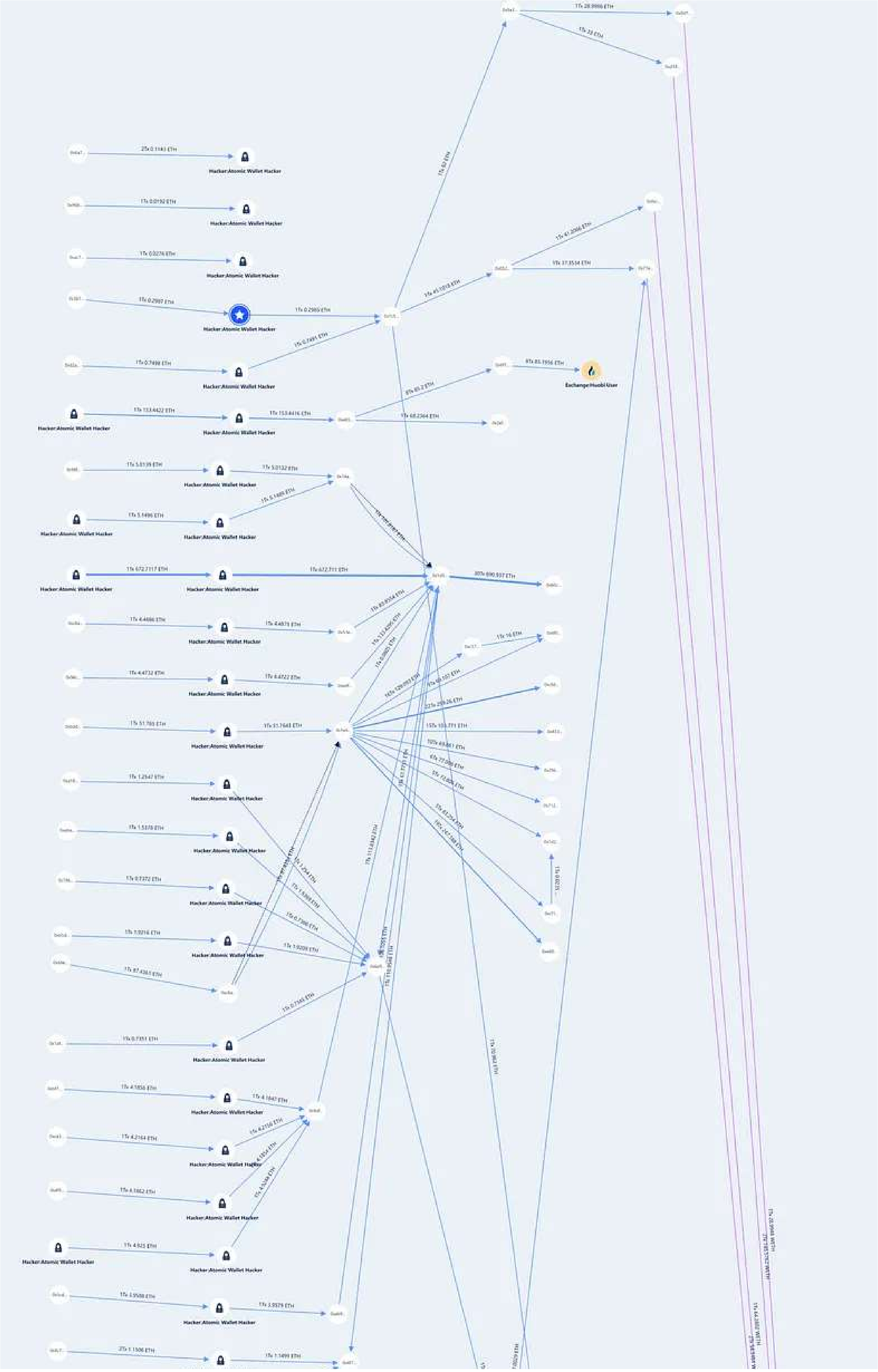
The two convergence contracts are confirmed by agreeing to the source of transaction fee, and part of the address without transaction behavior is hidden. The transaction fee route is as follows:

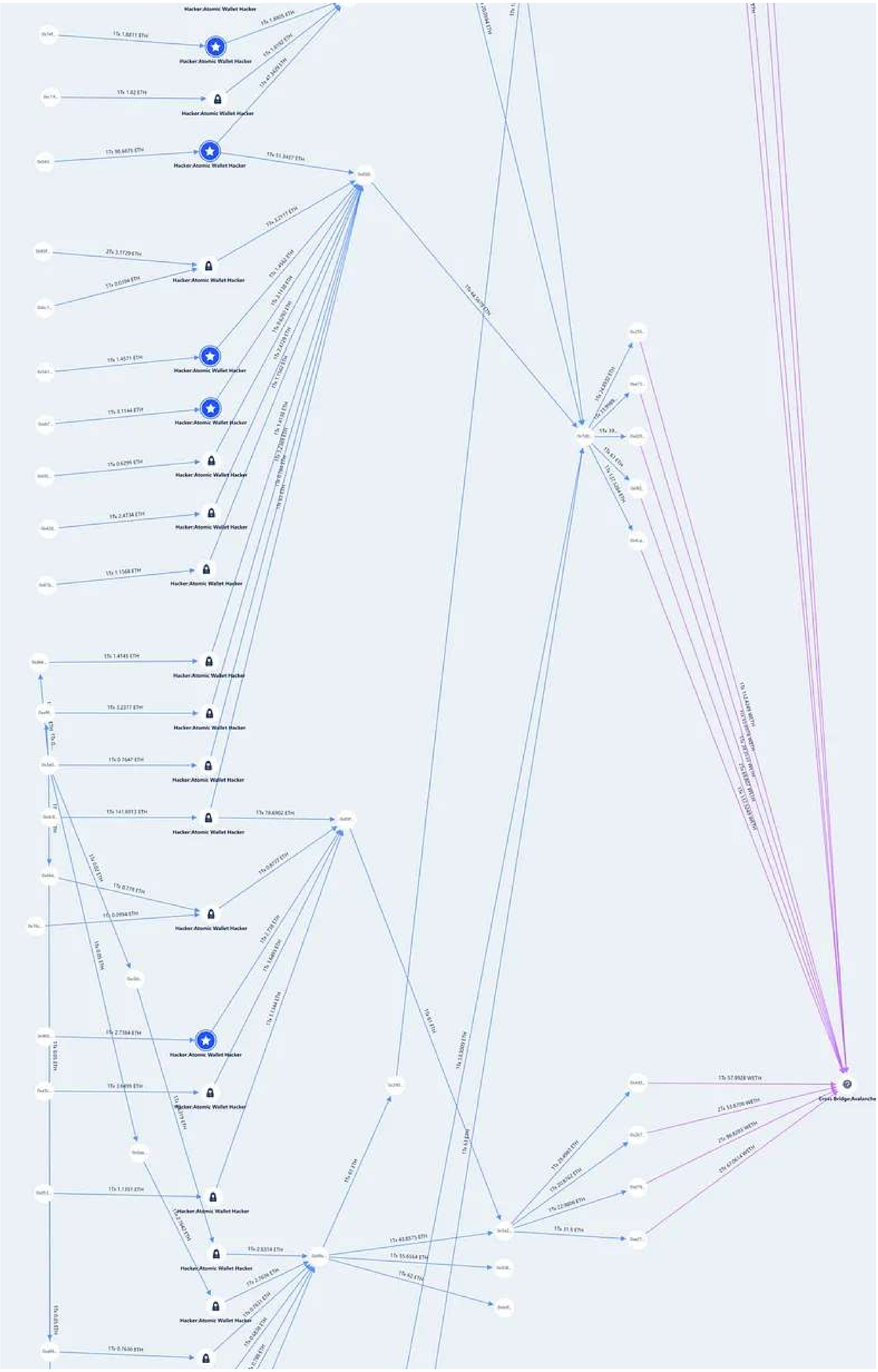


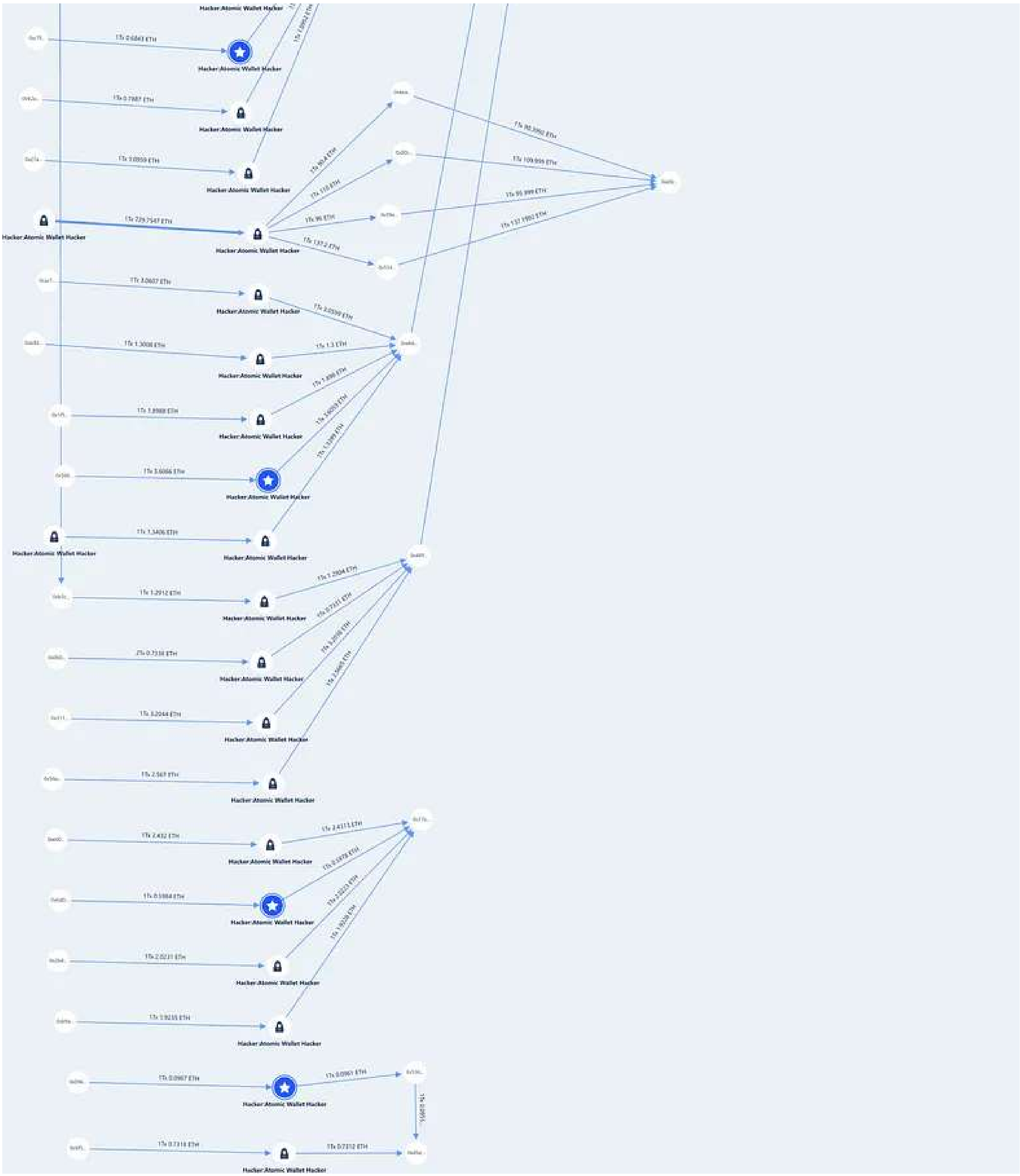
At present, only these four contracts with the act of converging stolen money are found.

2. Money laundering through various cross-chain bridge protocols and exchanges without direct dispersal through contracts.

