



# Crypto Asset Tracing Handbook



# Table of Contents

Introduction	3
On-chain Tracing	5
1. Basic Concepts	5
(1) Mainstream Blockchains and Cryptocurrencies	5
(2) Core Concepts in Tracing	8
(3) Blockchain Explorers	17
2. Tracing Tools	21
(1) Introduction to MistTrack	22
(2) MistTrack in Use	24
(3) Community Tools	33
3. Common Fund Movement Patterns	34
(1) Peel Chain	34
(2) One-to-Many Distribution	35
(3) Multi-Hop Transfers	36
(4) Mixer Usage	37
(5) Cross-Chain Bridge Hops	38
(6) Many-to-One Consolidation	39
(7) P2P / OTC	40
4. What to Do If You Get Hacked	41
(1) Prioritize Loss Prevention	42
(2) Preserve the Scene	43
(3) Conduct Preliminary Analysis	43
(4) Contact Professional Agencies	44
(5) File a Police Report and Seek Legal Assistance Early	44
(6) Ongoing Follow-up and Profiling	45
(7) Tokens Eligible for Freezing	45

5. Cross-chain Bridge Tracking Analysis	46
(1) Introduction to Bridges	46
(2) Bridge Analysis	48
Method 1: Bridge Explorer	48
Method 2: Blockchain Explorer Analysis	50
Method 3: MistTrack Cross-chain Parsing	53
6. Privacy Tool Tracking Analysis	55
(1) Introduction to Mixers	55
(2) Mixer Analysis	57
Case 1: Tornado Cash Analysis	58
Case 2: Wasabi Coinjoin Analysis	62
7. NFT Tracking Analysis	66
8. Address Behavior Analysis	73
(1) Active Behavior Feature Identification	73
(2) Address Clustering Analysis	74
(3) Risk Behavior Profiling	75
(4) Address Labels and Off-Chain Identity	75
(5) AI Tools and Analysis	76
9. Case Studies	79
10. Recommendations for Asset Freezing and Recovery	90
Conclusion	92
Disclaimer	93
About SlowMist	94

# Introduction

In recent years, the crypto industry has made significant technological advancements; however, crimes involving crypto assets have simultaneously intensified in both frequency and complexity. These crimes range from pervasive fraudulent schemes such as Ponzi scams, phishing websites, and fake projects, to sophisticated technical attacks including vulnerabilities exploited in DeFi protocols, unauthorized intrusions into exchanges, and asset theft resulting from leaked private keys.

In just 2024 and the first half of 2025, according to statistics from the [SlowMist Hacked archive](#), the blockchain ecosystem witnessed 531 security incidents, with total losses reaching \$4.386 billion. The Web3 anti-fraud platform [Scam Sniffer](#) also pointed out that Wallet Drainer phishing attacks alone have caused approximately \$534 million in losses, affecting over 375,600 wallet addresses. This figure continues to rise, and the actual number of victims is likely far greater than the data suggests.

Anonymity is a double-edged sword in the world of cryptocurrency. While it grants users the right to privacy, it also makes certain malicious activities far more difficult to pinpoint with precision. Coupled with blockchain's inherent global nature, the processes of cross-border investigations, judicial cooperation, and asset freezing are often slow and cumbersome. As a result, even when the on-chain path of funds is crystal clear, achieving meaningful legal or enforcement outcomes in the real world can be challenging. This paradox—where the trail is visible yet remains out of reach in practice—has become one of the greatest frustrations for victims of crypto asset crimes.

Many people initially assume: "Since crypto assets are on-chain and all transactions are publicly visible, recovering stolen funds should be easy, right?" The reality is far more complicated. On-chain visibility is merely the first step; actual fund recovery requires overcoming a series of complex technical and legal challenges. Attackers can employ various laundering tactics—cycling funds through dozens of wallets, withdrawing via unregulated or anonymity-enhanced exchanges, obfuscating assets through mixers, and leveraging proxy contracts. On the other hand, ordinary users often lack even the most basic on-chain knowledge and are left powerless when facing

such threats. This means that, even if the movement of stolen funds is fully traceable, freezing or retrieving those assets may still prove impossible.

For this reason, basic knowledge of on-chain tracing should not remain an exclusive “professional skill” for security researchers or ethical hackers. Instead, it should be a fundamental competency for everyone participating in the crypto ecosystem. Whether you are a retail investor, a contributor to crypto projects, a media analyst, a legal professional, or engaged in law enforcement or regulatory work, understanding how funds flow on-chain, mastering basic tracing tools and techniques, and recognizing abnormal transaction patterns can serve as your first line of defense against risk. In critical moments, promptly identifying a suspicious fund path could secure a precious few hours to freeze assets, and the correct use of basic tools might help victims reconstruct a complete chain of events.

This book, *The Crypto Asset Tracing Handbook*, was written with that purpose in mind. It is not a specialized research report, nor does it aim for overly technical discussions. Rather, it seeks to provide clear and practical guidance to help a broader audience understand the basic framework of on-chain tracing, learn how to use key tools, and strengthen their ability to assess and respond to on-chain risks. Whether you are a researcher, investor, journalist, legal practitioner, law enforcement officer, or an ordinary victim, you will find parts of this handbook relevant to you.

We recognize that no handbook can solve every on-chain security problem. But if it can help you pause for a few critical seconds when spotting an abnormal transaction, immediately preserve vital evidence when facing a potential rug pull, or describe suspicious asset flows more precisely in media or community discussions, then it will have achieved its purpose.

In the chapters ahead, we will start from the most fundamental concepts and gradually explore the subtle traces left behind on-chain.

# On-chain Tracing

## 1. Basic Concepts

Blockchain is not mysterious, but it does have its own language and structure that differ from the traditional financial system. Therefore, before starting any on-chain tracing, we need to first understand the most fundamental concepts in blockchain systems. In many cases, the key to determining a fund's path or identifying suspicious activity lies behind these seemingly simple terms.

### (1) Mainstream Blockchains and Cryptocurrencies

- Bitcoin (BTC)

Proposed by Satoshi Nakamoto (a pseudonym) in 2008, Bitcoin's genesis block was mined in 2009. Bitcoin uses the UTXO (Unspent Transaction Output) model, where each transaction functions like a "change" process, making on-chain paths relatively clear and transparent. The Bitcoin network does not support complex smart contracts, so on-chain activities are limited. While the tracing process is comparatively straightforward, it still requires specific analytical strategies.

- Ethereum (ETH)

Proposed by Vitalik Buterin in 2013, Ethereum's crowdfunding took place in 2014, and its mainnet launched in 2015 with the first block mined. Ethereum is currently the most widely used smart contract platform, hosting the largest DEX and DeFi ecosystems, and is the most common network targeted in attacks. ETH is Ethereum's native token, used to pay transaction fees (Gas) and participate in governance. Unlike Bitcoin, Ethereum is a Turing-complete smart contract platform, allowing the creation and deployment of decentralized applications (dApps) that power ecosystems such as DeFi (Decentralized Finance), NFTs (Non-Fungible Tokens), and DAOs. Ethereum uses the account model, where each address records its balance. Tracing requires analyzing complex contract interactions and token swaps. In 2022, Ethereum completed "The Merge," transitioning from PoW to PoS, greatly reducing energy consumption.

- TRON (TRX)

Launched by Justin Sun in 2017 with its mainnet going live in 2018, TRON's native token is TRX. TRON is compatible with Ethereum's account model and heavily optimized for transfers, offering near-zero fees and fast confirmation speeds. The most widely circulated asset on TRON is USDT (TRC20), which makes the network a frequent choice for scam groups to aggregate, split, and launder funds. As a result, TRON transactions warrant close attention in tracing.

- BNB Chain (BNB)

Launched by Binance in 2020 (formerly Binance Smart Chain, BSC), BNB Chain is a high-performance, EVM-compatible blockchain. Its native token is BNB. BNB Chain offers fast transactions, low fees, a mature ecosystem, active DEXs, and a large number of contracts. While highly compatible with Ethereum, it lacks strict auditing, leading to rampant phishing tokens and becoming a hotspot for Ponzi and copycat projects.

- Polygon (MATIC)

Polygon, formerly Matic Network, is one of Ethereum's scaling solutions. It offers sidechains and Layer 2 technologies such as ZK Rollup and Optimistic Rollup, delivering low-cost and high-performance transactions. Polygon is fully compatible with Ethereum smart contracts, so tracing methods are largely similar. However, its low fees make it attractive as an intermediary layer for laundering.

- Solana (SOL)

Launched in 2020, Solana is known for high throughput and low latency, using a hybrid consensus of PoH (Proof of History) and PoS (Proof of Stake). Solana is not EVM-compatible and uses a unique account model and the Rust programming language. Its explorers and toolchains are separate from Ethereum's ecosystem. In recent years, it has become a frequent target for hacks, including large-scale losses from wallet private key leaks.

- Avalanche (AVAX)

Launched in 2020, Avalanche is a blockchain platform supporting multiple subnets. It provides highly customizable blockchain environments, allowing projects to deploy independent subchains. Avalanche's primary C-Chain is EVM-compatible and serves as the main hub for

contract interactions and token trades. While its subnet mechanism is flexible, it can complicate tracing by dispersing data and introducing cross-chain complexity.

- Optimism (OP)

Optimism is an Ethereum Layer 2 network based on Optimistic Rollup technology, compatible with all Ethereum contracts and offering significantly lower costs and faster confirmations.

Developers can seamlessly deploy existing Solidity projects. In tracing, a key challenge is that transactions often originate from Ethereum mainnet bridges, requiring cross-chain analysis.

Common laundering patterns include: bridging funds in from the mainnet → swapping on a DEX → bridging funds out again.

- Arbitrum (ARB)

Arbitrum is another Ethereum Layer 2 network using Optimistic Rollup and currently has the highest user base and total value locked (TVL) among Layer 2s. Key characteristics include: the same address format as Ethereum but a different chain ID (requiring clear differentiation); on-chain mixers (e.g., Tornado Cash) still require interaction with Ethereum mainnet, allowing correlation through mainnet activity; and frequent cross-chain activity, with attackers often moving funds through Arbitrum after exploits to increase transfer efficiency or evade mainnet monitoring.

- USDT

USDT is a stablecoin issued by Tether, pegged to the U.S. dollar at 1 USDT = 1 USD, and issued on multiple blockchains. Attackers favor USDT for its stability and ease of transfer. Tether can freeze funds in cooperation with law enforcement, but only upon formal judicial request.

- USDC

USDC is a stablecoin jointly launched by Circle and Coinbase, emphasizing compliance and transparency, backed by real USD reserves, and subject to regular audits. USDC is also issued on multiple blockchains and is more common in North American markets. Like USDT, it can be frozen in cooperation with law enforcement following formal judicial procedures.



## (2) Core Concepts in Tracing

### Wallets

- Hot Wallet: Always connected to the internet, with private keys stored on network devices. Used for frequent transactions, such as mobile wallets (imToken) or browser extension wallets (MetaMask).
- Cold Wallet: Stores private keys offline, such as hardware wallets like Ledger or Trezor. Used for storing large amounts of assets or for long-term storage.

### Blockchain Addresses

- Deposit Address: Used for depositing to exchanges, typically controlled by the exchange and linkable to user accounts.

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Token
<a href="#">0xa1f5ddb909d...</a>	Transfer	15566025	2022-09-19 7:17:47	<a href="#">0x9225CE41...A7d31E831</a> <b>Binance deposit address</b>	<a href="#">0x2d7C8e61...6182a7462</a> <b>Binance hot address</b>	73	Tether USD (USDT)
<a href="#">0x8b8268eac7...</a>	Transfer	14064766	2022-01-23 23:06:57	<a href="#">0x2d7C8e61...6182a7462</a>	<a href="#">Binance 14</a>	1,086.021449	USDC (USDC)
<a href="#">0xb53a43462e...</a>	Transfer	13755499	2021-12-07 0:42:01	<a href="#">0xCdc22bFD...5A8669E59</a>	<a href="#">0x2d7C8e61...6182a7462</a>	1,086.021449	USDC (USDC)
<a href="#">0xfdea0921b3b...</a>	Transfer	13477946	2021-10-24 4:01:38	<a href="#">0x2d7C8e61...6182a7462</a>	<a href="#">Binance 14</a>	10,871.363208	USDC (USDC)
<a href="#">0x32f57883888...</a>	Transfer	13477815	2021-10-24 3:34:29	<a href="#">0x1275A8f8...1cA61A02d</a>	<a href="#">0x2d7C8e61...6182a7462</a>	10,871.363208	USDC (USDC)
<a href="#">0x3cbf77f680d...</a>	Transfer	12535001	2021-05-30 9:50:06	<a href="#">0x2d7C8e61...6182a7462</a>	<a href="#">Binance</a>	5,011.2643	Tether USD (USDT)
<a href="#">0x6e3204100b...</a>	Transfer From	12534638	2021-05-30 8:29:01	<a href="#">0x71F25432...60611da52</a>	<a href="#">0x2d7C8e61...6182a7462</a>	5,000	Tether USD (USDT)
<a href="#">0x47ef403656a...</a>	Transfer	11991383	2021-03-07 12:36:27	<a href="#">0x2d7C8e61...6182a7462</a>	<a href="#">Binance</a>	35	SushiToken (SUSHI)
<a href="#">0x239532ad94...</a>	Transfer	10779647	2020-09-02 4:20:57	<a href="#">0x471fD62c...BADea2098</a>	<a href="#">0x2d7C8e61...6182a7462</a>	35	SushiToken (SUSHI)

- Hot Wallet Address: Active exchange addresses for daily transactions, frequently interacting with multiple addresses.

**Address** 0x28C6c06298d514Db089934071355E5743bf21d60 99+

**Sponsored:** Advertise across our explorers and boost your visibility. [Book your slot here!](#)

**Binance 14** **Binance** **Exchange**

**Overview**

ETH BALANCE  
 ♦ 40,582.513959393412377643 ETH

ETH VALUE  
 \$148,132,592.53 (@ \$3,650.16/ETH)

TOKEN HOLDINGS  
 >\$268,508,203.90 (>401 Tokens) ⓘ

**More Info**

PRIVATE NAME TAGS  
+ Add

TRANSACTIONS SENT  
 Latest: 9 secs ago ↗ First: 4 yrs 100 days ago ↗

FUNDED BY  
 ♦ [Binance 31](#) | 4 yrs 101 days ago

- Cold Wallet Address: Long-term storage for large sums, with few transactions but large amounts.

**Address** 0xBE0eB53F46cd790Cd13851d5E5f43D12404d33E8 99+

**Sponsored:** Advertise across our explorers and boost your visibility. [Book your slot here!](#)

**Binance 7** **Binance** **# Cold Wallet** **Exchange**

**Overview**

ETH BALANCE  
 ♦ 1,996,008.370102613548925904 ETH

ETH VALUE  
 \$7,309,183,981.50 (@ \$3,661.90/ETH)

TOKEN HOLDINGS  
 >\$46,434.73 (>401 Tokens) ⓘ

**More Info**

PRIVATE NAME TAGS  
+ Add

TRANSACTIONS SENT  
 Latest: 243 days ago ↗ First: 6 yrs 284 days ago ↗

FUNDED BY  
[0x00f94513...6D1a3f243](#) | 6 yrs 308 days ago

- Regular Address: A wallet address controlled by an individual, without obvious labels.

**Address** 0x3464824903c2b8eae2895939096F2A4Aa1C59C5A

Feature Tip: Add private address tag to any address under [My Name Tag](#) !

**Overview**

ETH BALANCE  
0.000008611686646889 ETH

ETH VALUE  
\$0.03 (@ \$3,662.70/ETH)

TOKEN HOLDINGS  
\$0.00 (>205 Tokens)

**More Info**


PRIVATE NAME TAGS  
[+ Add](#)

TRANSACTIONS SENT  
Latest: 149 days ago | First: 4 yrs 154 days ago

FUNDED BY  
[0x5f76f00b...A54c6331A](#) | 4 yrs 154 days ago

- Contract Address: A deployed smart contract address that cannot initiate transactions itself; represents code on the blockchain capable of receiving assets, distributing funds, and executing logic (e.g., staking, lending, or trading).

**Contract** 0x881D40237659C251811CEC9c364ef91dC08D300C

Sponsored:  Remittix - Join the Remittix (RTX) presale today - **don't miss your chance to secure 100x gains!**

[Metamask: Swap Router](#) [Source Code](#) [# MetaMask](#) [# DEX](#)

**Overview**

ETH BALANCE  
0 ETH

ETH VALUE  
\$0.00

TOKEN HOLDINGS  
>\$188,971.60 (>323 Tokens)

**More Info**

PRIVATE NAME TAGS  
[+ Add](#)

CONTRACT CREATOR  
[AirSwap: Legacy Deplo...](#) | 4 yrs 292 days ago

- Multi-Signature Address: Requires multiple private keys for authorization, commonly used by teams or institutions for asset custody.

**Contract** 0xAF28bcB48C40dBC86f52D459A6562F658fc94B1e

**Sponsored:** Advertise across our explorers and boost your visibility. [Book your slot here!](#)

[Source Code](#) [Smart Account by Safe](#) [Owners](#)

**Overview**

ETH BALANCE  
9.34411529422890574 ETH

ETH VALUE  
\$34,180.90 (@ \$3,658.01/ETH)

TOKEN HOLDINGS  
\$226,033.76 (129 Tokens)

**More Info**

PRIVATE NAME TAGS  
[+ Add](#)

CONTRACT CREATOR  
[Juicebox: Deployer](#) | 4 yrs 17 days ago

- **Burn Address:** An address without a known private key, used to destroy or pseudo-destroy assets, e.g., the all-zero address (0x00).

**Address** 0x00

**Feature Tip:** Add private address tag to any address under [My Name Tag](#) !

This address is not owned by any user, is often associated with token burn & mint/genesis events and used as a generic null address

[Null: 0x000...000](#) [# Blocked](#) [# Burn](#) [# Genesis](#)

**Overview**

ETH BALANCE  
14,123.425941382448463519 ETH

ETH VALUE  
\$51,622,236.62 (@ \$3,655.08/ETH)

TOKEN HOLDINGS  
> 179965481786219000555... (>400 Tokens)

**More Info**

PRIVATE NAME TAGS  
[+ Add](#)

MINED:  
5,026 Blocks and 2 Uncles

TRANSACTIONS SENT  
Latest: N/A First: N/A

FUNDED BY  
[0xa89AC93b...2543F3E57](#) | 9 yrs 360 days ago

### Transaction Structure and Elements

- **Block Height:** The position of a block in the blockchain, used to determine transaction order.

**Block #23042969**

---

**Overview** | Consensus Info | Blob Info

---

Block Height: 23042969 < >

Status: Finalized

Timestamp: 5 hrs ago (Aug-01-2025 01:31:59 AM +UTC)

Proposed On: Block proposed on slot [12265658](#), epoch [383301](#)

Transactions: [109 transactions](#) and [11 contract internal transactions](#) in this block

Withdrawals: [16 withdrawals](#) in this block

---

Fee Recipient: [Fee Recipient: 0x6897...f88](#) in 12 secs

Block Reward: 0.004362010672765449 ETH (0 + 0.009867421207258149 - 0.0055054105344927)

Total Difficulty: 0

Size: 31,451 bytes

- Transaction Hash: The unique identifier (ID) for each transaction, enabling tracking of transfers or contract calls—like a transaction’s fingerprint.

Transaction Hash: 0x7214ce05ec66756b2e3e0effa9a413fb4add9e1c45baecb8c4e29172b34b6678


Status: Success

Block: 23042969 1713 Block Confirmations

Timestamp: 5 hrs ago (Aug-01-2025 01:31:59 AM UTC) | Confirmed within 30 secs

---

Sponsored: 



**Advertise on** BaseScan  
Scan Original

---

From: [0xB6E2cb86fefE1b3f9a61135D07AF2d614D4043AB](#)

To: [0x00 \(Null: 0x000...000\)](#)


---

Value: ♦ 0 ETH (\$0.00)

Transaction Fee: 0.00003391207090528 ETH (\$0.12)

Gas Price: 1.341458501 Gwei (0.000000001341458501 ETH)

- Gas: The “fuel” cost of blockchain operations. Gas analysis can reveal transaction timing, priority, and even the source of fee funding.