This part involves 9896 ETH according to current statistics, and this part will be consolidated through multiple consolidation addresses. The money chain diagram is shown below:


Hacker:Atomic Wallet Hacker
Exchange:Huobi User
2Tx 0.1143 ETH
1Tx 0.0192 ETH
1Tx 0.0276 ETH
1Tx 0.2987 ETH
1Tx 0.2985 ETH
1Tx 0.7491 ETH
1Tx 0.7498 ETH
1Tx 153.6422 ETH
1Tx 153.6416 ETH
1Tx 82 ETH
1Tx 28.9986 ETH
1Tx 33 ETH
1Tx 41.1018 ETH
1Tx 41.2066 ETH
1Tx 37.3534 ETH
8Tx 85.2 ETH
8Tx 85.1936 ETH
1Tx 68.2364 ETH
1Tx 5.0139 ETH
1Tx 5.0132 ETH
1Tx 5.1496 ETH
1Tx 5.1489 ETH
1Tx 672.7117 ETH
1Tx 672.711 ETH
307x 890.937 ETH
1Tx 4.4886 ETH
1Tx 4.4879 ETH
1Tx 85.8554 ETH
1Tx 13.4095 ETH
1Tx 0.0885 ETH
1Tx 4.4732 ETH
1Tx 4.4722 ETH
1Tx 16 ETH
14Tx 128.093 ETH
9Tx 66.107 ETH
22Tx 259.26 ETH
1Tx 51.785 ETH
1Tx 51.7643 ETH
15Tx 103.771 ETH
10Tx 49.661 ETH
6Tx 77.098 ETH
5Tx 72.806 ETH
5Tx 65.254 ETH
16Tx 147.598 ETH
1Tx 0.0215
1Tx 1.2547 ETH
1Tx 1.254 ETH
1Tx 1.5378 ETH
1Tx 1.5368 ETH
1Tx 0.7372 ETH
1Tx 0.7366 ETH
1Tx 1.9216 ETH
1Tx 1.9209 ETH
1Tx 87.4361 ETH
1Tx 0.7345 ETH
1Tx 0.7351 ETH
1Tx 111.6342 ETH
1Tx 19.963 ETH
1Tx 4.1856 ETH
1Tx 4.1847 ETH
1Tx 4.2164 ETH
1Tx 4.2156 ETH
1Tx 4.1862 ETH
1Tx 4.1854 ETH
1Tx 4.923 ETH
1Tx 4.9246 ETH
1Tx 3.9588 ETH
1Tx 3.9579 ETH
2Tx 1.1506 ETH
1Tx 1.1499 ETH
1Tx 28.9986 WETH
2Tx 185.576 WETH
1Tx 44.3602 WETH


Hacker:Atomic Wallet Hacker
1Tx 1.8811 ETH
1Tx 1.8805 ETH
1Tx 1.8192 ETH
1Tx 1.82 ETH
1Tx 47.3405 ETH
1Tx 96.6675 ETH
1Tx 51.3407 ETH
2Tx 3.1729 ETH
1Tx 0.0394 ETH
1Tx 3.2917 ETH
1Tx 1.4571 ETH
1Tx 3.1144 ETH
1Tx 0.6299 ETH
1Tx 2.4734 ETH
1Tx 1.1568 ETH
1Tx 44.5619 ETH
1Tx 1.4145 ETH
1Tx 3.2377 ETH
1Tx 0.7647 ETH
1Tx 141.6013 ETH
1Tx 78.6902 ETH
1Tx 0.779 ETH
1Tx 0.0994 ETH
1Tx 2.7384 ETH
1Tx 2.6699 ETH
1Tx 1.1351 ETH
1Tx 2.6314 ETH
1Tx 0.7636 ETH
1Tx 61 ETH
1Tx 43.8375 ETH
1Tx 35.6554 ETH
1Tx 62 ETH
1Tx 25.4981 ETH
2Tx 20.8762 ETH
1Tx 22.9806 ETH
1Tx 31.5 ETH
1Tx 57.9928 WETH
2Tx 53.8736 WETH
2Tx 96.8283 WETH
2Tx 67.0614 WETH
1Tx 39...
1Tx 61 ETH
1Tx 112.4249 WETH
Cross Bridge:Avalanche



Map of ETH non-contract transfered funds as shown by Beosin KYT

Wavefield Chain

Wavefield chain is similar to the ethereum chain in that it transfers all the virtual currency from the stolen wallet to the public chain’s native token TRX through two layers of addresses and then continues to transit. The difference is that the convergence address is no longer carried out using a contract but a common address, which is dispersed and then transferred to various exchange deposit addresses. A part of the stolen funds remain on the chain without transfer, and there are many consolidated addresses.

We can see that there are many channels for hackers to launder money, mainly through various exchange accounts, but also directly into the cross-chain bridge contract.

The consolidation addresses are mainly the following two addresses

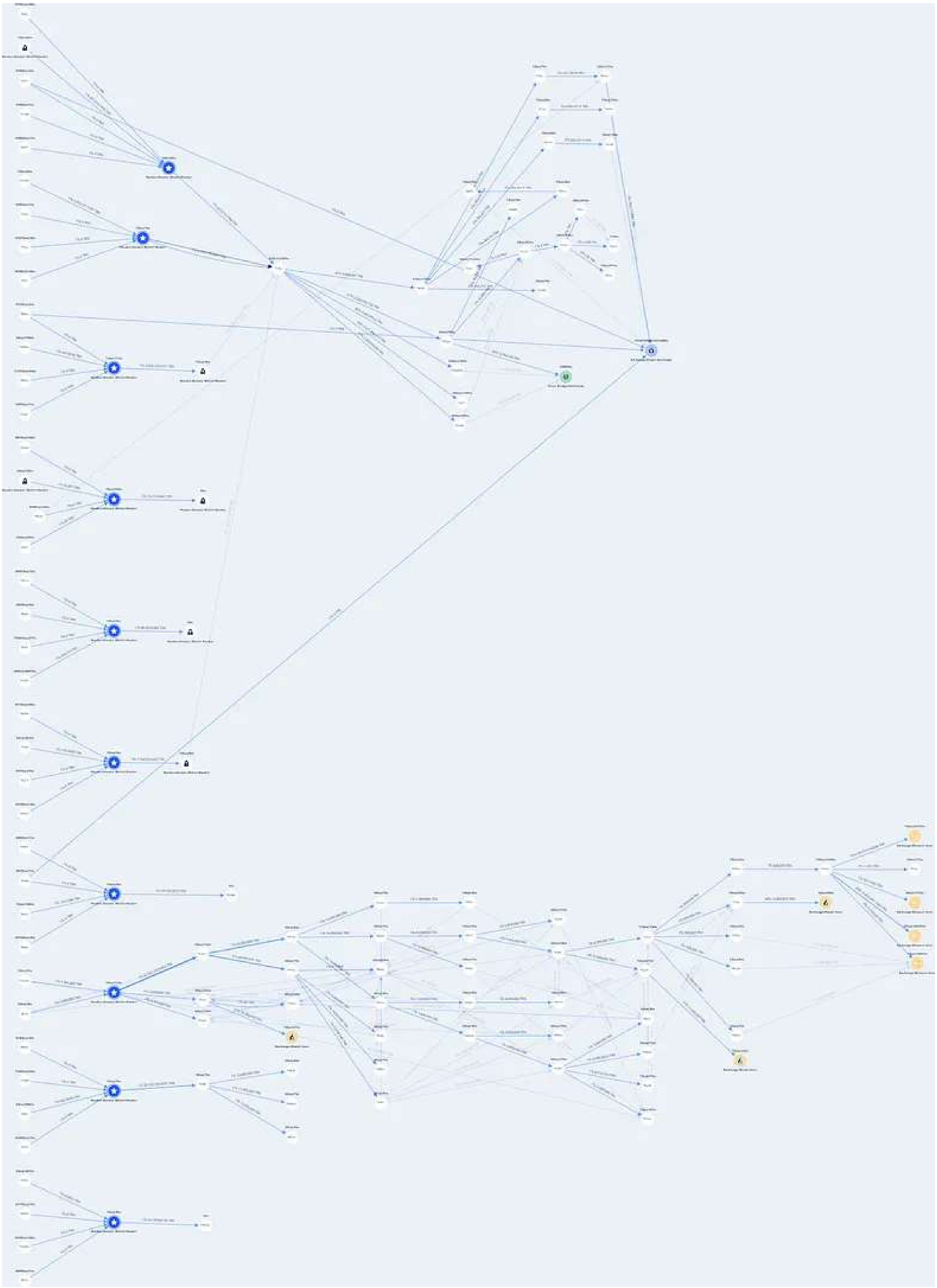
TCSEiuNnYHJ3E1LPxAFdDd1xERWUPeUeEC

Flow involved: 157,401,175.7231 TRX

TL4w1Xo6PBfa41StEgpNAZWtS65HRPgrHS

Flow involved: 93,934,211.5977 TRX

The route pattern is shown in the chart below:



Beosin KYT shows an example of the flow of funds in the wavefield chain

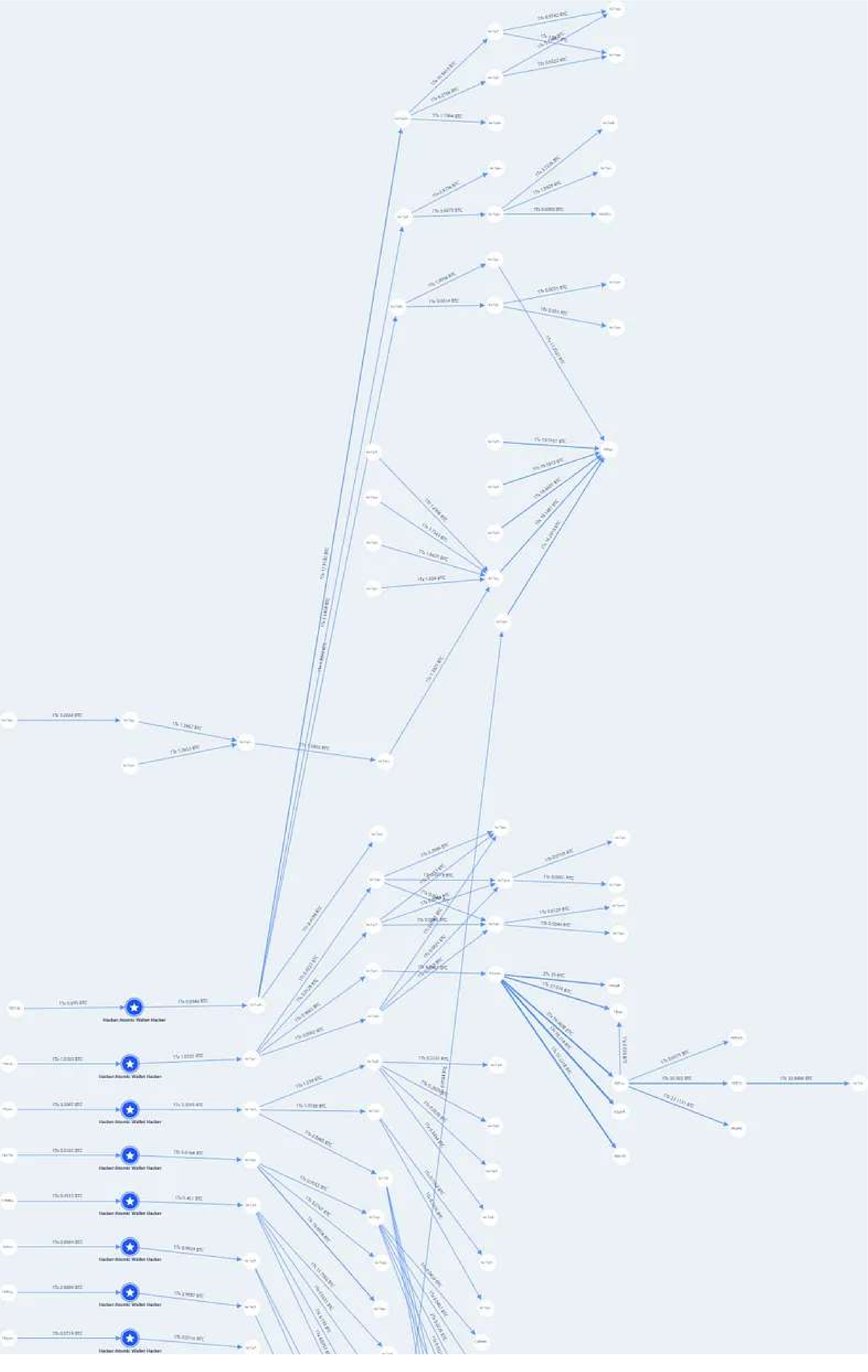
BTC Chain

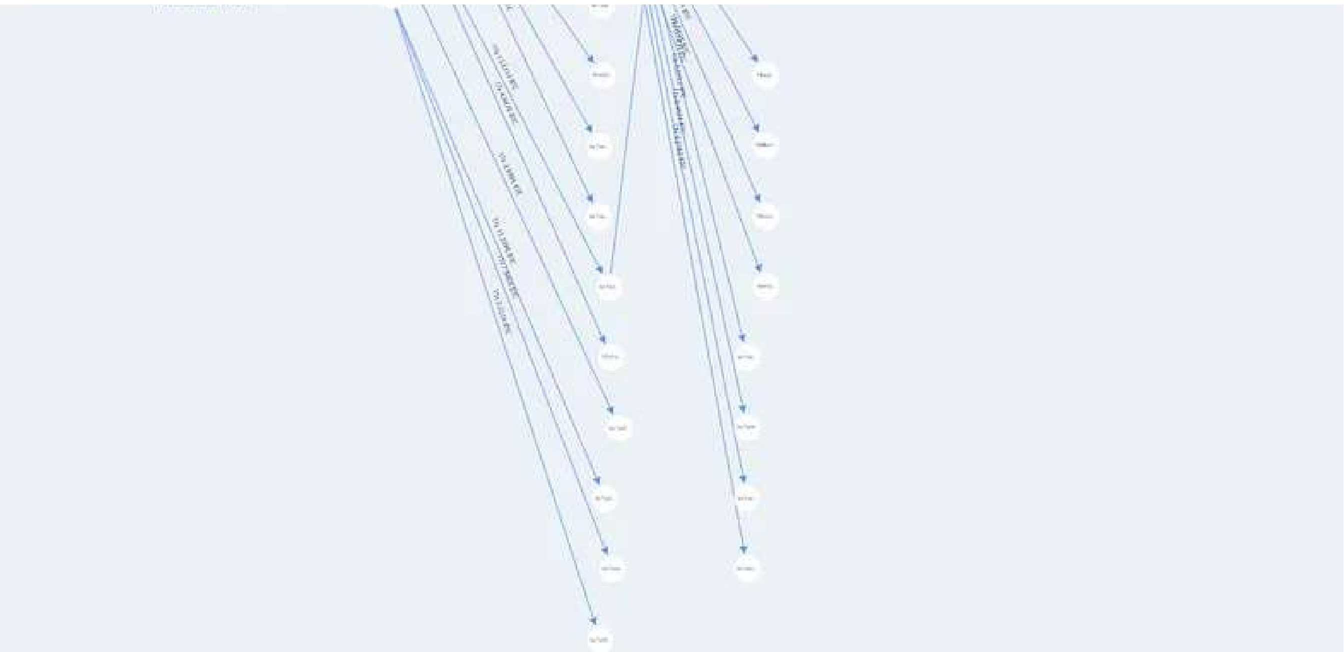
BTC already known consolidation address involved in the case is 420.882 BTC.

BTC chain involved addresses are divided into multiple consolidation addresses, and there is no subsequent crossover of funds from the consolidation addresses and a large number of consolidated addresses.

Similar to other chains, the stolen funds will be directly transferred to the hacker’s address, and then transferred to the consolidation address by the hacker’s control through a layer of transit and dispersed afterwards. The number of dispersion layers is at least 4, after which it will be deposited or mixed into a larger stream of suspected money laundering addresses.