Transaction Hash:	0xfa0ec652b2e959ae33f4a774bc39da016fb2a64436e87a66c1782da239361c97
Status:	Success
Block:	20890900 2153816 Block Confirmations
Timestamp:	300 days ago (Oct-04-2024 08:15:59 AM UTC)   Confirmed within 8 secs
Sponsored:	<div style="text-align: center;">  </div>
From:	0xEbA88149813BEc1cCcccFDb0daCEfaaa5DE94cB1
To:	0xA7A1c66168cC0b5fC78721157F513c89697Df10D
Value:	0.04080424 ETH \$148.71
Transaction Fee:	0.000105 ETH \$0.38
Gas Price:	5 Gwei (0.000000005 ETH)
Ether Price:	\$2,414.67 / ETH
Gas Limit & Usage by Txn:	60,000   21,000 (35%)
Gas Fees:	Base: 4.287140895 Gwei
Burnt Fees:	Burnt: 0.000090029958795 ETH (\$0.33)

- Mixing: Using mixer protocols or services (e.g., Tornado Cash, Wasabi) to obfuscate transaction sources and destinations.

8f6c2b9bc4bc87093ef6ca31ed13f1065b275ff179c1e27aa08ca90eb2892b5a	2024/05/04 04:37:36 (1年2个月前)		
bc1qwygjry8ylcug7vdfdyafucuktyryenx9uf0htg	3.0703 BTC	Wasabi V2.0(bc1q...exf4)	3.07024205 BTC

- Swap: Token exchanges on DEXs (e.g., Uniswap, PancakeSwap), which may change asset form in the process.

Overview
Internal Txns
Logs (22)
State
</> API

**TRANSACTION ACTION**

- Swap 78,095.55 (\$88,247.97) EIGEN for 109.98 (\$399,287.23) ETH on Uniswap V3
- Swap 109.98 (\$399,287.23) ETH for 261,034.52 (\$260,984.14) USDC on Uniswap V3
- Swap 4,338.64 (\$4,902.67) EIGEN for 6.088111 (\$22,103.64) ETH on Uniswap V3
- Swap 6.088111 (\$22,103.64) ETH for 14,417.70 (\$14,414.91) USDC on Uniswap V3
- Swap 4,338.64 (\$4,902.67) EIGEN for 8,075.80 (\$8,074.24) USDC on Uniswap V3

---

Transaction Hash: [0x1f3ee9ceed31e463d8e4bd6388f77dfdd4c6f20c51f8affa5c6259f3da2934f8](#)

Status: Success

Block: 20891470 2153318 Block Confirmations

Timestamp: 300 days ago (Oct-04-2024 10:10:23 AM UTC) | Confirmed within 1 sec

Sponsored: 

**Advertise on** **BaseScan**  
Scan Original

From: [0xA7A1c66168c0b5fC78721157F513c89697Df10D](#)

Interacted With (To): [0x881D40237659C251811CEC9c364ef91dC08D300C](#) (Metamask: Swap Router) ✔

ERC-20 Tokens Transferred: 15

All Transfers
Net Transfers

- ▶ From [0xA7A1c661...9697Df10D](#) To [MetaMask: Swaps Spe...](#) For 173,545.66828466 (\$196,106.61) Eigen (EIGEN)
- ▶ From [MetaMask: Swaps Spe...](#) To [0x807cF9A7...2f0D9bD38](#) For 86,772.834142330004 (\$98,053.30) Eigen (EIGEN)
- ▶ From [0x807cF9A7...2f0D9bD38](#) To [MetaMask: Swaps Spe...](#) For 288,135.759299 (\$288,080.15) USDC (USDC)
- ▶ From [Uniswap V3: EIGEN 4](#) To [0x: Exchange Proxy](#) For 109.977588069589813608 (\$399,307.39) Wrapped Ether (WETH)
- ▶ From [MetaMask: Swaps Spe...](#) To [Uniswap V3: EIGEN 4](#) For 78,095.550728096995600001 (\$88,247.97) Eigen (EIGEN)
- ▶ From [Uniswap V3: USDC 3](#) To [MetaMask: Swaps Spe...](#) For 261,034.518202 (\$260,984.14) USDC (USDC)

- Cross-Chain: Asset transfers between different blockchains, often involving bridge contracts; frequently used for laundering and dispersing funds.

Transaction Hash: [0x16ed29f9bf9914ea3b62e4e94829eaeef10118d04e82849a285ef8a5700defa1a](#)

Status: Success

Block: 21967334 1077579 Block Confirmations

Timestamp: 150 days ago (Mar-03-2025 03:44:47 PM UTC) | Confirmed within 9 secs

Sponsored: 

**Advertise on** **BaseScan**  
Scan Original

From: [0x8Ab1D1d3E7db399835172576CcE0bD1C200a1Ce8](#)

To: [0xD37BbE5744D730a1d98d8DC97c42F0Ca46aD7146](#) (THORChain: THORChain Router v4.1.1) ✔

Internal Transactions: 1

All Transfers
Net Transfers

- ▶ Transfer 257.26903778 ETH \$937,300.03 From [THORChain: THORChai...](#) To [0x9b3F783E...7274ba091](#)

Value: ♦ 257.26903778 ETH \$937,300.03

Transaction Fee: 0.000060192806372036 ETH \$0.22

Gas Price: 1.542258484 Gwei (0.00000001542258484 ETH)

- Input Data: Parameters included when calling a smart contract, decodable to reveal swap paths, recipients, etc., often viewable in blockchain explorers.

Ether Price: \$2,147.50 / ETH  
 Gas Limit & Usage by Txn: 44,103 | 39,029 (88.5%)  
 Gas Fees: Base: 1.411482404 Gwei | Max: 1.542258484 Gwei | Max Priority: 1.542258484 Gwei  
 Burnt & Txn Savings Fees: Burnt: 0.00055088746745716 ETH (\$0.20) | Txn Savings: 0 ETH (\$0.00)

Other Attributes: Txn Type: 2 (EIP-1559) | Nonce: 0 | Position in Block: 106

**Input Data:**  
 Function: depositWithExpiry(address vault, address asset, uint256 amount, string memo, uint256 expiration) \*\*\*  
 MethodID: 0x44bc937b  
 [0]: 00  
 [1]: 00  
 [2]: 00  
 [3]: 00a0

View Input As | Decode Input Data | View In Decoder | Advanced Filter | Write Contract

More Details: [Click to show less](#)

- Event Logs: Records of key operations during contract execution, useful for identifying token transfers, swaps, deposits, and withdrawals.

Overview | Internal Txns | **Logs (1)** | State

Transaction Receipt Event Logs

Address: 0xd37bbe5744d730a1d98d8dc97c42f0ca46ad7146 (THORChain: THORChain Router v4.1.1)

Name: Deposit (index\_topic\_1 address to, index\_topic\_2 address asset, uint256 amount, string memo) [View Source](#)

Topics: 0 0xef519b7eb82aaf6ac376a6df2d793843ebfd593de5f1a0601d3cc6ab49ebb395  
 1: to Dec → 0x9b3f783e80751a64cc38b5613267e097274ba091  
 2: asset Dec → 0x00

Data: amount : 257269037780000000000000  
 memo: =:b:191du9ivk3k5YekuXFgtkoVeI6pK76wZmf:0/1/0:dx:10

### Platform Type

- Centralized Exchanges (CEX): Platforms where users deposit assets into platform-controlled accounts, allowing for asset freezes and fiat on/off-ramps, but with identifiable addresses linked to user identities (e.g., Binance, OKX).



- Decentralized Exchanges (DEX): On-chain platforms where users hold their own private keys and trade via smart contracts. No identity checks, making them popular for illicit swaps; assets can be traced but not frozen (e.g., Uniswap, Curve).
- Bridges: Cross-chain asset transfer protocols, often used by attackers to evade tracing or launder funds (e.g., THORChain, Wormhole).
- Nested Platforms: Third-party services that store assets in large CEX wallets (e.g., Binance), requiring secondary path resolution to determine actual ownership.

## UTXO and Change

In the Bitcoin network, the source and destination of every transaction are based on the UTXO (Unspent Transaction Output) model. You can think of it as a “change” system—you cannot directly modify an account balance; instead, you must “spend” an entire note and receive the remainder as change. This model differs from account-based blockchains like Ethereum.

<a href="#">c45c3d7c972857f299e28192e3e30f9f2adc3fd3cdd1962f809faa869227fb65</a>		2025/08/04 23:25:20 (2 天前)	
<a href="#">bc1qph3wqvnequn0cmz5jpvwu9yyyz0sv8gex4wz0</a>	1.27098433 BTC	<a href="#">bc1q46vm4zgg0p22fc03m5qkfmwevlmqasleef9</a>	0.111 BTC
		<a href="#">bc1qph3wqvnequn0cmz5jpvwu9yyyz0sv8gex4wz0</a>	1.1599801 BTC

For example, suppose you want to pay 0.6 BTC, and your wallet contains a single UTXO worth 1 BTC. You cannot “cut out” just 0.6 BTC from that 1 BTC; you must use the entire 1 BTC as the transaction input: 0.6 BTC is sent to the recipient, and the remaining 0.4 BTC (minus transaction fees) is returned to you. However, it is not sent back to your original address—it is returned to a newly generated address in your wallet, called the change address. Typically, wallets automatically generate a new change address for each transaction to enhance privacy and avoid address reuse. In some wallet configurations, however, the change may be sent to an existing address in your wallet.

The core logic of this system is that a UTXO must be fully consumed, and any unspent portion is turned into a new UTXO via the change mechanism for future use. This ongoing process of “spending old UTXOs and producing new UTXOs” is the foundation of how Bitcoin and similar blockchains (e.g., Litecoin, Dogecoin) operate. In contrast, account-based chains like Ethereum

allow partial spending of an account balance, where each transaction directly updates the account state without the “bill-splitting” and change-handling process of the UTXO model.

Because each transaction must fully consume its input UTXOs and generate new outputs, the UTXO model naturally produces multiple output addresses—one being the recipient address, and another being the change address. From an on-chain data perspective, these two addresses are treated equally in the transaction, with no explicit indicator of which one is change and which one is the actual recipient. This presents certain challenges for blockchain analysis.

Understanding these concepts helps us more quickly assess address behavior, risk exposure paths, and potential laundering activities during investigations. Next, we will use a blockchain explorer to examine a real transaction and demonstrate how to locate and interpret public data to improve tracing efficiency.

### (3) Blockchain Explorers

Once you have mastered the basic concepts, the first step in on-chain tracing is usually the blockchain explorer. Whether you are checking transaction records, viewing an address balance, or verifying the details of a smart contract call, you will inevitably rely on an explorer. Each blockchain has its own dedicated explorer, but the operation logic is generally similar—once you learn how to use one, you can easily adapt to others. Common blockchain explorers include:

Chain	Explorer
Bitcoin	<a href="https://www.blockchain.com/explorer">https://www.blockchain.com/explorer</a> <a href="https://mempool.space">https://mempool.space</a>
Ethereum	<a href="https://etherscan.io">https://etherscan.io</a>
TRON	<a href="https://tronscan.org">https://tronscan.org</a>
BNB Chain	<a href="https://bscscan.com">https://bscscan.com</a>
Polygon	<a href="https://polygonscan.com">https://polygonscan.com</a>

Solana	<a href="https://solscan.io/">https://solscan.io/</a>
Avalanche	<a href="https://snowtrace.io/">https://snowtrace.io/</a>
Optimism	<a href="https://optimistic.etherscan.io">https://optimistic.etherscan.io</a>
Arbitrum	<a href="https://arbiscan.io">https://arbiscan.io</a>
Aggregated	<a href="https://www.oklink.com/">https://www.oklink.com/</a>

Let's take Etherscan as an example. When you have a suspicious address, the first step is to enter it into the search bar. On the address details page, you can view its balance, token holdings, and transaction history. Etherscan and other explorers often tag addresses and contracts—for example, marking exchange addresses, bridge contracts, known hacker wallets, or project wallets—helping you quickly identify the counterparty's background. By clicking on any transaction, you can view detailed information such as the transaction hash, sender and recipient addresses, transfer amount, timestamp, block height, gas fees, and even the specific contract function called.

ETH Price: \$3,619.55 (-6.32%) Gas: 1.023 Gwei

0x9D42A049F88f1DB4b304441081Aff7C40D857BeA

Etherscan Home Blockchain Tokens NFTs Resources Developers More Sign In

Address 0x9D42A049F88f1DB4b304441081Aff7C40D857BeA Buy Presale Play Gaming

Feature Tip: Add private address tag to any address under My Name Tag!

This address has been reported as **compromised**. Do not send funds here. Reported by ZachXBT.

Compromised: 0x9d4...bea

**Overview**

ETH BALANCE  
0.000081596937618 ETH

ETH VALUE  
\$0.30 (@ \$3,619.55/ETH)

TOKEN HOLDINGS  
\$254.56 (2 Tokens)

**More Info**

PRIVATE NAME TAGS  
+ Add

DELEGATED ADDRESS  
0x63c0c19a...A07DAE32B

TRANSACTIONS SENT  
Latest: 21 days ago First: 69 days ago

FUNDED BY  
Tornado.Cash: 1 ETH | 69 days ago

**Multichain Info**

\$258.72 (Multichain Portfolio)

1 address found via Blockscan

Advertise on BaseScan

Search for Token Name

ERC-20 Tokens (2)

- ASTRA PROTOC... (ASTRA) \$254.56 @0.0021
- Dai Stableco... (DAI) \$0.00 @0.9996

VIEW ALL HOLDINGS

Transactions Analytics Assets Cards New

Download Page Data

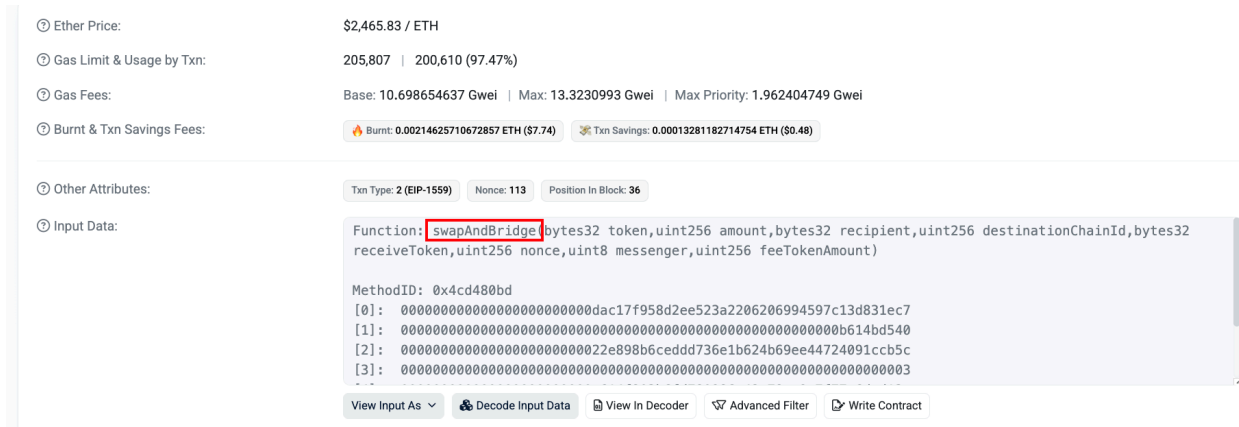
Date Time (UTC)	From	To	Amount	Txn Fee
2025-07-11 1:16:47	Compromised: 0x9d4...	0x0FCE3B1e...3f3Afb3c9	0.8775545 ETH	0.00007086
2025-07-11 1:15:35	Compromised: 0x9d4...	Blocklords: LRDS T...	0 ETH	0.00016587
2025-07-11 1:05:47	Compromised: 0x9d4...	Tornado.Cash: Ro...	100 ETH	0.00514406
2025-07-11 1:03:35	0x13d3326b...695B990E2	Compromised: 0x9d4...	19.9081974 ETH	0.00004965
2025-07-07 8:13:11	0x451983E4...1D489c92C	Compromised: 0x9d4...	18.4161621 ETH	0.0000122
2025-07-07 8:02:11	0x45192110...81Bb2c92C	Compromised: 0x9d4...	0 ETH	0.00001314

Going further, the Token Transfers tab displays the token transfer records involving this address. For example, a USDT transfer record will show the amount, sender, recipient, token contract address, and symbol (such as USDT, DAI, USDC). This allows you to trace each transaction to see where the funds came from and where they went. Many scams use “airdrop scams” to create false impressions—for instance, you might receive a token that is neither verified nor valuable, indicating it could be a fake. By checking the Token page and contract code on the explorer, you can verify whether a token is a legitimate asset or an imitation.

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Token
0xfa25686f4b2...	Transfer	22902825	2025-07-12 11:35:47	Compromised: 0x9d4...	OUT 0x451983cc...049f8c92c	0.1	ERC-20: ETH
0x4bf2b84240c...	Transfer	22892658	2025-07-11 1:28:23	Compromised: 0x9d4...	OUT 0x45192519...9a390c92c	0.1	ERC20 ***
0x1460bf06ecf...	Transfer	22892594	2025-07-11 1:15:35	Compromised: 0x9d4...	OUT 0x0FCE3B1e...3f3Afb3c9	2,553.79512888	BLOCKLORDS (LRDS)
0x492c43c70b...	Transfer	22866076	2025-07-07 8:18:23	Compromised: 0x9d4...	OUT 0x451983cc...049f8c92c	0.1	ERC-20: ETH
0xa02e8c1b1fc...	Transfer	22866056	2025-07-07 8:14:11	Compromised: 0x9d4...	OUT 0x45192519...9a390c92c	0.1	ERC20 ***
0xb43ced826b...	Transfer	22865983	2025-07-07 7:59:35	Compromised: 0x9d4...	OUT 0x45192110...81Bb2c92c	0.1	ERC-20: ETH
0xf236412f824...	Transfer	22865980	2025-07-07 7:58:59	Compromised: 0x9d4...	OUT 0x45192519...9a390c92c	0.1	ERC20 ***
0x83ce83d300...	Fill Relay	22795902	2025-06-27 12:53:23	Across Protocol: Ether...	IN Compromised: 0x9d4...	0.01878363	Wrapped Ethe... (WETH)
0xc82dd76196f...	Fill V3Relay	22795899	2025-06-27 12:52:47	Across Protocol: Ether...	IN Compromised: 0x9d4...	0.95854701	Wrapped Ethe... (WETH)
0xf1d0b74951e...	Mooo Z10896...	22795866	2025-06-27 12:46:11	Compromised: 0x9d4...	OUT CoW Protocol: GPv2Se...	315,342.34732222	QBX (QBX)
0xccb8e780ff0...	Swap	22568004	2025-05-26 15:58:35	Uniswap V2: BLOODBO...	IN Compromised: 0x9d4...	14,767,798,388	ERC-20: Blo...rie
0x47b4921f23f...	Swap	22563321	2025-05-26 0:10:47	Compromised: 0x9d4...	OUT MetaMask: Swaps Spe...	50,493.94180252	PORTAL (PORTAL)
0x7d07aa6744...	Swap	22563317	2025-05-26 0:09:59	Compromised: 0x9d4...	OUT MetaMask: Swaps Spe...	107,950.028117	HyperCycle T... (HyPC)

SCAM

Blockchain explorers can also analyze contract calls. When an address interacts with a smart contract (such as executing a DEX swap, borrowing funds, or minting an NFT), the system will display the contract function name (such as swapExactTokensForTokens or borrow). These details often help you determine the real purpose of the address. If the Input Data is encoded, you can try decoding it to better understand the exact action taken. For advanced users, you can go to the contract's source code page to check whether it is open source and assess its functionality and security. The Event Logs section is also crucial, recording contract-triggered events and parameter details, such as how many tokens were received by an address and through which function they were sent.



In addition to viewing static data, it is equally important to observe the timing and flow of funds. For example, does the attacker frequently perform batch transfers? Is there evidence of wash trading or other abnormal activity? While the interfaces of different blockchain explorers may vary, the underlying logic is nearly identical. Becoming familiar with several platforms will significantly improve your cross-chain tracking capabilities.

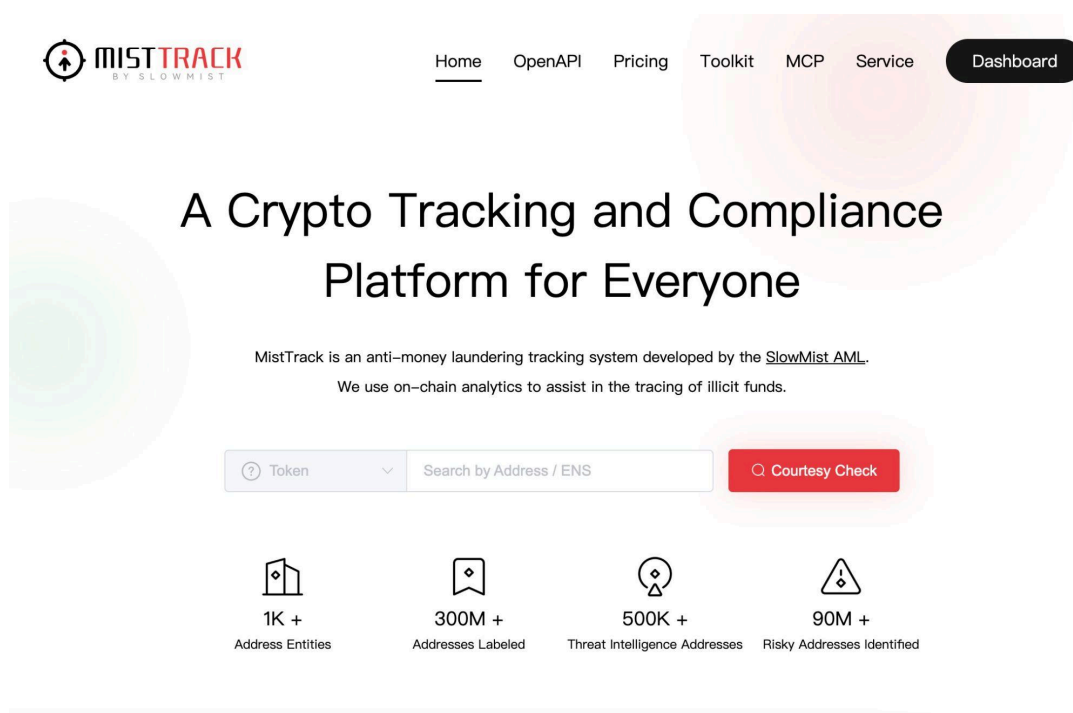
Blockchain explorers are the most basic and commonly used portals for on-chain intelligence, but they serve merely as a “window for reading data” and have their limitations. Therefore, in the next section, we will introduce some additional tools.

## 2. Tracing Tools

In real-world applications, we often face highly complex scenarios such as multi-chain asset transfers, fund mixing, and contract interaction analysis. Blockchain explorers, due to their dispersed data and less intuitive presentation, are not well suited for identifying and tracing complex fund flows. As a result, more users and professionals are turning to specialized asset tracing tools to achieve more efficient and systematic on-chain security management. Among these tools, [MistTrack](#), an on-chain analysis and anti-money laundering tracing platform developed by SlowMist, is the one we use most and recommend the most. If a blockchain explorer is the “magnifying glass” for on-chain data, then MistTrack is more like an “on-chain intelligence analysis desk” – it not only summarizes data but also helps you interpret it.

## (1) Introduction to MistTrack

MistTrack provides multiple functions, covering transaction monitoring, risk assessment, address labeling, and transaction behavior analysis, aiming to help users more efficiently identify illicit transactions, trace fund flows, enhance compliance capabilities, and build a full lifecycle security protection system for digital assets. Since its launch in 2022, MistTrack has been widely adopted in the blockchain security industry, serving over 100,000 users – tens of thousands of them paid customers – and playing a critical role in multiple major on-chain security incidents worldwide. It has gradually become an indispensable compliance and risk control tool in the global crypto industry.



As of now, MistTrack has accumulated over 300 million address labels, 1,000+ on-chain entities, 500,000+ threat intelligence data points, and 90 million+ risky addresses. The system supports tracking on 18 mainstream public blockchains and hundreds of different tokens, covering a wide range of asset types and on-chain ecosystems. MistTrack also supports cross-chain tracing, currently compatible with 15 mainstream cross-chain bridge protocols and tools including Chainflip, AllbridgeCore, and LIFI, with continuous expansion underway. Backed by this massive

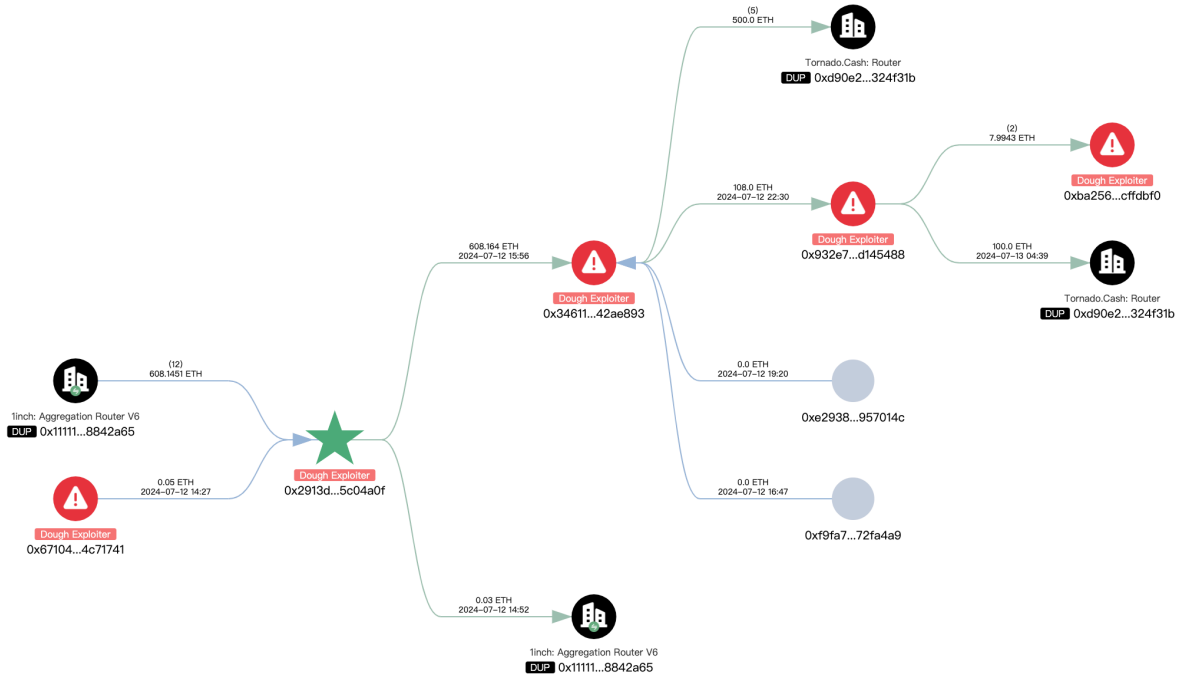
and ever-updating data foundation, MistTrack provides users with strong technical support to tackle complex and evolving on-chain security threats.

Core functions of MistTrack include:

- **AML Risk Score:** MistTrack calculates an AML risk score for each address based on its associated entity, historical transaction activity, and data from SlowMist's malicious wallet address database. If the address belongs to a high-risk entity (such as a mixing service) or has interacted with known risky entities, it will be flagged as a risky address. Using verified datasets of ransomware, theft, phishing, and other illicit activities, MistTrack marks involved addresses accordingly. Users can analyze each wallet address like a professional compliance officer, determining whether it is linked to illicit funds. By clicking the "Risk Report" button, users can instantly generate a risk analysis report for the address.
- **Address Labels:** MistTrack can identify the entity behind an address (e.g., Coinbase or Binance), locate on-chain and off-chain tags such as ENS, MEV Bots, DeFi Whales, and detect which wallet app (e.g., imToken, MetaMask) the address uses. With the address labeling feature, users can better understand the background of an address.
- **Counterparty Analysis / Transaction Action Analysis:** MistTrack provides the information that matters most to users. Unlike standard blockchain explorers, which can be complex and unintuitive, MistTrack evaluates all historical transactions of an address and summarizes its behavior in an easy-to-understand way, helping users interpret activity patterns.
- **Address Profile Analysis:** Collects all historical data for a target address and summarizes its traces, including platforms used, related incidents, and related information, helping users build a profile of the target address.
- **Favorites / Monitoring:** Users can save specific wallet addresses in their private favorites list and gather all needed information in one place. They can also add whale and KOL addresses to monitor their on-chain activities in real time, track their latest transactions, and gain investment insights.
- **Investigation Graphs:** MistTrack visualizes all incoming and outgoing transaction relationships of a queried address in dynamic, interactive graphs. Users can filter and sort data directly on the chart to monitor selected information easily. MistTrack supports



flexible tracing, analysis, and record-keeping, and its sharing feature enables collaborative case work with colleagues.



At the same time, to facilitate more efficient address analysis, we have developed the MistTrack OpenAPI for seamless integration into third-party applications.

- OpenAPI interface service: By calling the OpenAPI, MistTrack will return the label list for a given address, an address overview, risk score, detailed risk information list, transaction investigation results, transaction behavior analysis results, address profile analysis results, and counterparty analysis results.

## (2) MistTrack in Use

The following is the tracking process of the Cork Protocol attack on May 28, 2025. The attacker's address is [0xea6f30e360192bae715599e15e2f765b49e4da98](https://etherscan.io/address/0xea6f30e360192bae715599e15e2f765b49e4da98).

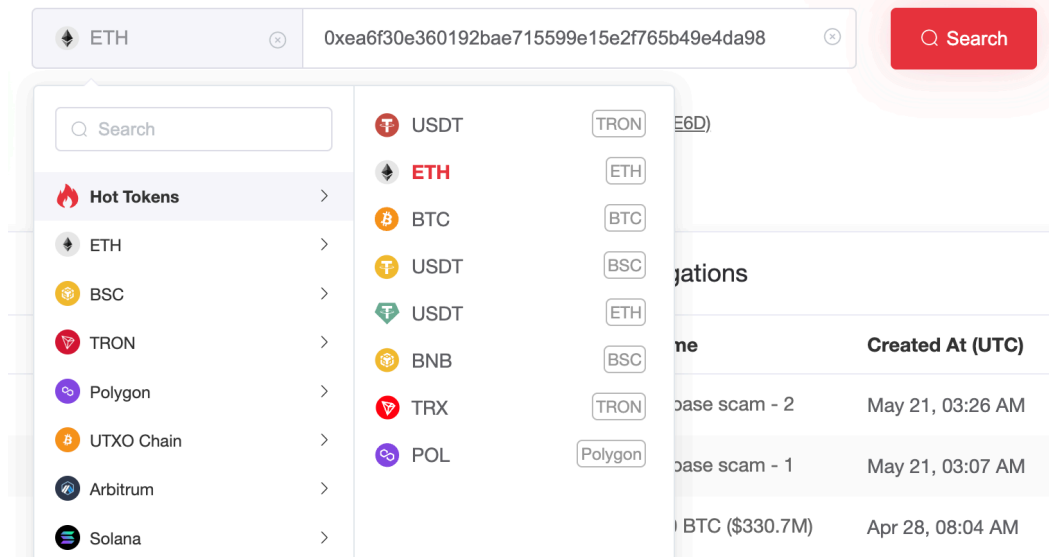
First, using tools such as Etherscan and DeBank, we can initially determine that the attacker gained 3,761.878 wstETH. At the same time, the wstETH was converted into 4,527 ETH through 8 transactions.

2025/05/28 19:51:35 0x8940...ada0	fillOrderArgs Ox0000...0d95	-1,212.2009 wstETH (\$3,911,859) +1,458.7190 ETH (\$3,911,701)
2025/05/28 19:50:59 0x060f...9e97	fillOrderArgs 1inch	-242.4402 wstETH (\$782,371.78) +291.7485 ETH (\$782,352.85)
2025/05/28 19:49:59 0x95e7...fb86	fillOrderArgs Ox2d58...631a	-365.9360 wstETH (\$1,180,902) +440.3652 ETH (\$1,180,883)
2025/05/28 19:47:35 0xf947...5859	fillOrderArgs Ox2d58...631a	-457.9925 wstETH (\$1,477,974) +551.1588 ETH (\$1,477,987)
2025/05/28 19:46:11 0x713f...f91c	Contract Interaction Ox2d58...631a	-341.9547 wstETH (\$1,103,512) +411.5309 ETH (\$1,103,561)
2025/05/28 19:46:11 0xab0a...6cf5	Contract Interaction Ox2d58...631a	-253.9268 wstETH (\$819,439.83) +305.5922 ETH (\$819,476.12)
2025/05/28 19:46:11 0x2061...ba38	Contract Interaction Ox2d58...631a	-511.2392 wstETH (\$1,649,806) +615.2590 ETH (\$1,649,879)
2025/05/28 19:45:23 0xa874...d5bc	Contract Interaction 1inch	-376.1878 wstETH (\$1,213,985) +452.7362 ETH (\$1,214,058)
2025/05/28 19:41:35 0x605e...0c50	Contract Interaction Ox9af3...bb09	+3,761.8780 wstETH (\$12,139,849)

Swap

At this point, we input the attacker's address into MistTrack and initiate a query.

## Risk Analysis, Intelligent Tracking



Name	Created At (UTC)
base scam - 2	May 21, 03:26 AM
base scam - 1	May 21, 03:07 AM
BTC (\$330.7M)	Apr 28, 08:04 AM

The [results](#) show that the address has a risk score of 100 (high risk), has transactions on both the Ethereum and Base chains, with its first transaction on May 20 and the most recent one on June 30. In total, it has received 4,531.977 ETH, currently holds a balance of 0 ETH, and has interacted with both DeFi platforms and exchanges.

ETH | EOA

0xea9f30e360192bae715599e15e2f765b49e4da98 Copy Report Favorites

Chains: Ethereum

Portfolio Explorer

**AML Risk Score**

Risk Score: 100

Risk Level: Severe

Threats:
 

- Threat
- Malicious address
- Involved illicit Activity
- Interact with high-risk tag address

Overview

Balance: 0.0053 ETH

First seen (UTC): May 20, 02:52 PM

Total received: 4,531.977 ETH

Incoming txn: 19

Txn count: 40

Last seen (UTC): Jun 30, 02:10 PM

Total spent: 4,532.7988 ETH

Outgoing txn: 21

Counterparty Analysis Transaction Actions Analysis

Incoming Transaction Actions

Category	Percentage
Exchange	75%
Transfer	16.67%
DEX	8.33%

Outgoing Transaction Actions

Category	Percentage
Create contract	50%
Transfer	33.33%
DEX	16.67%

Address Profile Analysis

Gas fee source: Swapuz.com Common use time: 10:00-12:00 14:00-16:00 (UTC)

Platform Interaction

Exchange: 1	DeFi: 2	Coin Mixer: 0	NFT: 0
-------------	---------	---------------	--------

Related Events

Theft: 3	Phishing: 0	Ransom: 0	Laundering: 0
----------	-------------	-----------	---------------

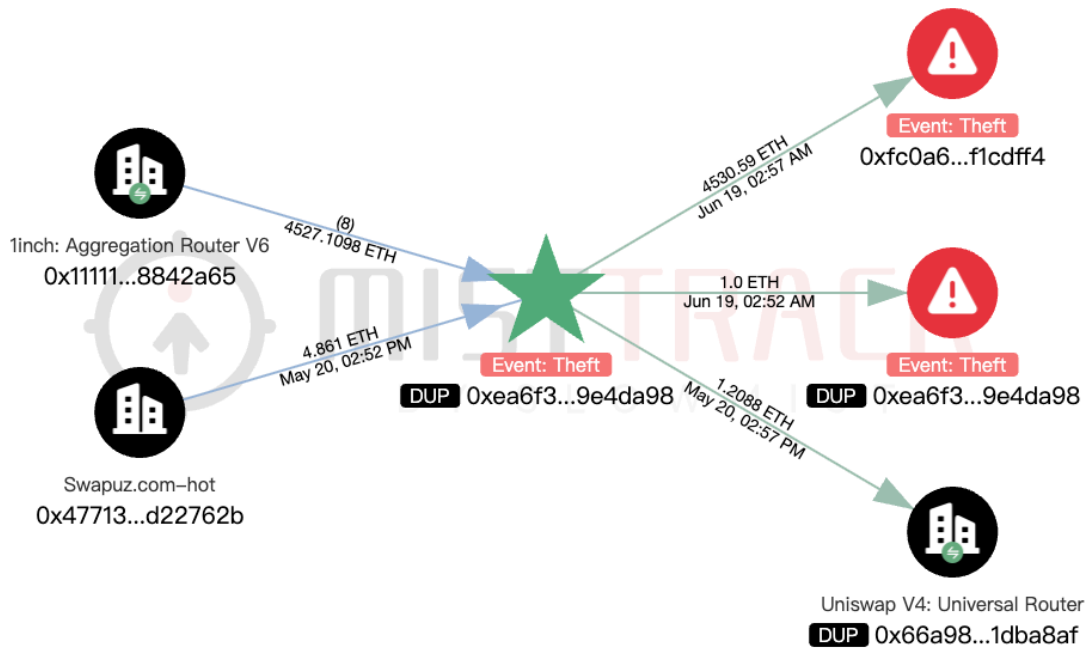
Related Information

Wallet: 0	ENS: 0	Twitter: 0
-----------	--------	------------

Transaction Graph

Investigate with OpenAPI

























Next, we focus on the fund transfer graph.



Starting with the left side (incoming funds), from bottom to top:

- The first entry shows 4.861 ETH transferred from Swapuz.com, which—based on the timeline—appears to be the initial source of funds for the attacker.
- The second entry consists of a total of eight transactions. By clicking on the arrow line, we can see the details of each.

Transaction Details ×

✓	Time (UTC) ↕	Sender	Recipient	Amount ↕	TXID
✓	May 28, 11:45 AM	0x111111...f8842a65  <small>(1inch: Aggregation Router V6)</small>	0xea6f30...49e4da98  <small>(1inch: Aggregation Router V6)</small>	452.7362 ETH	0xa8741f...4215d5bc 
✓	May 28, 11:47 AM	0x111111...f8842a65  <small>(1inch: Aggregation Router V6)</small>	0xea6f30...49e4da98  <small>(1inch: Aggregation Router V6)</small>	551.1588 ETH	0xf9472a...3c015859 
✓	May 28, 11:51 AM	0x111111...f8842a65  <small>(1inch: Aggregation Router V6)</small>	0xea6f30...49e4da98  <small>(1inch: Aggregation Router V6)</small>	1,458.719 ETH	0x8940ca...ac24ada0 
✓	May 28, 11:49 AM	0x111111...f8842a65  <small>(1inch: Aggregation Router V6)</small>	0xea6f30...49e4da98  <small>(1inch: Aggregation Router V6)</small>	440.3652 ETH	0x95e79d...acb7fb86 
✓	May 28, 11:50 AM	0x111111...f8842a65  <small>(1inch: Aggregation Router V6)</small>	0xea6f30...49e4da98  <small>(1inch: Aggregation Router V6)</small>	291.7485 ETH	0x060f81...e9369e97 
✓	May 28, 11:46 AM	0x111111...f8842a65  <small>(1inch: Aggregation Router V6)</small>	0xea6f30...49e4da98  <small>(1inch: Aggregation Router V6)</small>	615.259 ETH	0x206175...f3b1ba38 
✓	May 28, 11:46 AM	0x111111...f8842a65  <small>(1inch: Aggregation Router V6)</small>	0xea6f30...49e4da98  <small>(1inch: Aggregation Router V6)</small>	411.5309 ETH	0x713f29...2d2bf91c 
✓	May 28, 11:46 AM	0x111111...f8842a65  <small>(1inch: Aggregation Router V6)</small>	0xea6f30...49e4da98  <small>(1inch: Aggregation Router V6)</small>	305.5922 ETH	0xab0a99...33b96cf5 

< 1 >
↓ Export

Randomly checking the last transaction ([0xab0a99...b96cf5](#)), we find that it involves the attacker swapping 253.9267 wstETH for 305.5922 ETH. Checking the remaining seven transactions confirms they all involve swapping wstETH for ETH, consistent with the earlier finding that the attacker converted wstETH to 4,527 ETH through eight transactions.