The route pattern is shown in the following diagram:

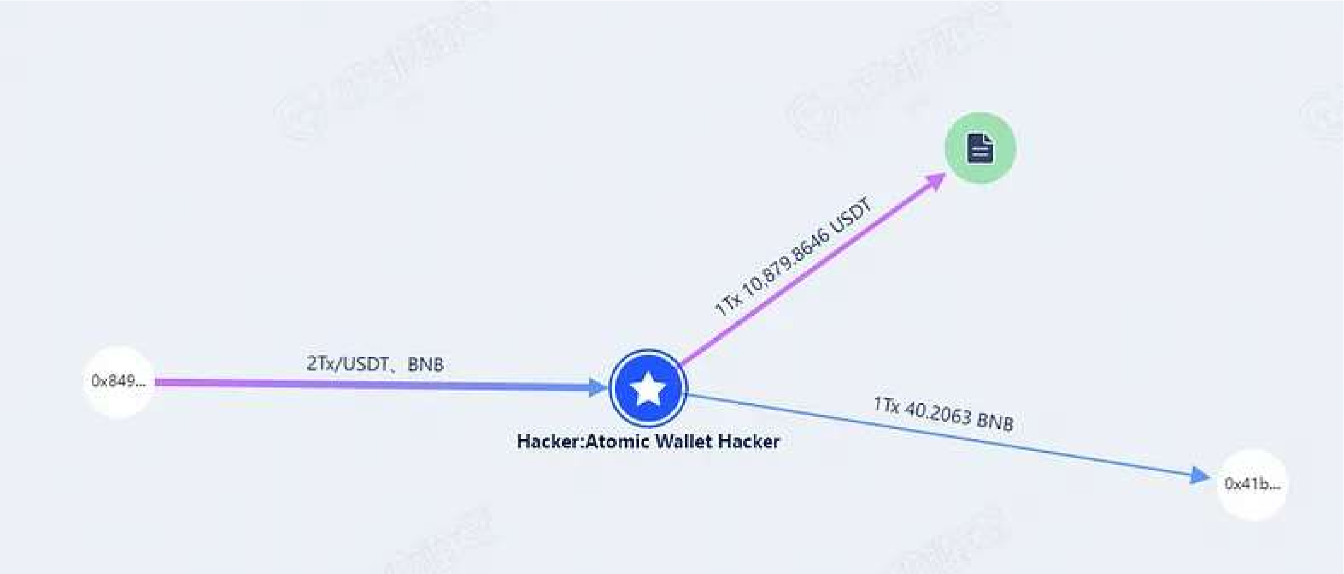

Hacker Atomic Wallet Hacker
Hacker Atomic Wallet Hacker
Hacker Atomic Wallet Hacker
Hacker Atomic Wallet Hacker
Hacker Atomic Wallet Hacker
Hacker Atomic Wallet Hacker
Hacker Atomic Wallet Hacker
Hacker Atomic Wallet Hacker



Example diagram of BTC money flow shown by Beosin KYT

BSC Chain

The BSC chain has only one address, and funds are currently locked on the chain.



Another 35 BNB from stolen wallets.

The other chain addresses

XRP: 1676015 XRP, equivalent to $838,007

LTC: 2839.873689 LTC, equivalent to $217,789

DOGE: 800575.67369797 DOGE, equivalent to $51,194

The above chain model is similar to other chains, all of them are stealing coins from wallets after exchanging them for native tokens and then entering different consolidation addresses through a layer of transit, and there are more addresses still locked on the chain.

Regarding progress related to this incident, it is reported in mid-June that Estonian police said they are investigating the theft of cryptocurrency from Atomic Wallet users in the country. Estonian authorities said they have been investigating the theft since last week, that the investigation is still in its early stages and that they will not comment on the source of the attack at this time.

As can be seen from the above incident, cybercrime, money laundering, dark web trading and other crimes involving virtual assets have become common in recent years, and the decentralization, openness and anonymity of blockchain have posed a huge challenge to regulators.

To solve the above problem, a group of security institutions represented by Beosin has proposed a solution idea — KYT (Know Your Transactions), which aims to let trading platforms and regulators understand each transaction on the chain. In traditional financial transactions, financial service institutions design anti-money laundering systems through KYC and transaction data. In virtual asset transactions, trading platforms can use KYC and KYT technologies to bind the entity behind each transaction, analyze its transaction behavior, identify its criminal logic, use on-chain analysis and tracking tools to locate each transaction, profile the user, and rate the transaction, thus reducing the risk of criminals using virtual assets to launder money.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, South Korea, Japan and other 10+ countries. With the mission of “Securing Blockchain Ecosystem”, Beosin provides “All-in-one” blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance. You are welcome to contact us.