Transaction Hash: [0xab0a997f307ff45d9fcbfd2672f108d49546b86104eb06146bf90c3433b96cf5](#)

Status: Success

Block: 22581052 485139 Block Confirmations

Timestamp: 67 days ago (May-28-2025 11:46:11 AM UTC)

---

From: [0x477CAC2fC44A60492A8B637b77a99BE4deBCEf20](#)

Interacted With (To): [0x2d5805A423D6CE771f06972Ad4499f120902631a](#)

---

Internal Transactions:

All Transfers Net Transfers

- ▶ Transfer 305.594960586459 ETH \$1,081,130.64 From [Fluid: Liquidity](#) To [0x5141B82f...27640a190](#)
- ▶ Transfer 305.594960586459 ETH \$1,081,130.64 From [0x5141B82f...27640a190](#) To [Wrapped Ether](#)
- ▶ Transfer 305.592227258019927378 ETH \$1,081,120.97 From [Wrapped Ether](#) To [Aggregation Router V6](#)
- ▶ Transfer 305.592227258019927378 ETH \$1,081,120.97 From [Aggregation Router V6](#) To [Cork Protocol Exploiter 1](#)

---

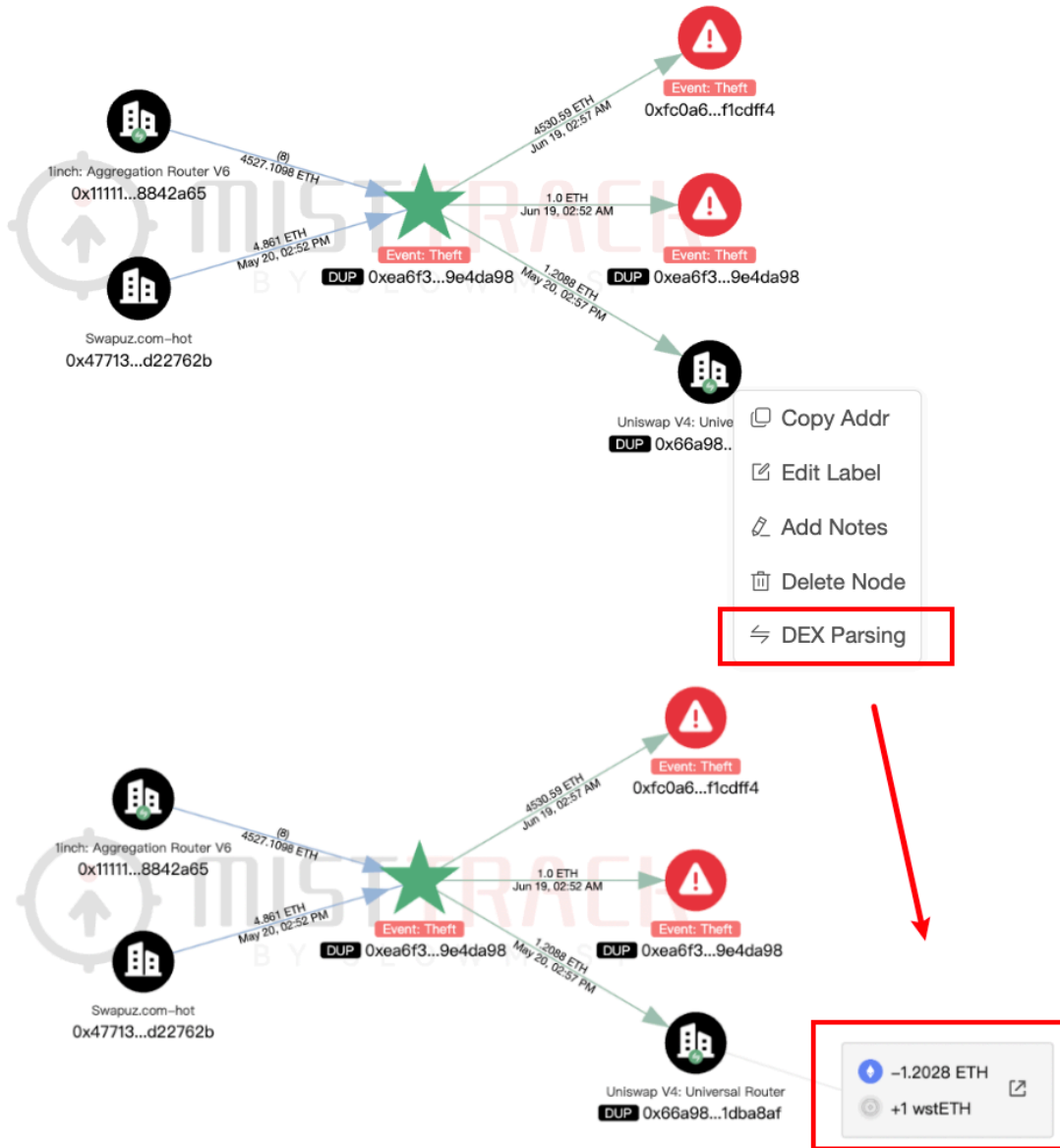
ERC-20 Tokens Transferred: 4

All Transfers Net Transfers

- ▶ From [Cork Protocol Exploiter 1](#) To [0x5141B82f...27640a190](#) For 253.926761987444613656 (\$1,085,564.84) 🔵 [Wrapped liqu... \(wstETH\)](#)
- ▶ From [0x5141B82f...27640a190](#) To [Fluid: Liquidity](#) For 253.926761987444613656 (\$1,085,564.84) 🔵 [Wrapped liqu... \(wstETH\)](#)
- ▶ From [0x5141B82f...27640a190](#) To [0x2d5805A4...20902631a](#) For 305.594960586459 (\$1,081,130.64) ⚪ [Wrapped Ethe... \(WETH\)](#)
- ▶ From [0x2d5805A4...20902631a](#) To [Aggregation Router V6](#) For 305.592227258019927378 (\$1,081,120.97) ⚪ [Wrapped Ethe... \(WETH\)](#)

Now looking at the right side (outgoing funds), from bottom to top:

The first entry shows 1.2088 ETH interacting with Uniswap. By right-clicking on Uniswap and selecting “DEX Parsing,” we can quickly determine that this transaction swapped 1.2028 ETH for 1 wstETH.



The second entry shows the attacker transferring 1 ETH to their own address. Reviewing the [transaction](#) details reveals an on-chain message: "sherlock missed it. ct > ds. uniswap hook is not problem." It is rumored that during the discussion of the issue, the Sherlock team, which audited the Cork Protocol, reportedly suspected the issue was caused by the Uniswap hook. The attacker intentionally left an on-chain message to clarify that the Uniswap hook had nothing to do with the issue.



**TRANSACTION ACTION**  
IDM: sherlock missed it. ct > ds. uniswap hook is not problem.

Read Chat 1

---

Transaction Hash: [0x92a53d817e9a626292270d93259b10cba05a1e55bd0651ca7ef57b63b7294cf0](#)

Status: Success

Block: 22735663 330766 Block Confirmations

Timestamp: 46 days ago (Jun-19-2025 02:52:23 AM UTC)

---

From: [0xEA6f30e360192bae715599E15e2F765B49E4da98](#) (Cork Protocol Exploiter 1)

To: [0xEA6f30e360192bae715599E15e2F765B49E4da98](#) (Cork Protocol Exploiter 1)

---

Value: ◆ 1 ETH \$3,559.70

Transaction Fee: 0.00002169347430888 ETH \$0.08

Gas Price: 0.931850271 Gwei (0.000000000931850271 ETH)

---

Ether Price: \$2,521.84 / ETH

Gas Limit & Usage by Txn: 35,425 | 23,280 (65.72%)

Gas Fees: Base: 0.431850271 Gwei | Max: 1.160162775 Gwei | Max Priority: 0.5 Gwei

Burnt & Txn Savings Fees: 🔥 Burnt: 0.00001005347430888 ETH (\$0.04) 💧 Txn Savings: 0.00000531511509312 ETH (\$0.02)

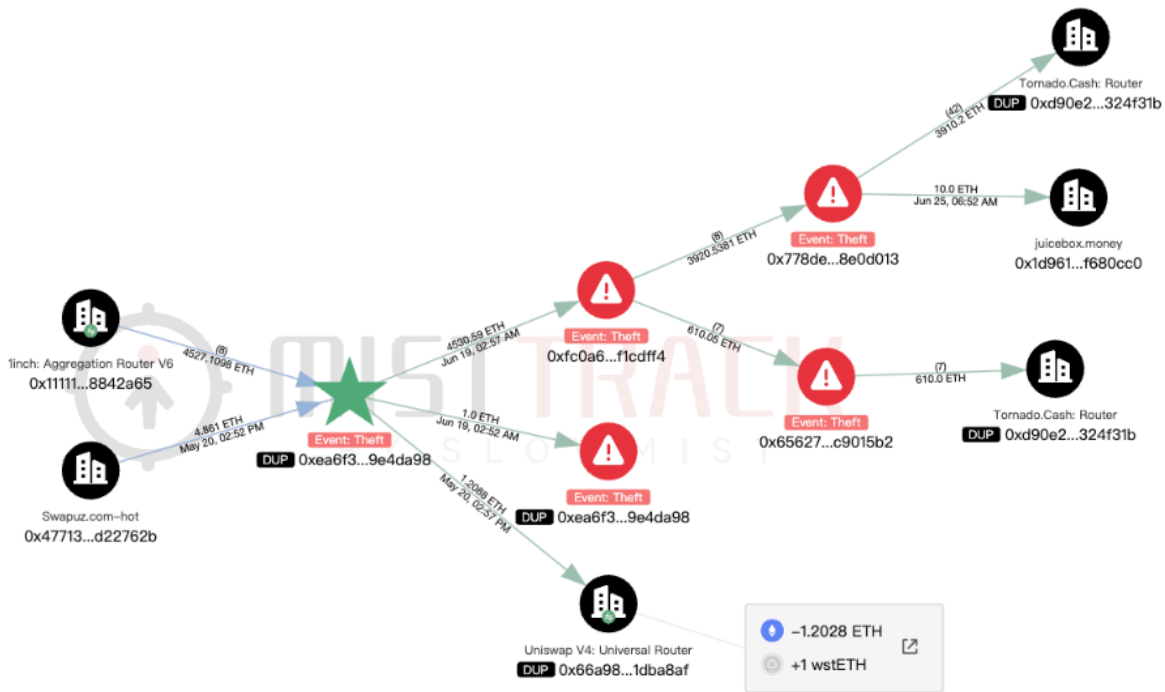
---

Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 16 Position In Block: 129

Input Data: sherlock missed it. ct > ds. uniswap hook is not problem.

View Input As ▼

The third entry shows the attacker transferring most of the funds—4,530.59 ETH—to a new address (0xfc0a6de0abd0985e7a910f8874c3abf23f1cdff4). Double-clicking this address reveals that it then split the ETH into two new addresses. Further expansion shows that 10 ETH was sent to juicebox.money, while the remaining 4,520.2 ETH was deposited into the mixing service Tornado Cash (an analysis of Tornado Cash will be provided later).



### (3) Community Tools

Well-known cryptocurrency investigator [ZachXBT](#) has publicly shared his commonly used tools for on-chain analysis and open-source intelligence (OSINT) investigations:

- Cielo - Wallet tracking (EVM, Bitcoin, Solana, TRON, etc.)
- TRM - Create graphs for addresses/transactions
- MetaSuites - Chrome extension that adds additional data on block explorers
- OSINT Industries - email/username/phone lookups
- LeakPeek - db lookups
- Snusbase - db lookups
- Intelx - db lookups
- Spur - IP lookups
- Cavalier (Hudson Rock) - Infostealer lookups
- Impersonator - Chrome extension to spoof login to dApps
- MetaSleuth - Similar to TRM but intended for retail users
- Arkham - Multichain block explorer, entity labels, create graphs, alerts

- Obsidian - Create flow charts / diagrams
- Wayback Machine - archive web pages
- Archive Today - archive web pages
- Etherscan / Solscan - block explorer for EVM / Solana
- Blockchair - bitcoin block explorer
- Range - CCTP bridge explorer
- Pulsy - bridge explorer aggregator
- Socketscan - EVM bridge explorer
- Dune - Analytics platform to query blockchain data
- Mugetsu - X/Twitter username history & meme coin lookups
- TelegramDB Search Bot - Basic Telegram OSINT
- Discord\[\.\\]ID - Basic Discord account info
- CryptoTaxCalculator - Track PNL for an address

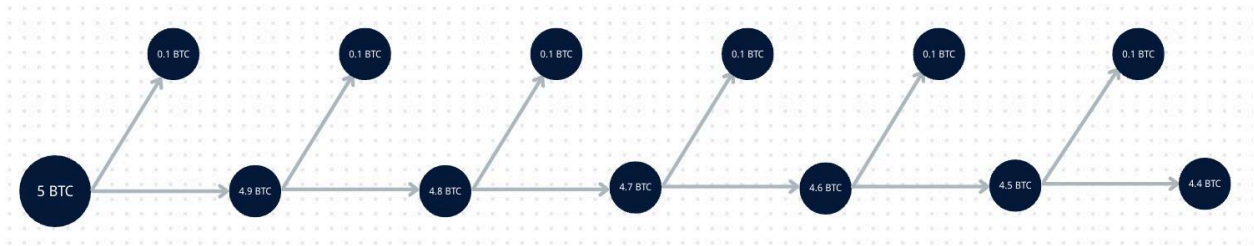
In the next section, we will explore common fund movement patterns, laying the groundwork for behavioral analysis in tracing paths.

### 3. Common Fund Movement Patterns

In cryptocurrency asset tracking, understanding the “transfer playbook” of attackers or scammers is a crucial step in determining transaction paths. Although fund movements on-chain may appear to be a series of simple address-to-address transfers, they often follow certain patterns or “behavior templates.” This section summarizes several common fund movement methods to help you quickly identify “non-standard” behavior in practical investigations.

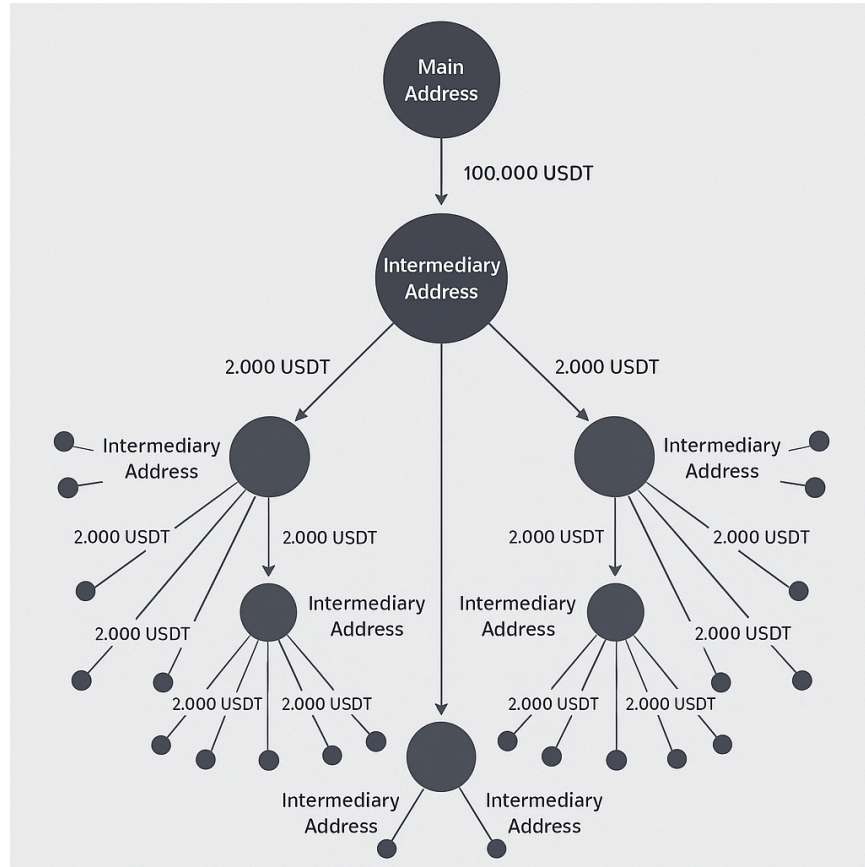
#### (1) Peel Chain

A Peel Chain refers to a laundering technique in which large amounts of cryptocurrency are split into a long series of small transactions. This pattern is common in blockchain analysis. It typically starts from a “dirty” address linked to illicit activity. For example, Address A sends funds to Addresses B and C, with the transfer to B being very small while the transfer to C contains most of the value. C then sends a small amount to D and a large amount to E, and so on, until numerous addresses receive tiny amounts of cryptocurrency.



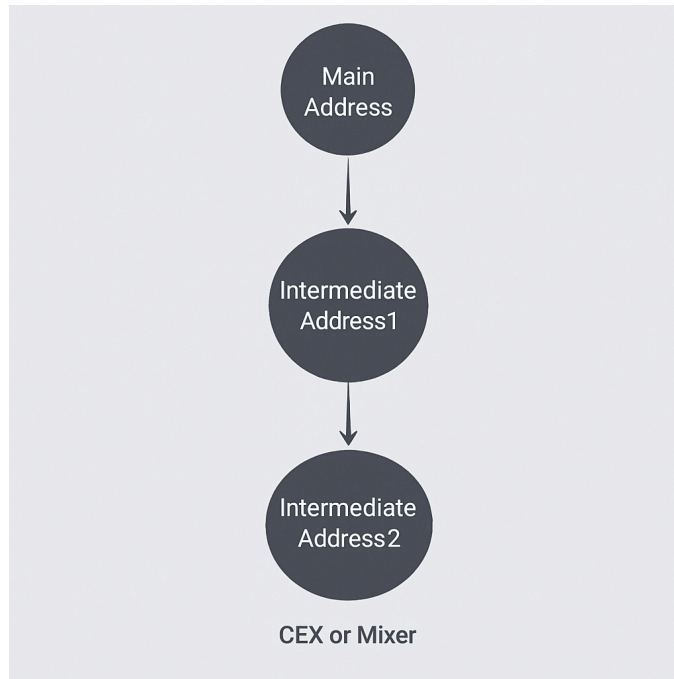
## (2) One-to-Many Distribution

After receiving a large sum, an attacker may transfer the funds from the main wallet to dozens or even hundreds of intermediary addresses. For example, a single transaction worth 100,000 USDT might be split into 50 transfers of roughly 2,000 USDT each, with each address further splitting and sending out funds. This creates a complex “fan-shaped transfer structure” intended to confuse investigators, obscure transaction paths, dilute the original source of funds, delay investigative response time, and avoid having the entire sum frozen at once. On blockchain visualization tools, this appears as a large central address radiating multiple layers of outward fund flows—a classic early-stage laundering pattern.



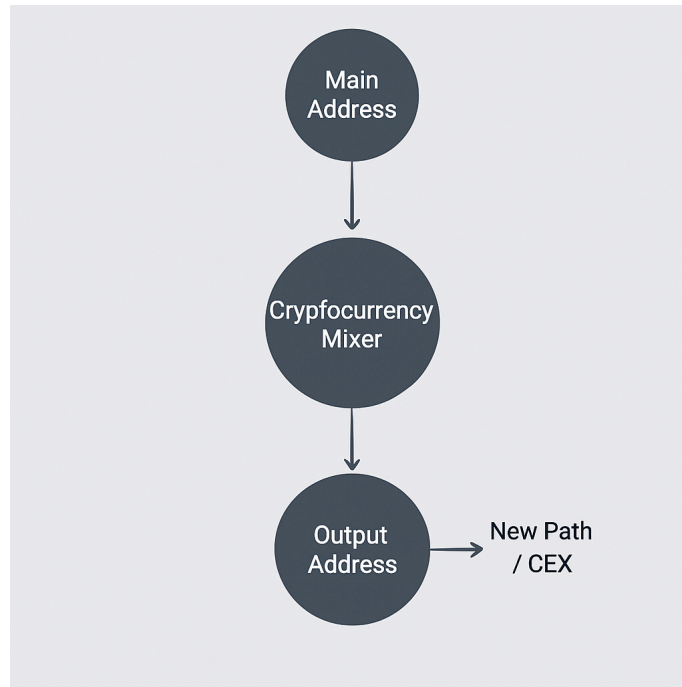
### (3) Multi-Hop Transfers

Attackers often move funds through rapid, multi-hop transfers, where each address is used only once before quickly sending funds onward, and most do not interact with any on-chain dApps. This intermediary structure, by increasing path length and nesting, disrupts behavior-model detection and delays risk-control responses—especially when executed intensively in the first few minutes after an incident, in order to sever the trail before monitoring systems react.



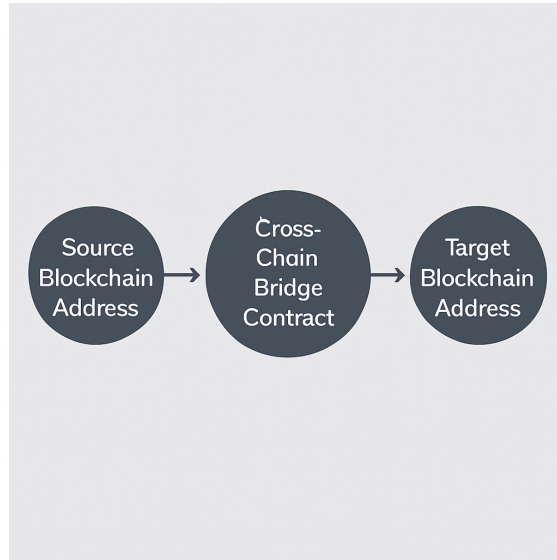
#### (4) Mixer Usage

Mixers are a classic tool for attackers to break on-chain traceability. The principle is to pool funds with those of other users, process them together, and output assets that cannot be directly matched to their original inputs. Common protocols include Tornado Cash and Wasabi. Mixer transactions often follow standardized patterns, such as uniform deposit sizes, specific waiting times, and synchronized withdrawals. If an address exhibits such characteristics, it is reasonable to suspect laundering activity. Mixers typically obscure paths by using uniform entry points, delayed outputs, and fragmented withdrawals, making “fund in” and “fund out” relationships visually unlinked. When combined with privacy coins (such as XMR) or other anonymity protocols, tracking becomes significantly more difficult.



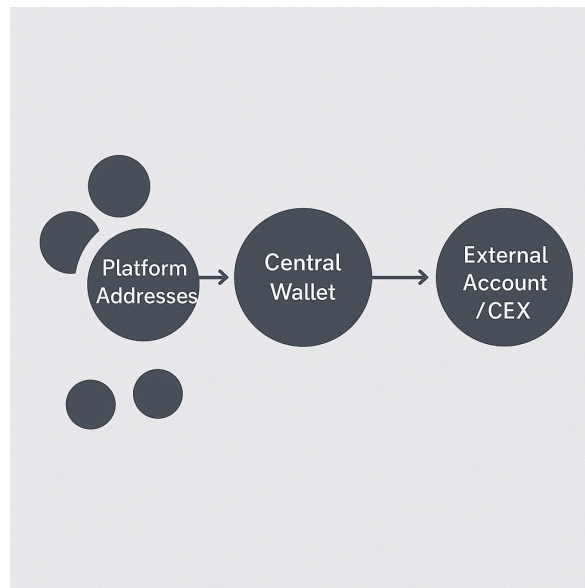
## (5) Cross-Chain Bridge Hops

To evade monitoring and tracing on a given blockchain, attackers may use cross-chain bridges to transfer assets to another network before continuing the movement. Common bridges include THORChain, LayerZero, and Across, with target chains often being networks with weaker investigative coverage (such as TRON). These cross-chain transfers often occur shortly after the attack, and the process may involve asset token changes, path interruptions, and reconstruction of destination addresses, further increasing the difficulty of tracing.



### (6) Many-to-One Consolidation

In Ponzi schemes or rug-pull events, attackers often consolidate victim assets into one or a few “core wallets” within a short time, and then use those addresses to execute cross-chain transfers, mixer deposits, or withdrawals. This behavior often occurs when early signs of collapse emerge, representing an emergency asset transfer. In transaction paths, this produces clear consolidation peaks.





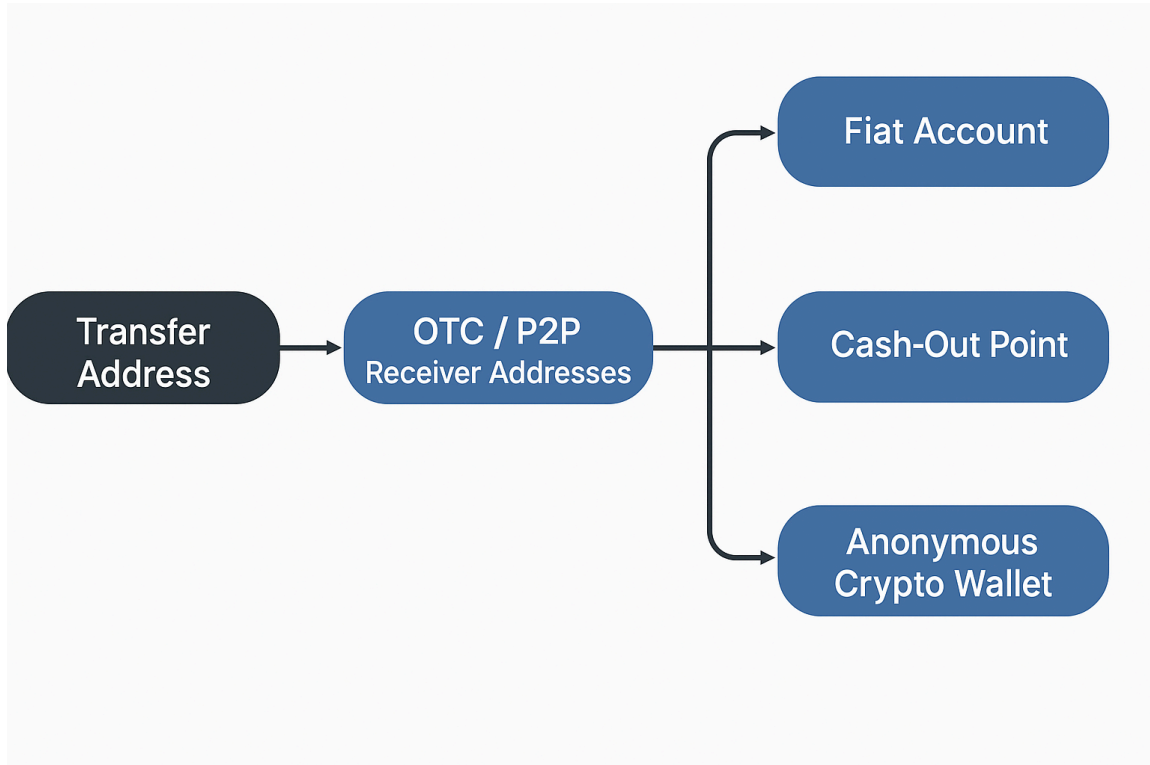
## (7) P2P / OTC

After obscuring the origin of illicit assets via mixers, cross-chain bridges, or fragmented transfers, attackers may turn to P2P platforms, OTC brokers, or offshore non-KYC exchanges to perform “off-chain” operations—converting cryptocurrency into fiat currency or privacy coins. For example, Huione Guarantee, a Southeast Asia–centered escrow platform, is frequently used for this purpose. This process often relies on off-chain deals and identity-masking methods, further breaking the link between on-chain funds and real-world identities.

P2P platforms allow direct user-to-user trades between cryptocurrency and fiat. Examples include Paxful, Bitquick, and LocalBitcoins (now defunct). Attackers can match with other users and accept bank transfers, Alipay/WeChat Pay, PayPal, or even gift cards as payment, using rented accounts or fake identity documents to evade controls. Such off-chain payments often lack robust identity verification, making post-transaction tracing extremely difficult.

OTC (Over-The-Counter) trading involves large off-chain cryptocurrency transactions via intermediaries, often conducted over Telegram, Discord, or similar platforms. Many OTC brokers do not check the source of funds or require KYC from either party, providing attackers with an “anonymous, fast, unregulated” cash-out channel. Some OTC intermediaries maintain laundering networks, payment account resources, or even their own gray-market platforms, offering “one-stop cash-out” services.

If immediate off-ramping is not possible, illicit funds may be routed into small exchanges in loosely regulated jurisdictions—such as certain Caribbean, African, or Eastern European platforms—with weak KYC/AML policies, completing the final conversion. Eventually, the funds may be withdrawn via third-party payment processors, underground banking systems, e-commerce accounts, or converted into privacy coins like Monero or Zcash for long-term hiding, making on-chain tracing and law enforcement action significantly more difficult.



While these patterns are common, it’s important to note that attackers continuously adapt their techniques. A single fund path may combine multiple strategies—for example, “splitting + cross-chain + mixing + reconsolidation”—which is the non-linear complexity seen in most real-world cases. Understanding fund movement patterns is therefore not just about memorizing playbooks, but about recognizing the intent behind the transaction structure: Is it to evade detection? To cash out? To launder and reuse assets? Only by answering such questions can tracing efforts get closer to the truth.

Next, we will move to the practical aspect: what to do immediately if you or your friend become a victim.

## 4. What to Do If You Get Hacked

The [Blockchain Dark Forest Selfguard Handbook](#) notes that “being hacked is a matter of when, not if.” With scams and attacks becoming increasingly rampant, individual users, project teams,

and community operators can hardly stay unaffected. So, when assets are actually stolen, what should you do?

## (1) Prioritize Loss Prevention

Once you notice abnormal asset movement, “loss prevention” should always be the top priority, generally in two stages:

### **Stage 1: Emergency Loss Prevention**

- If the attack is ongoing (e.g., the hacker is still transferring funds), immediately move remaining assets to a secure wallet, or attempt “front-running” transactions to minimize losses.
- Check if you hold assets that support freezing functions (e.g., USDT, USDC) and, if applicable, contact the issuer to request freezing.
- If stolen funds have entered a centralized exchange (CEX), quickly collect transaction hashes, timestamps, and addresses, and submit a freeze request to the platform. Note that most exchanges will not freeze an address immediately based on individual complaints.
- Users with technical capability can also track the hacker’s path using on-chain analysis tools (e.g., MistTrack) to identify fund flows.
- If your wallet assets cannot be transferred, it may be due to malicious multisig or replaced/limited signing permissions. Use blockchain explorers or security tools to verify whether permissions now belong to unknown addresses. For more on malicious multisig risks, refer to the relevant [resources](#).

### **Stage 2: Prevent Further Damage**

- Check associated wallets and mnemonic phrases for additional risks.
- Review token approvals and revoke suspicious ones using tools like [Revoke.cash](#).
- Change all related account passwords and enable multi-factor authentication (MFA) to prevent further cross-platform intrusion.
- Block potential re-entry points that hackers could exploit, including browser extensions, desktop wallets, and GitHub projects.

- Be aware of “fake customer service” or “asset recovery” scams post-theft, and do not trust unsolicited contacts.

## (2) Preserve the Scene

A common instinct is to panic, reinstall systems, or delete files, which may destroy crucial evidence. What you need is:

- Calmly disconnect from the Internet, keep the computer powered on, and preserve the original environment. Do not shut down or delete any files immediately—maintain the scene as it is for professionals to collect evidence.
- Record and retain all relevant evidence. For example, if the phishing occurred via Telegram, email, or a website, save the Telegram group chat, usernames, email IP addresses, links, and the original email content.
- If the case involves the promotion of a fraudulent platform, retain original materials such as screenshots of KOL posts, content from the official website, and any local documents.

## (3) Conduct Preliminary Analysis

Even if you are not an expert in blockchain analysis, you can still make basic judgments using blockchain explorers and some simple tools:

- Input your address into a blockchain explorer to observe fund flows.
- Use MistTrack to trace on-chain paths and identify if assets were mixed, bridged, or moved into centralized exchanges.
- Check address profiling on MistTrack to see if it is flagged as high-risk or associated with scams.
- Export reports via MistTrack to get an overview of fund flows even as a non-professional.
- Submit hacker addresses to platforms like MistTrack to help prevent others from being scammed.

#### (4) Contact Professional Agencies

For large amounts or complex cases, it's advisable to contact professional security firms promptly:

- Conduct on-chain analysis and full path tracing, and profile the hacker.
- Assess whether assets can still be frozen and coordinate emergency freezes with exchanges (where possible).
- Provide “on-chain messaging” services to communicate with hackers or apply pressure (e.g., leaving messages on Etherscan).
- Generate tracking reports for investigative or reporting purposes.

On-chain messages have repeatedly succeeded in prompting hackers to return assets. Reference implementations exist on:

- [Ethereum](#)
- [Bitcoin](#)

#### (5) File a Police Report and Seek Legal Assistance Early

Even if you can track hacker addresses and fund flows precisely, judicial enforcement is ultimately needed for freezing and recovery:

- File a report with local authorities.
- Prepare detailed materials and reports, including transaction records, chat screenshots, timelines, and loss amounts.
- If cross-border funds involve overseas exchanges, contact law firms to prepare international assistance documentation.
- Multiple victims can consider collective reporting to increase chances of successful case registration and cooperation.

## (6) Ongoing Follow-up and Profiling

According to “Roca’s Law” (“where there is intrusion, traces will remain”), hackers often leave clues both on-chain and off-chain. Continuously building a “hacker profile” can aid subsequent investigations:

- On-chain clues: transaction paths, receiving addresses, mixing behavior, cross-chain bridges.
- Off-chain clues: email registrations, Telegram IDs, IP addresses, device fingerprints.
- Social links: connections to known scammers or rug-pull groups.

## (7) Tokens Eligible for Freezing

Some tokens with official freezing mechanisms include:

- USDT (issuer: Tether)
- USDC (issuer: Circle)
- MERL (issuer: Merlin Chain)
- BUSD (issuer: Paxos)
- TUSD (issuer: TrustToken)
- PAX (issuer: Paxos)
- GUSD (issuer: Gemini)

...

These tokens are typically issued centrally, with smart contracts containing “blacklist” or freeze functionalities. These powers are generally used to comply with legal requirements, combat fraud, money laundering, or other illegal activities. If your stolen assets include these tokens, request a freeze as soon as possible before they flow into non-regulated platforms or mixing protocols. Early response, evidence preservation, and analysis greatly increase the chance of intercepting funds and recovering losses.

The next section will dive deeper into tracing — identifying mixing activity, cross-chain paths, complex laundering networks, and reviewing multiple case studies.

## 5. Cross-chain Bridge Tracking Analysis

### (1) Introduction to Bridges

With the growth of the multi-chain ecosystem, the demand to move assets from one blockchain to another has increased. Cross-chain bridges have emerged as critical infrastructure, connecting assets and data across different chains. Their core function is to allow users to lock assets on one chain and obtain equivalent assets on another chain in the form of Wrapped Tokens, or directly release native assets. Attackers frequently exploit bridges to perform “on-chain jumps,” evading tracking tools and analysis on the source chain.

Major Types of Bridges:

#### **Decentralized Verification Bridges**

- Characteristics: Do not rely on centralized entities. They typically use light clients or zero-knowledge proofs to validate the state of the target chain. Security aligns with the target chain, providing strong resistance to attacks.
- Representative Projects: LayerZero, zkBridge
- Risks: High complexity, high verification costs, and performance requirements.

#### **Relayer / Observer Bridges**

- Characteristics: A set of third-party nodes observes on-chain events and relays data to the target chain. Lighter than fully decentralized bridges, but trust assumptions are required.
- Representative Projects: Wormhole, deBridge, Axelar
- Risks: Security depends on the number and honesty of relayer nodes; malicious activity by a small number of nodes is possible.

#### **Multisig / Custodial Bridges**

- Characteristics: Users lock assets in a source-chain smart contract, and the corresponding assets are minted on the target chain after approval by a set of multisig addresses or custodians. Simple structure and flexible deployment.
- Representative Projects: Multichain, Binance Bridge

- Risks: Significant trust dependency; if multisig keys are leaked, all assets can be stolen. Many past bridge hacks (e.g., Ronin, Harmony) fall into this category.

### **Liquidity Pool Bridges**

- Characteristics: Do not lock real assets but rely on on-chain liquidity pools on both sides for swaps, similar to AMM DEXs. Cross-chain behavior is effectively an “exchange” rather than true asset transfer.
- Representative Projects: Hop Protocol, THORChain
- Risks: Dependent on liquidity size; pool depletion may cause slippage or failed swaps. AMM price volatility can trigger arbitrage or losses.

### **Native Bridges**

- Characteristics: Maintained directly by the base blockchain or its core development team, common between an L1 and its L2/sidechains. Security is tied to the protocol layer, usually the most reliable.
- Representative Projects: Arbitrum Bridge, Polygon PoS Bridge, Near Rainbow Bridge
- Risks: Technical issues or failed upgrades may temporarily disable the bridge. Typically slower, not suitable for high-frequency trading.

Traditional on-chain tracking assumes a transparent single-chain logic: one address sends to another, and subsequent outflows can be traced. Once cross-chain activity occurs, there is no direct record linking the “outflow” on the source chain to the “inflow” on the target chain. Even if it is known that funds were “moved across chains,” it is difficult to determine where they landed, who received them, or how they are being used.

Additionally, many cross-chain protocols are not fully open-source on-chain. Transaction records may reside in Layer 2 logs, Rollup events, or non-standard contract calls. Cross-chain transfers are therefore not simple “transactions” but rather “burn-and-mint” or “lock-and-release” operations. On the blockchain, this creates a visible “gap” in fund flow: funds no longer continue on the source chain but “appear” on another chain. Attackers exploit this opacity to create obfuscated transfer paths, forming complex combinations such as “cross-chain + dispersal + mixing.”



## (2) Bridge Analysis

In crypto asset tracking, “cross-chain” activity has become a standard tactic for fund laundering. However, bridges are not entirely “black boxes.” We can still track cross-chain movements using the following methods:

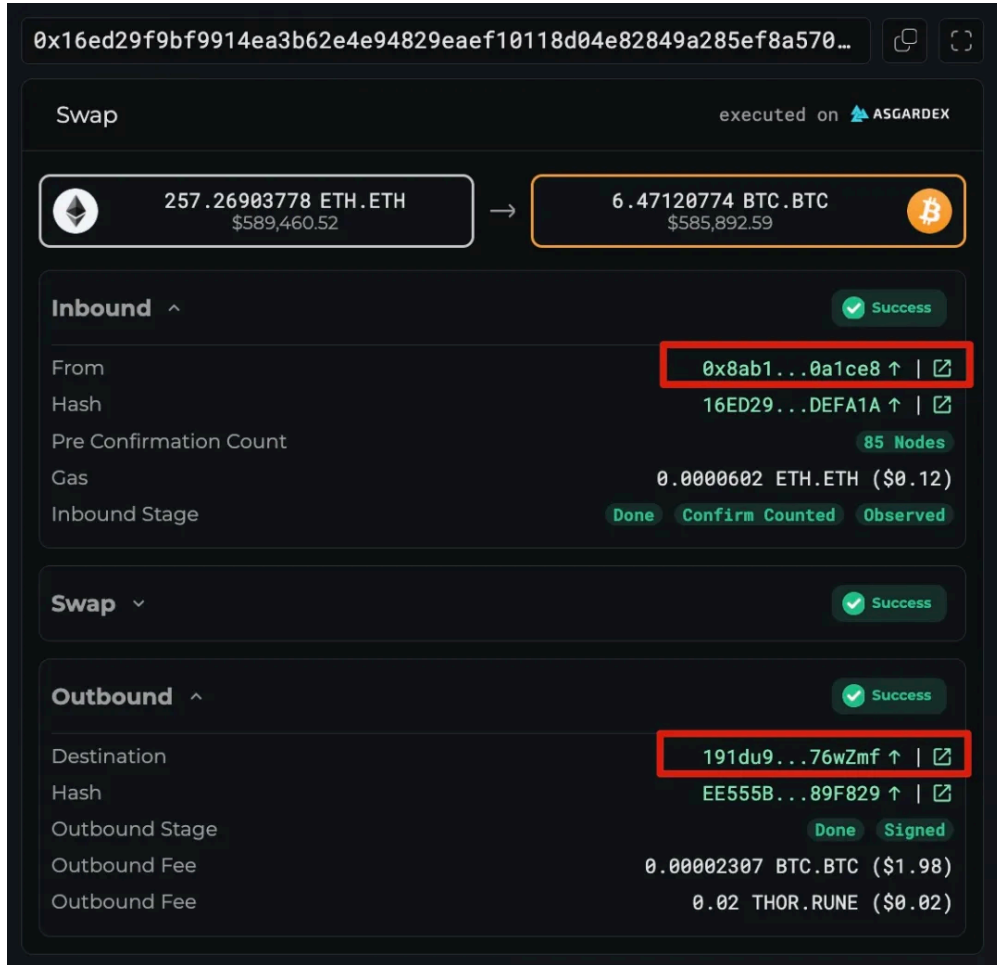
### Method 1: Bridge Explorer

The simplest and most direct approach is to check whether the bridge provides an Explorer. For example, in the Bybit hack case, the attacker’s intermediary address [0x8ab1d1d3e7db399835172576cce0bd1c200a1ce8](https://etherscan.io/address/0x8ab1d1d3e7db399835172576cce0bd1c200a1ce8) sent the received funds through THORChain, which ultimately flowed to a BTC address.

Latest 2 from a total of 2 transactions Download Page Data

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Txn Fee
<a href="#">0x16ed29f9b9...</a>	Deposit With ...	21967334	2025-03-03 15:44:47	<a href="#">0x8Ab1D1d3...C200a1Ce8</a>	OUT THORChain: THOR...	257.26903778 ETH	0.00006019
<a href="#">0x3463e5c003...</a>	Transfer	21967325	2025-03-03 15:42:59	<a href="#">0x6591c653...b4FA3e3ab</a>	IN <a href="#">0x8Ab1D1d3...C200a1Ce8</a>	257.26918276 ETH	0.00004914

By inputting the cross-chain transaction [hash](#) in THORChain’s Explorer, you can clearly see the token type, amount, and receiving address after the bridge transaction.



Common Bridge Explorers:

Chain	Bridge	Explorer
Solana	Wormhole	<a href="https://wormholescan.io">https://wormholescan.io</a>
Solana	Mayan	<a href="https://explorer.mayan.finance">https://explorer.mayan.finance</a>
EVM	Symbiosis	<a href="https://explorer.symbiosis.finance/transactions">https://explorer.symbiosis.finance/transactions</a>
EVM	Synapse	<a href="https://explorer.synapseprotocol.com">https://explorer.synapseprotocol.com</a>
EVM / BTC	Chainflip	<a href="https://scan.chainflip.io/">https://scan.chainflip.io/</a>

EVM	Socket	<a href="https://www.socketscan.io/">https://www.socketscan.io/</a>
EVM / Tron	Bridgers / SwftSwap	<a href="https://explorer.bridgers.xyz/">https://explorer.bridgers.xyz/</a> <a href="https://explorer.allchainbridge.com/">https://explorer.allchainbridge.com/</a>
EVM	Range	<a href="https://explorer.rango.exchange">https://explorer.rango.exchange</a>
MultiChain	THORChain	<a href="https://viewblock.io/thorchain/">https://viewblock.io/thorchain/</a>
EVM	PolyNetwork	<a href="https://explorer.poly.network">https://explorer.poly.network</a>
EVM	Wanchain	<a href="https://www.wanscan.org">https://www.wanscan.org</a>
EVM / Solana	LI.FI	<a href="https://scan.li.fi">https://scan.li.fi</a>
EVM / Solana	deBridge	<a href="https://app.debridge.finance/explorer">https://app.debridge.finance/explorer</a>
EVM	Stargate	<a href="https://layerzeroscan.com">https://layerzeroscan.com</a>
EVM	Layerswap	<a href="https://layerswap.io/explorer">https://layerswap.io/explorer</a>
	Circle CCTP Bridge	<a href="https://usdc.range.org/usdc">https://usdc.range.org/usdc</a>
	CowSwap	<a href="https://explorer.cow.fi">https://explorer.cow.fi</a>

## Method 2: Blockchain Explorer Analysis

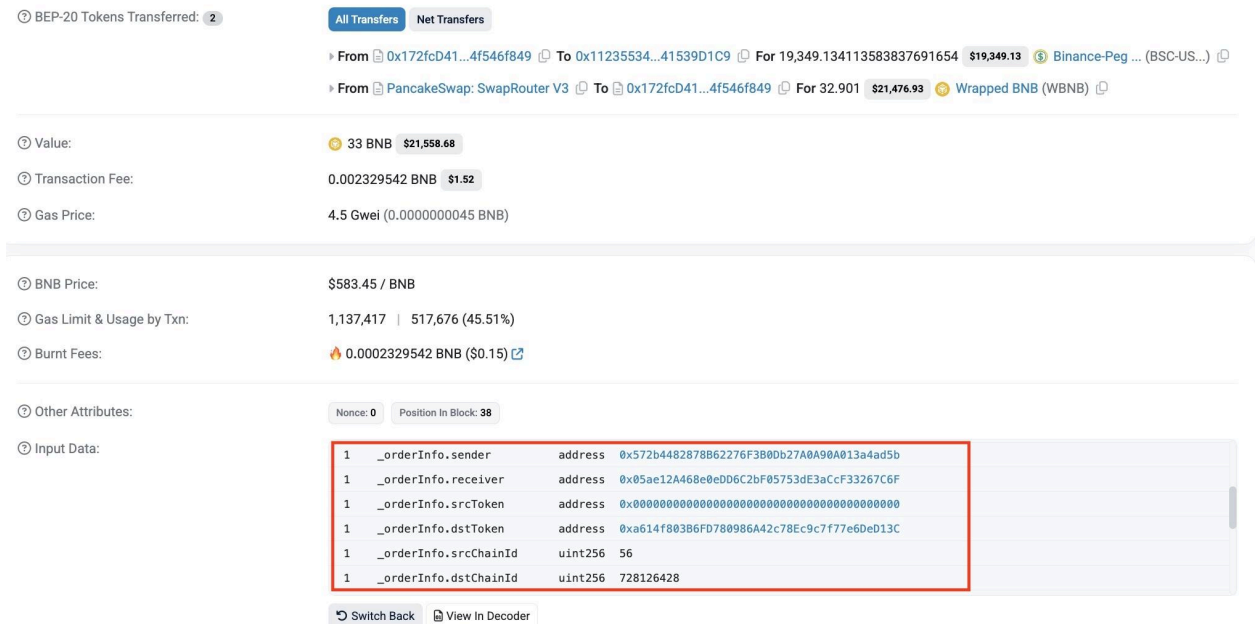
If the bridge does not provide an Explorer, you can use standard blockchain explorers to track cross-chain transfers. For instance, the BSC address

[0x572b4482878B62276F3B0Db27A0A90A013a4ad5b](https://bscscan.com/address/0x572b4482878B62276F3B0Db27A0A90A013a4ad5b) sent 100 BNB through Bitget Swap across three cross-chain transactions.

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount
<a href="#">0xf437dfb6bc6...</a>	Transfer	37366493	2024-03-28 14:36:32	<a href="#">0x572b4482...013a4ad5b</a>	<a href="#">0x37607F2c...85a1aBAD3</a>	0.00410697 BNB
<a href="#">0xcef23d00bd5...</a>	Send V1	37357556	2024-03-28 7:09:00	<a href="#">0x572b4482...013a4ad5b</a>	Bitget Wallet: Swa...	33.59 BNB
<a href="#">0x15f5abe059f...</a>	Send V1	37357537	2024-03-28 7:08:03	<a href="#">0x572b4482...013a4ad5b</a>	Bitget Wallet: Swa...	33.4 BNB
<a href="#">0x70faf9cd3e2...</a>	Transfer	37357523	2024-03-28 7:07:21	<a href="#">0x7E98982d...11cef2783</a>	<a href="#">0x572b4482...013a4ad5b</a>	0.000001 BNB
<a href="#">0x5c22b19097...</a>	Send V1	37357516	2024-03-28 7:07:00	<a href="#">0x572b4482...013a4ad5b</a>	Bitget Wallet: Swa...	33 BNB
<a href="#">0x3a503cbb1...</a>	Transfer	37357497	2024-03-28 7:06:03	<a href="#">0x7E982212...928717483</a>	<a href="#">0x572b4482...013a4ad5b</a>	100 BNB

Since Bitget Swap lacks an Explorer, blockchain explorers can help trace the transactions.

Take the earliest cross-chain transaction [0x5c22b1...7e3a64](#) as an example. Using a blockchain explorer (such as BscScan), click Decode Input Data to view and obtain the parsed information:



The screenshot shows a transaction summary with the following details:

- Value:** 33 BNB (\$21,558.68)
- Transaction Fee:** 0.002329542 BNB (\$1.52)
- Gas Price:** 4.5 Gwei (0.0000000045 BNB)
- BNB Price:** \$583.45 / BNB
- Gas Limit & Usage by Txn:** 1,137,417 | 517,676 (45.51%)
- Burnt Fees:** 0.0002329542 BNB (\$0.15)

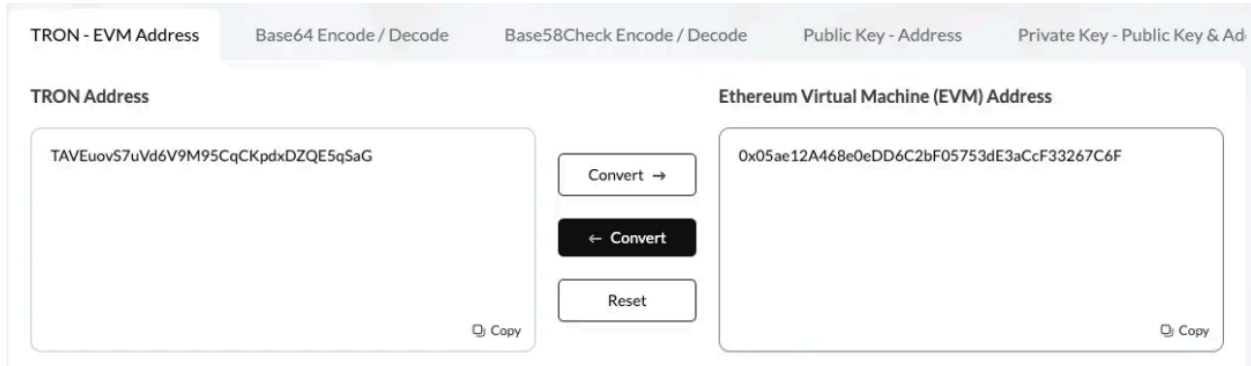
Under "Input Data", the decoded information is as follows:

Index	Field	Type	Value
1	_orderInfo.sender	address	0x572b4482878B62276F3B0Db27A0A9A013a4ad5b
1	_orderInfo.receiver	address	0x05ae12A468e0eDD6C2bF05753dE3aCcF33267C6F
1	_orderInfo.srcToken	address	0x00
1	_orderInfo.dstToken	address	0xa614f803B6FD780986A42c78Ec9c7f77e6DeD13C
1	_orderInfo.srcChainId	uint256	56
1	_orderInfo.dstChainId	uint256	728126428

Key points to note:

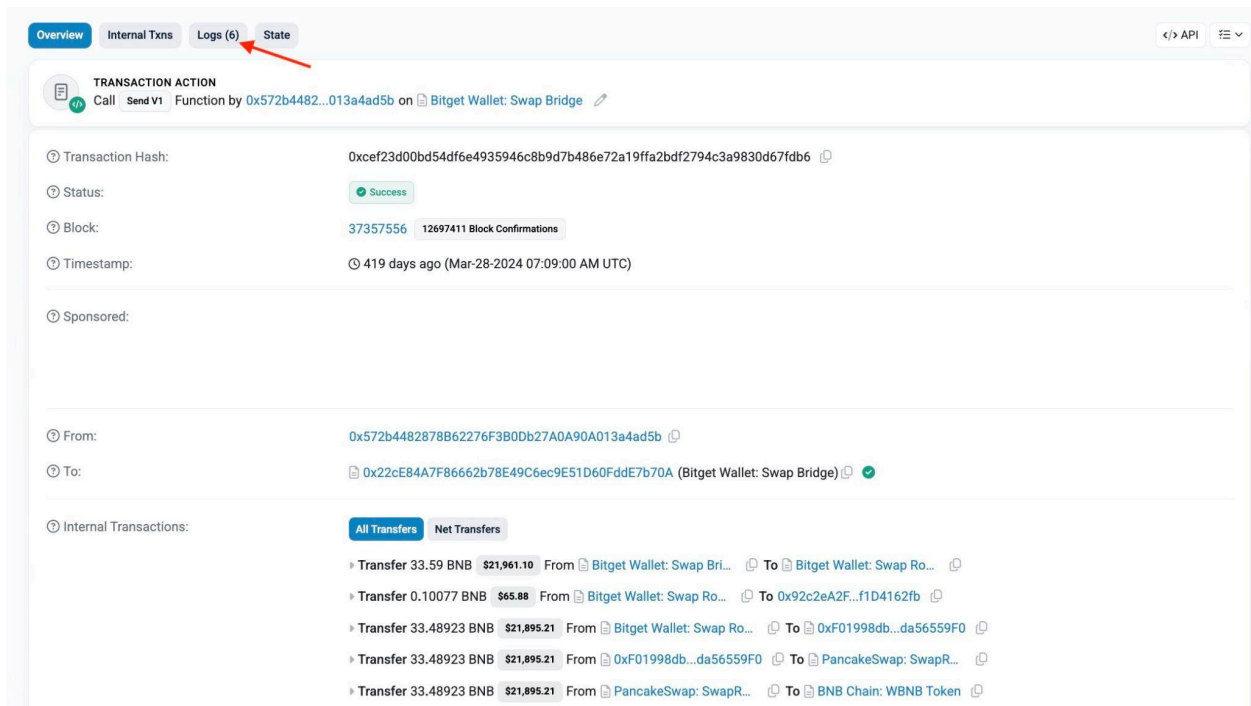
- receiver: The receiving address after the cross-chain transfer.
- dstChainId: The destination chain of the cross-chain transaction.

For example, the dstChainId in this transaction is 728126428, representing the TRON chain, meaning a cross-chain transaction from BSC to TRON. Note that the receiver (0x05ae12A468e0eDD6C2bF05753dE3aCcF33267C6F) is an EVM address and needs to be converted to a TRON address using a [tool](#):



The converted TRON address is TAVEuovS7uVd6V9M95CqCKpdxDZQE5qSaG, which is the receiving address after cross-chain.

In addition, you can also check via Logs. For example, take the latest cross-chain transaction by timestamp, [0xcef23d...67fdb6](#):



Click Logs and find the last event record - BKBridge:

**Address** `0x22ce84a7f86662b78e49c6ec9e51d60fde7b70a` (Bitget Wallet: Swap Bridge) 🔗 🔍

BKBridge (index\_topic\_1 uint256 orderStatus, index\_topic\_2 bytes32 transferId, address vaultReceiver, address sender, address receiver, address srcToken, address dstToken, uint256 srcChainId, uint256 dstChainId, uint256 amount, uint256 timestamp) View Source

**Name** timestamp

**Topics**

- 0 0x8ef23af58b418171e290a5dc439b3323c6ffe2261498014cd0d2a8152d93057b
- 1: orderStatus Dec → 1
- 2: transferId Dec → 637F01954000D386DEFD6424AF9CEDD2EA58F9A691A98268BAE52D6BC494F9A

**Data**

```

vaultReceiver : 0x11235534a66A33c366b84933D5202c841539D1C9
sender : 0x572b4482878B62276F3B0Db27A0A90A013a4ad5b
receiver : 0x05ae12A468e0eDD6C2bF05753dE3aCcF33267C6F
srcToken : 0x0000000000000000000000000000000000000000000000000000000000000000
dstToken : 0xa614f803B6FD780986A42c78Ec9c7f77e6DeD13C
srcChainId : 56
dstChainId : 728126428
amount : 19655901190916552090914
timestamp : 1711609734
    
```

Dec Hex

Similarly, using the same method, we find that the cross-chain destination address is the TRON address TAVEuovS7uVd6V9M95CqCKpdxDZQE5qSaG.

### Method 3: MistTrack Cross-chain Parsing

For more efficient parsing of multiple cross-chain activities, you can use MistTrack’s cross-chain transaction parsing feature. For example, take the ETH address [0x4e398288d0b7514fcc1a109f4687cffa80d01a94](https://etherscan.io/address/0x4e398288d0b7514fcc1a109f4687cffa80d01a94). This address received 85,245.5199 USDC and performed two cross-chain transfers via Across Protocol.

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Txn Fee
<a href="#">0 added833d18e9...</a>	Transfer	20327987	2024-07-17 18:18:11	0x4E398288...a80D01a94	OUT 0xDd8906cD...590BcEA96	0.01500625 ETH	0.00023269
<a href="#">0x55199339fde...</a>	Deposit V3	20326255	2024-07-17 12:29:35	0x4E398288...a80D01a94	OUT Across Protocol: E...	0 ETH	0.00064197
<a href="#">0x7b101fd40c9...</a>	Deposit V3	20326237	2024-07-17 12:25:59	0x4E398288...a80D01a94	OUT Across Protocol: E...	0 ETH	0.00068531
<a href="#">0xe43327bf205...</a>	Approve	20326235	2024-07-17 12:25:35	0x4E398288...a80D01a94	OUT Circle: USDC Token	0 ETH	0.00043659
<a href="#">0x9772cd2c23...</a>	Uniswap V3S...	20326212	2024-07-17 12:20:59	0x4E398288...a80D01a94	OUT 0xF3dE3C0d...172509127	24.65279699 ETH	0.00121977
<a href="#">0x532c8b9f9b...</a>	Transfer	20326202	2024-07-17 12:18:59	0xB778BbFF...21aa50a6E	IN 0x4E398288...a80D01a94	24.67112043 ETH	0.00021

In the MistTrack Standard Plan, right-click on Across Protocol: Ethereum Pool and select Cross-chain Parsing to quickly obtain the post-swap assets and the receiving addresses across chains for the two transactions.

Example:

36,742.5199 USDC-ERC20

→ 36,738.6996 USDC-Base

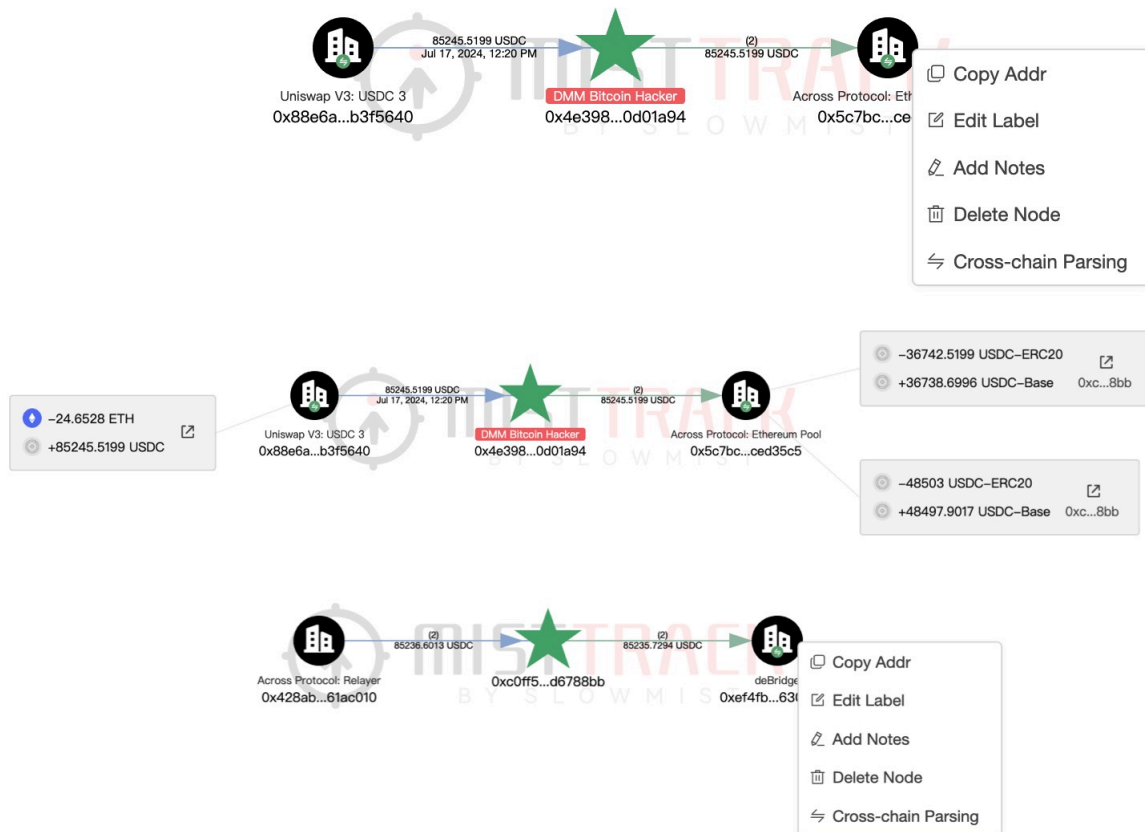
→ Base address 0xc0Ff58cf15E4F07f8210Cc44b43bE7121d6788bb

48,503 USDC-ERC20

→ 48,497.9 USDC-Base

→ Base address 0xc0Ff58cf15E4F07f8210Cc44b43bE7121d6788bb

By clicking on a parsed address, you can directly access its detail page to further analyze the fund flows after the cross-chain transaction. For example, from the chart below, you can see that the cross-chain address used deBridge for another cross-chain transfer. The method for further analysis is similar.



In addition, as shown in the figure above, the source of the address 0x4e398288d0b7514fcc1a109f4687cffa80d01a94 is Uniswap. We can use a similar method: right-click on “Uniswap V3: USDC 3” and select “DEX Parsing” to quickly obtain the post-swap details of this transaction.

In summary, the three methods described above can be used in combination, which is sufficient to cover the analysis of most cross-chain bridges.

## 6. Privacy Tool Tracking Analysis

### (1) Introduction to Mixers

In numerous on-chain security incidents, it is common to see stolen assets quickly funneled into a special type of tool—mixers. These tools are originally designed to enhance transaction privacy. Essentially, they pool assets from multiple users, deduct a small service fee, and then return equivalent assets from the pool to each user, breaking the direct mapping between transaction inputs and outputs and thereby achieving transaction privacy. In recent years, mixers have been widely misused to obscure the source of illicit assets, making them one of the most challenging nodes in on-chain asset tracking.

#### Smart Contract Mixers

- Characteristics: Fully operate on the blockchain and implement “mixing” via contract logic. Users send funds to the mixer and receive a “cryptographic note” proving their deposit. The system waits for multiple users to participate, then randomly splits and reassembles outputs. Users can redeem the note at any time to withdraw funds to a new address. These mixers run on-chain and are transparent in operation, but due to strong encryption and anonymity mechanisms, tracking fund flows is extremely difficult.
- Representative projects:
  - Tornado Cash: Based on zk-SNARK zero-knowledge proofs, sanctioned by the U.S. OFAC.
  - zkSend / Railgun: New privacy protocols combining zero-knowledge encryption with contract control.

#### Centralized Mixers



- Characteristics: Operate on centralized servers. Users send funds to the platform, which manually or automatically mixes and sends the assets to new user addresses. These mixers rely on the operator’s reputation and carry risks such as exit scams, regulatory issues, or non-compliance.
- Representative projects:
  - Helix: Formerly Bestmixer.io, now shut down.
  - ChipMixer: Seized by German authorities.
  - Sinbad Mixer: Successor to Blender.io, sanctioned by OFAC.

### **Collaborative Mixing Protocols (CoinJoin)**

- Characteristics: Multiple participants collaboratively initiate a single transaction, mixing inputs and outputs to obscure transaction relationships. Users typically repeat this process multiple times. Commonly used in the Bitcoin ecosystem, often integrated into privacy wallets.
- Representative projects:
  - Wasabi Wallet: Uses the WabiSabi protocol.
  - Samourai Wallet: Works with the Whirlpool module.
  - JoinMarket: An open mixing protocol allowing users to set participation roles.

### **Privacy Coins**

- Characteristics: Not a mixing “service,” but cryptocurrencies designed to conceal transaction details and ensure user anonymity.
- Representative projects:
  - Monero (XMR): Uses ring signatures, RingCT, and stealth addresses to mix sender inputs with others, providing anonymity for both sender and receiver. It is currently the largest and most widely used privacy coin, often appearing in darknet markets and banned in multiple countries.
  - Zcash (ZEC): Uses zk-SNARK zero-knowledge proofs to validate transactions without revealing information about the sender, receiver, or amount.
  - Dash (DASH): Uses PrivateSend technology to mix transactions with others, thereby obfuscating the source of funds.

## (2) Mixer Analysis

These tools typically make asset “destination invisible” through technical mechanisms: users send funds into a “pool” that contains assets from other users, and then withdraw “equivalent” but not identical funds from the pool, breaking direct transaction links. The transfer records lack on-chain logical connections, creating analysis gaps. However, mixers are not truly “endpoints.” Through a series of technical and analytical methods, we can still gradually deconstruct their operational characteristics, establish “possible paths,” and create conditions for subsequent tracking and attribution.

- Mixer Entry Address Identification: Mixer contract addresses, such as those of Tornado Cash, are publicly accessible. Seeing assets enter these addresses allows for a preliminary determination of mixer usage, or known mixer contracts can be identified using MistTrack.
- Fixed Amount Features: Some mixers only support fixed amounts (e.g., Tornado Cash’s 0.1 / 1 / 10 / 100 ETH), and transaction amounts themselves can serve as clues.
- Analyzing Withdrawal Target Behavior: Although mixers scramble direct paths, the behavior of new addresses after withdrawals can still be analyzed (e.g., using a newly created wallet for a single transaction, remaining dormant for a long period, or funds quickly moving into CEXs, using the same DEX or Bridge, etc.). Behavior patterns can be used to infer whether addresses belong to the same entity.
- Time Correlation Analysis: Multiple addresses depositing or withdrawing from a mixer at the same time may belong to the same group. Time, paths, and beneficiaries can be combined to form address clusters.

First, when observing on-chain mixer behavior, it is important to identify the fund-splitting pattern. For example, Tornado Cash allows deposits in fixed amounts (0.1, 1, 10, 100 ETH), and attackers often split funds according to these standard amounts, then withdraw them in bulk to new addresses. This amount-alignment behavior is highly abnormal on-chain and can serve as a core clue for focusing on suspicious paths.

Second, time-series analysis is crucial. Although mixers scramble the direct mapping between funds and addresses, most attackers, constrained by time costs, will still attempt to launder

assets shortly after an attack. Analyzing deposit-withdrawal behavior within specific time windows and constructing behavior graphs to identify obvious temporal correlations is an important method for building address behavior chains.

Furthermore, some attackers adopt multi-hop mixing or combined obfuscation paths to increase laundering stealth—splitting funds into multiple mixers (even cross-chain) and then withdrawing, using multiple new wallet addresses to recombine funds. Although this “layered laundering” strategy seems thorough, it leaves key traces in the behavior chain, such as:

- Withdrawal addresses quickly aggregating funds again after withdrawal;
- Short-term bursts of transfers or repeated Gas usage patterns between certain addresses;
- A large number of newly created addresses interacting densely with an old address, forming abnormal concentrated paths.

## Case 1: Tornado Cash Analysis

### (1) Background

A project was hacked, and the stolen funds were transferred to Tornado Cash. The project team approached the MistTrack team for assistance. The MistTrack team conducted a withdrawal analysis of Tornado Cash and helped the project team recapture the stolen funds that had been obfuscated by Tornado Cash.

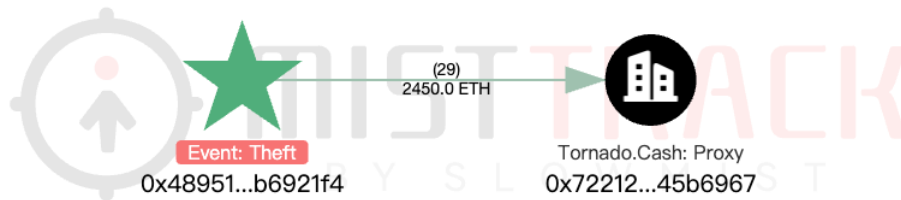
Key roles of MistTrack in this case:

- Establishing mutual trust with the project;
- Tracking stolen funds;
- Analyzing hacker traces;
- Tornado Cash withdrawal analysis;
- Monitoring stolen funds;
- Supporting law enforcement intervention when necessary.

Next, we will detail the MistTrack team's specific work and analysis process in this case.

## (2) Stolen Funds Tracking

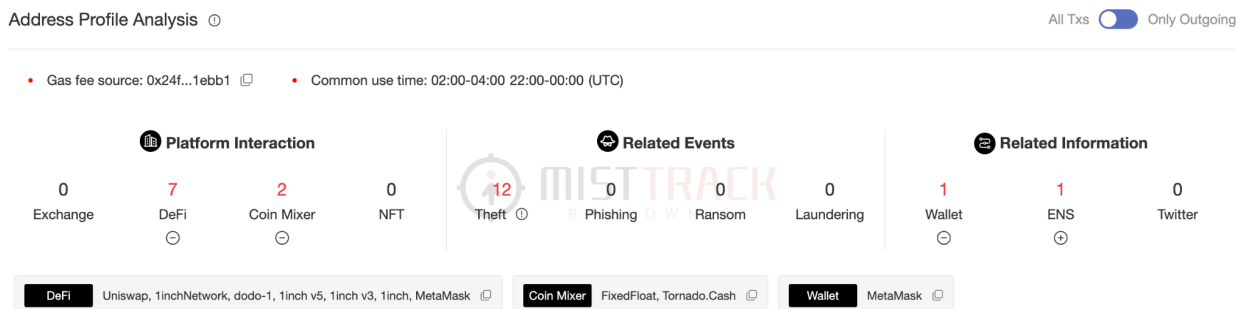
Upon receiving the assistance request, MistTrack immediately began investigation. Analysis showed that the hacker transferred 2,450 ETH into Tornado Cash in batches of 5 x 10 ETH + 24 x 100 ETH.



MistTrack then conducted further analysis of the hacker’s addresses along the workflow:

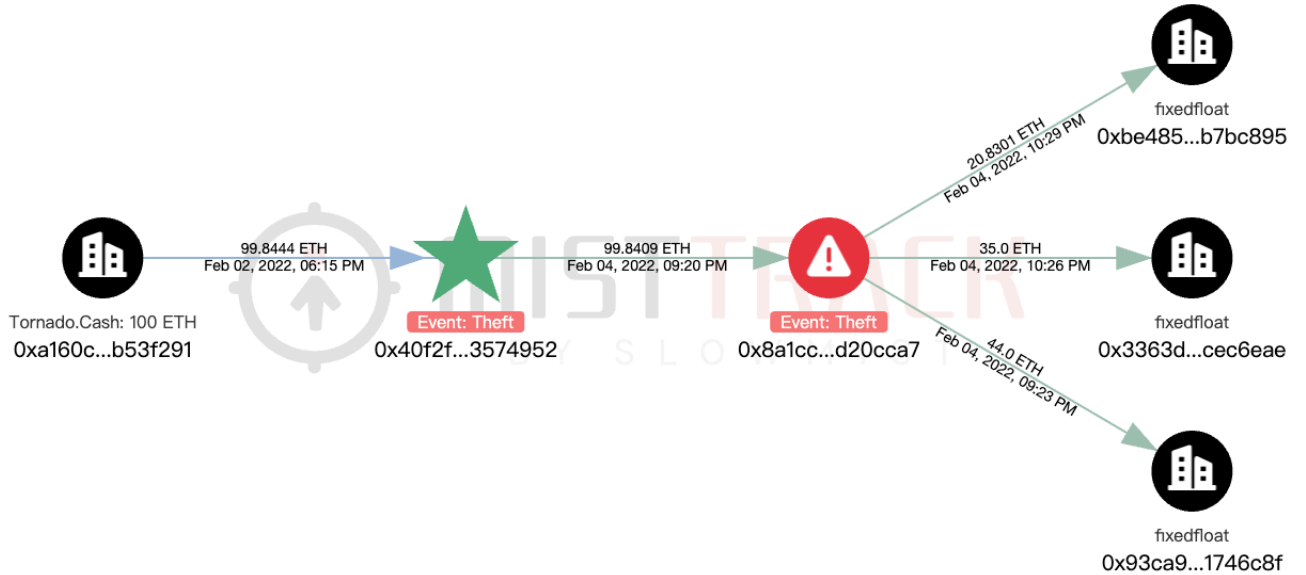
- Fee source tracing
- Tool usage
- Hacker operation timeline
- Hacker profile
- Pre-attack traces

During fund exchange and transfer, the hacker used multiple tools such as Uniswap and 1inch, and also transferred 199 ETH to FixedFloat, which became relevant for subsequent Tornado Cash withdrawal analysis.



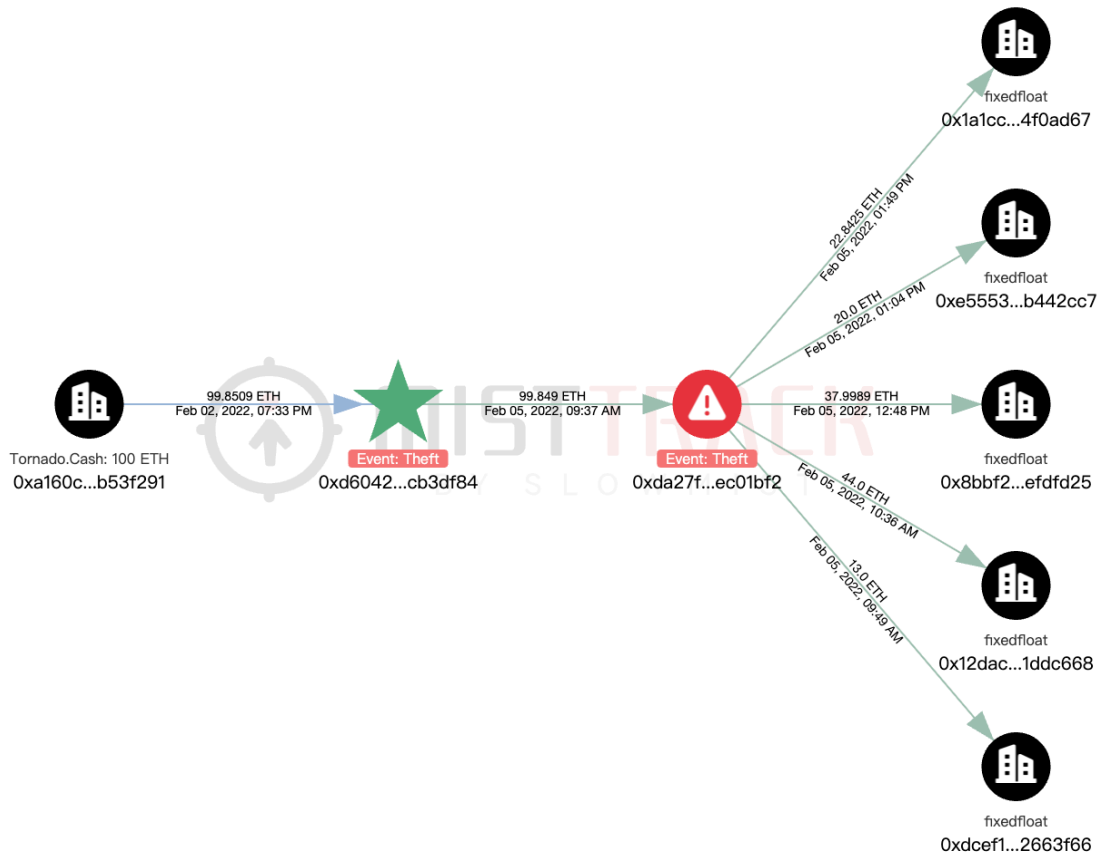
## (3) Tornado Cash Withdrawal Analysis





Of course, this could be a coincidence, and we need to continue to verify it. Further analysis revealed three more addresses with similar characteristics:

- A → B → Multiple FixedFloat addresses
- A → Multiple FixedFloat addresses



In total, 24 addresses matching these characteristics were identified, confirming the hypothesis.

## Case 2: Wasabi Coinjoin Analysis

### (1) Background

A whale’s wallet private key was leaked and the funds were stolen, with the stolen assets moved into Wasabi CoinJoin. The affected user sought assistance from the MistTrack team. MistTrack conducted withdrawal analysis on the stolen funds mixed into Wasabi CoinJoin, successfully tracking and recovering the flow of the funds. Subsequently, the hacker attempted cross-chain transfers. MistTrack identified historical traces of the hacker’s addresses moving funds to exchanges and assisted law enforcement in contacting the exchanges to request evidence and apply risk controls on the relevant accounts. Later, as the hacker further transferred stolen funds to exchange-related accounts, part of the stolen funds was successfully frozen.

Key steps by MistTrack:

- Establish trust: Establish a good trust relationship with the stolen user, which is the basis for analysis and tracking;
- Tracking stolen funds: Tracking the flow of stolen funds through professional technology;
- Analyze hacker behavior: Conduct in-depth analysis of hacker behavior patterns to understand their operations and predict their possible next moves;
- Wasabi Coinjoin Withdrawal Analysis: Utilize analytical tools to study stolen funds mixed into Wasabi Coinjoin;
- Cross-chain tracing: When hackers conduct cross-chain transactions to try to transfer funds, track the flow of funds;
- Law enforcement involvement: If necessary, ask law enforcement to intervene and provide support.

Next, we will detail the MistTrack team's specific work and analysis process in this case.

## (2) Stolen Funds Tracking

Upon request, MistTrack rapidly investigated and found most funds had been moved into Wasabi CoinJoin.



## (3) Wasabi Coinjoin Withdrawal Analysis

The critical breakthrough was analyzing Wasabi CoinJoin withdrawals. MistTrack studied input and output addresses and analyzed intersections across multiple transactions.

Withdrawal addresses were examined for:

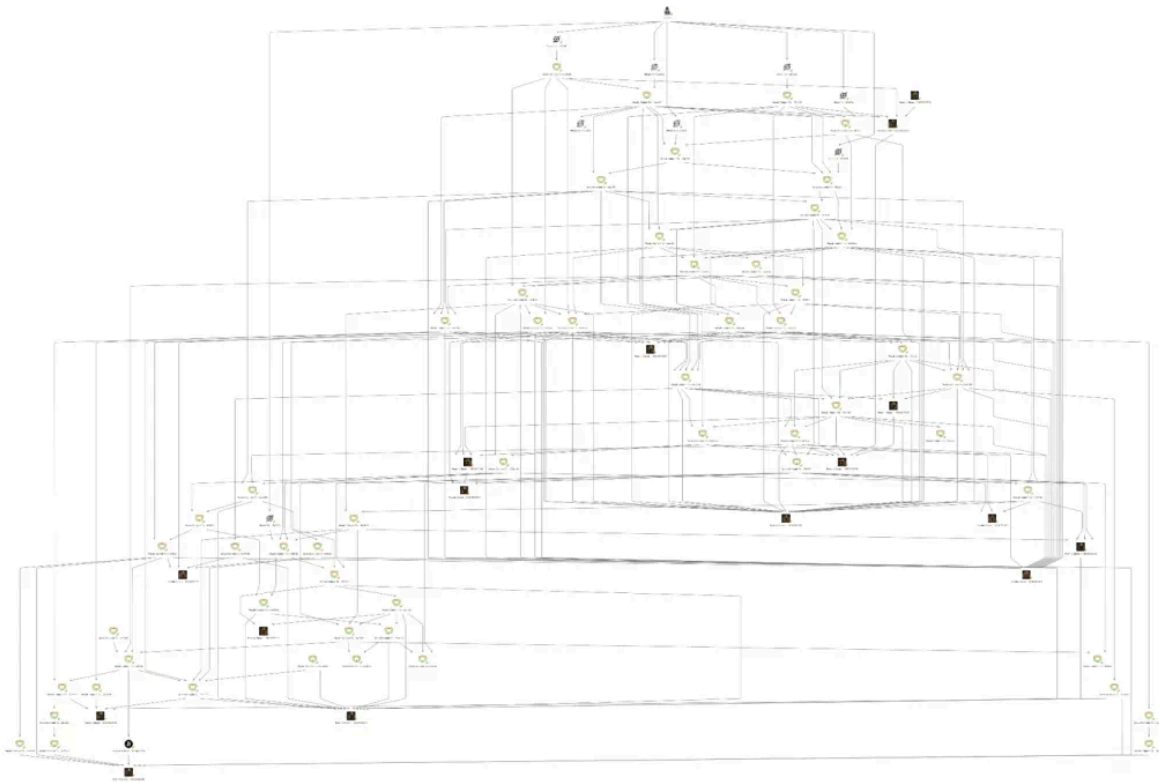
- Address usage frequency



- Input amounts
- Withdrawal amounts
- Post-withdrawal transaction behavior

After a series of detailed analyses, the team successfully identified several suspicious withdrawal addresses. We then compiled and compared the withdrawal amounts from these addresses and found that these amounts were largely consistent with the funds transferred to Wasabi Coinjoin by the hackers. We discovered a correlation between different Wasabi Coinjoin withdrawal transactions, and the withdrawal addresses showed a clustering relationship. Therefore, we can confirm that these addresses are the hackers' withdrawal addresses.

Here's a bird's-eye view of the hacker's Coinjoin transaction:



#### (4) Cross-Chain Tracking

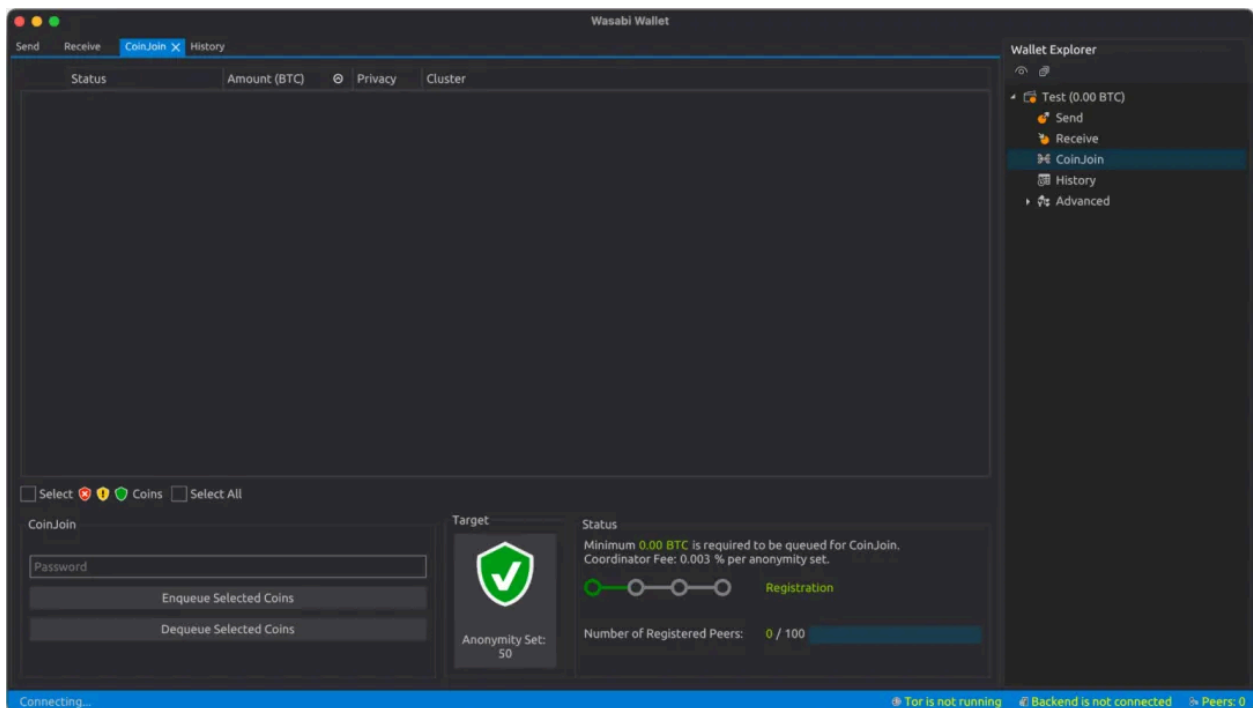
After identifying Wasabi CoinJoin withdrawal addresses, MistTrack further tracked stolen funds. The hacker used renBTC for cross-chain operations. Analysis revealed Ethereum renBTC

withdrawal addresses, which were then exchanged for ETH and dispersed across multiple exchanges.

### (5) Hacker Trace Analysis

Based on on-chain traces, MistTrack profiled the hacker:

- Highly knowledgeable in crypto laundering techniques, proficient in automation and darknet tools.



- Additional transactions: Ethereum renBTC withdrawal addresses showed deposits and withdrawals from exchanges.



### (6) Outcome

After analyzing the hacker's exchange history, the MistTrack team immediately shared this information with the affected users and assisted law enforcement agencies in contacting the exchange to request evidence. The exchange then implemented risk control measures for potentially implicated accounts. Ultimately, as the hacker attempted to transfer further stolen funds to exchange-related accounts, the close collaboration between the MistTrack team, law enforcement agencies, and the exchange successfully froze a portion of the stolen funds.

It's important to note that once funds enter a mixer, the original path is unlikely to be fully reconstructed, creating a natural blind spot in on-chain tracing. However, external clues can be used for lateral verification: for example, behavioral patterns before mixing and a consistent destination after mixing; leveraging on-chain fixed-amount characteristics to trace mixing behavior; analyzing inflow and outflow paths within a time window; developing outflow address profiles and behavioral clustering models; linking post-mixing paths with exchange deposits; and leveraging open-source intelligence to supplement on-chain deficiencies and establish attribution. In judicial investigations, mixing behavior can serve as a clue to the motive behind intentional concealment of funds, enhancing the nature of the case (e.g., fraud vs. money laundering). Furthermore, open-source intelligence (OSINT) can be combined to further uncover clues of manipulation behind the mixer's path. For example, an attacker may have used an ENS domain name for a withdrawal address, uploaded NFTs, or even connected to social applications (such as Lens Protocol). Using this non-financial data, researchers can attempt to link technical paths to real-world identities. Mixers are inherently a direct challenge to on-chain tracing capabilities. However, as long as we understand its operating logic and identify its common usage patterns, we can still provide valuable upstream and downstream clues for the overall case analysis.

Mixers aren't unbreakable; they simply increase the difficulty of analysis. The real challenge lies in attackers' flexible tool combinations and strategy switching. Rather than reproducing each attack path, investigators should build a behavioral signature library to identify potential mixing motives and path structures, thereby taking proactive action at the strategic level.

## 7. NFT Tracking Analysis

NFTs (Non-Fungible Tokens), as a new form of crypto assets, do not typically have the high liquidity of mainstream tokens, but due to their uniqueness, collectible value, and emotional

premium, they have become new targets for attackers. Many phishing attacks, rug pull projects, and account theft cases revolve around NFTs, making understanding how to track them an essential part of on-chain analysis.

Unlike standard ERC20 assets, NFTs are usually issued under ERC721 or ERC1155 standards, with unique Token IDs and ownership addresses. Their ownership transfers are fully transparent, but tracking them poses challenges. The uniqueness of NFTs means each transfer may represent a change in value, and NFT contracts often use complex functions (such as Multicall) to obscure critical actions. Additionally, NFT trading records are fragmented across multiple platforms, price data can be manipulated, and contracts are frequently updated, all of which increase tracking difficulty.

In tracking, the process typically starts by identifying the NFT's contract address and Token ID. Tools such as NFTScan or NFTGo can be used to query the full history from minting to the present. During this process, NFTs may be sold at high prices or moved to other addresses controlled by the attacker before sale. The focus should be on the assets received from the sale rather than continuing to track the NFT itself.

Case Study: A user clicked the first search result when searching for Aave on Google and visited a phishing site at `app.avaea[.]eu[.]com/dashboard`. On this page, the user was induced to sign a malicious transaction, resulting in the theft of their Uniswap V3 LP Position NFT, causing a direct loss of approximately \$1.23 million (491,239 USDe + 744,997 USDT). Based on information provided by the victim, the following key transactions were identified:

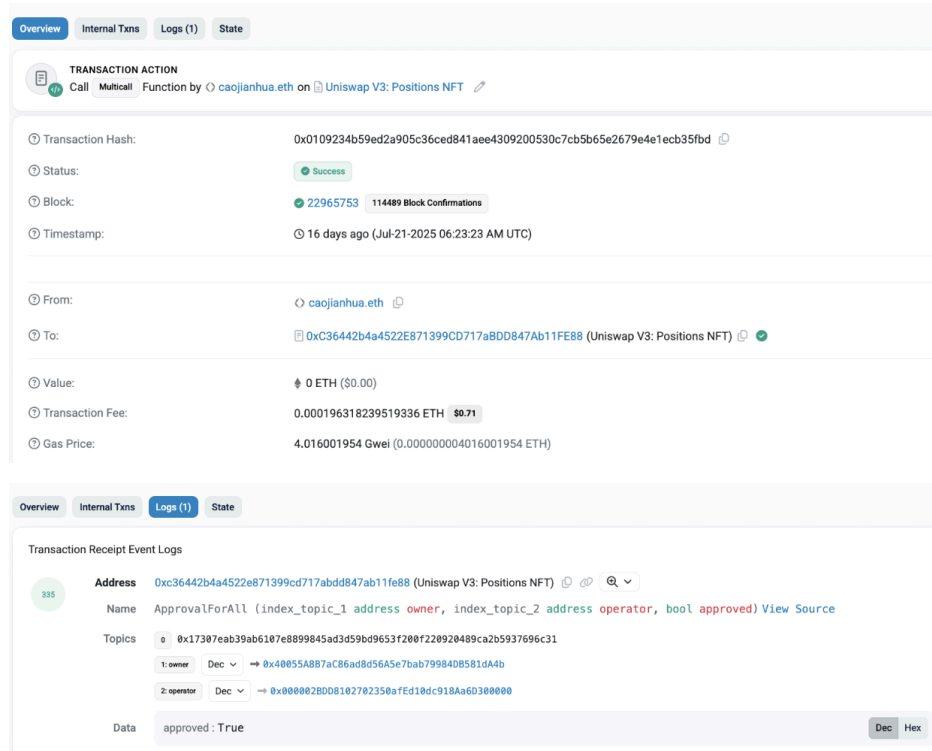
- Victim Signs Authorization Transaction

Transaction Hash:

<https://etherscan.io/tx/0x0109234b59ed2a905c36ced841aee4309200530c7cb5b65e2679e4e1ecb35fbd>

Operation: The victim's address (0x400...A4b) signed a malicious Multicall transaction in 0x010923...b35fbd, which appeared legitimate on the surface but included a "setApprovalForAll" authorization to the phishing contract address

0x000002BDD8102702350afEd10dc918Aa6D300000, granting control of their LP NFT to the phishing contract.



The screenshot shows a transaction action on Etherscan. The transaction is titled "TRANSACTION ACTION" and is a "Call" function by "caojianhua.eth" on the "Uniswap V3: Positions NFT" contract. The transaction hash is 0x0109234b59ed2a905c36ced841aee4309200530c7cb5b65e2679e4e1ecb35fbd. The status is "Success" with 22965753 blocks and 114489 block confirmations. It occurred 16 days ago (Jul-21-2025 06:23:23 AM UTC). The transaction was sent from "caojianhua.eth" to "0xC36442b4a4522e871399cd717abdd847ab11fe88 (Uniswap V3: Positions NFT)". The value is 0 ETH (\$0.00), the transaction fee is 0.000196318239519336 ETH (\$0.71), and the gas price is 4.016001954 Gwei (0.00000004016001954 ETH).

The "Transaction Receipt Event Logs" section shows a log for "ApprovalForAll" with the following details:

- Address:** 0xc36442b4a4522e871399cd717abdd847ab11fe88 (Uniswap V3: Positions NFT)
- Name:** ApprovalForAll (index\_topic\_1 address owner, index\_topic\_2 address operator, bool approved) View Source
- Topics:**
  - 0: 0x17307eab39ab6107e8899845ad3d59b9653f200f220920489ca2b5937696c31
  - 1: owner: Dec → 0x40855A8B7aC86ad8d56A5e7bab799840B581dA4b
  - 2: operator: Dec → 0x000002BDD8102702350afEd10dc918Aa6D300000
- Data:** approved: True

- Attacker Transfers NFT

Transaction Hash:

<https://etherscan.io/tx/0xf81db5307fd1d71fce993f1d1c42f04b6240868c8fc06f1abdd58c648aa873ba>

Operation: The attacker, in transaction 0xf81db5...a873ba, called the batchTransferERC721 method to move the victim's LP NFT to a wallet controlled by the attacker. This transfer succeeded because the victim had granted authorization in the previous step.





**TRANSACTION ACTION**  
 Remove 490,365.34 (\$490,365.34) USDe And 744,087.58 (\$743,988.62) USDT Liquidity From Uniswap V3  
 Collect 491,239.81 (\$491,239.81) USDe And 744,997.35 (\$744,898.26) USDT From Uniswap V3

Transaction Hash: 0x219b4d06d072e83dde2d6507deed64cb43bad0bae3dcbe50dba9bfe35824bc67 [🔗](#)  
 Status: Success  
 Block: 22965775 114522 Block Confirmations  
 Timestamp: 16 days ago (Jul-21-2025 06:27:59 AM UTC)

From: 0x000093161E379aEBCf40E7aCfd387Edb3000000 (Fake\_Phishing1306155) [🔗](#)  
 Interacted With (To): [0xC36442b4a4522E871399CD717aBDD847Ab11FE88 \(Uniswap V3: Positions NFT\)](#) [🔗](#) ✔️

ERC-20 Tokens Transferred: 2

All Transfers Net Transfers

▶ From [Uniswap V3: USDe-USD...](#) [🔗](#) To [Fake\\_Phishing1306155](#) [🔗](#) For 491,239.80548608213193257 (\$491,239.81) USDe (USDe) [🔗](#)  
 ▶ From [Uniswap V3: USDe-USD...](#) [🔗](#) To [Fake\\_Phishing1306155](#) [🔗](#) For 744,997.345205 (\$744,898.26) Tether USD (USDT) [🔗](#)

Value: 0 ETH (\$0.00)  
 Transaction Fee: 0.000888917545153315 ETH \$3.23  
 Gas Price: 4.597334153 Gwei (0.000000004597334153 ETH)

Ether Price: \$3,764.26 / ETH  
 Gas Limit & Usage by Txn: 277,032 | 193,355 (69.8%)  
 Gas Fees: Base: 1.597334153 Gwei | Max: 6.546371091 Gwei | Max Priority: 3 Gwei  
 Burnt & Txn Savings Fees: 🔥 Burnt: 0.000308852545153315 ETH (\$1.12) 💰 Txn Savings: 0.00037685603714699 ETH (\$1.37)

Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 376 Position In Block: 49































Input Data:

```
Function: multicall(bytes[] data)
MethodID: 0xac9650d8
[0]: 0000000000000000000000000000000000000000000000000000000000000020
[1]: 0000000000000000000000000000000000000000000000000000000000000002
[2]: 0000000000000000000000000000000000000000000000000000000000000040
[3]: 0000000000000000000000000000000000000000000000000000000000000120
[4]: 00000000000000000000000000000000000000000000000000000000000000a4
```

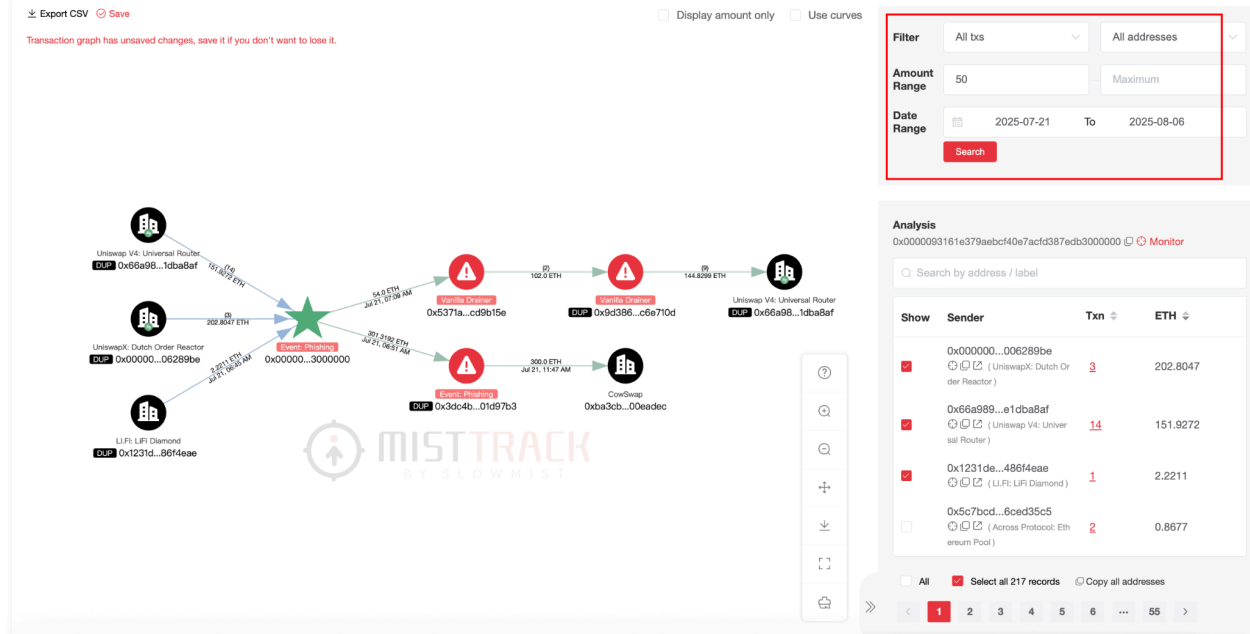
View Input As Decode Input Data View In Decoder Advanced Filter Write Contract

Once the NFT has been converted into standard assets, tracking can continue as with regular tokens. In this case, the attacker exchanged the obtained USDe and USDT for 355 ETH via Uniswap.



2025/07/21 14:45:35 0x5ff8...8132	execute Ox0000...0000	 -8,396.0997 USDe (\$8,405.67)  +2,221.1 ETH (\$8,356.67)	Gas Fee 0.0011ETH(\$4.08)
2025/07/21 14:43:59 0x8ff5...1d44	execute Uniswap V4	 -2,798.6999 USDe (\$2,801.89)  +0,7368 ETH (\$2,771.94)	Gas Fee 0.0011ETH(\$4.03)
2025/07/21 14:41:59 0x28d5...d303	execute Uniswap V4	 -3,731.5999 USDe (\$3,735.85)  +0,9812 ETH (\$3,691.58)	Gas Fee 0.0011ETH(\$4.12)
2025/07/21 14:39:47 0xaeff...5165	execute Uniswap V4	 -14,926.3994 USDe (\$14,943.42)  +3,9256 ETH (\$4,769.56)	Gas Fee 0.0019ETH(\$7.09)
2025/07/21 14:35:23 0x907b...c7fd	execute Uniswap V4	 -29,852.7988 USDe (\$29,886.84)  +7,8355 ETH (\$29,479.77)	Gas Fee 0.0016ETH(\$5.95)
2025/07/21 14:34:23 0x037c...11c2	execute Uniswap V4	 -59,705.5976 USDe (\$59,773.68)  +15,6917 ETH (\$59,037.31)	Gas Fee 0.0023ETH(\$8.58)
2025/07/21 14:33:23 0x4b10...e23c	execute Uniswap V4	 -39,803.7318 USDe (\$39,849.12)  +10,4621 ETH (\$39,361.88)	Gas Fee 0.0014ETH(\$5.25)
2025/07/21 14:32:11 0x8899...d8e7	execute Uniswap V4	 -25,000.0000 USDe (\$25,028.51)  +6,5670 ETH (\$24,707.18)	Gas Fee 0.0014ETH(\$5.18)
2025/07/21 14:30:59 0xd16d...75a4	execute Uniswap V4	 -61,404.9757 USDe (\$61,475.00)  +16,1274 ETH (\$60,676.72)	Gas Fee 0.0026ETH(\$9.81)
2025/07/21 14:29:59 0xb3a2...f56d	execute Uniswap V4	 -245,619.9027 USDe (\$245,899.98)  +64,3217 ETH (\$241,999.59)	Gas Fee 0.0027ETH(\$10.29)
2025/07/21 14:28:59 0xe659...8482	executeFFsYo Oxa69b...e78c	 -769,723.7119 USDT (\$770,070.09)  +201,5054 ETH (\$758,129.84)	
2025/07/21 14:28:35 0x526a...fed0	Approve infinite USDT for Uniswap Permit2		Gas Fee 0.0002ETH(\$0.84)
2025/07/21 14:27:59 0x219b...bc67	multicall Uniswap V3	 +744,997.3452 USDT (\$745,332.59)  +491,239.8055 USDe (\$491,799.97)	Gas Fee 0.0009ETH(\$3.34)
2025/07/21 14:27:35 0x95cc...150a	execute Ox0000...0000	 -96,034.8628 USDe (\$96,144.37)  +25,1429 ETH (\$94,596.07)	Gas Fee 0.0018ETH(\$6.75)
2025/07/21 14:23:59 0xe1bd...6bbf	collect Uniswap V3	 +96,034.8628 USDe (\$96,144.37)  +24,726.3667 USDT (\$24,737.49)	Gas Fee 0.0003ETH(\$1.01)
2025/07/21 14:23:47 0x7366...7abe	decreaseLiquidity Uniswap V3		Gas Fee 0.0003ETH(\$1.07)
2025/07/21 14:23:35 0xf81d...73ba	batchTransferERC721 Ox0000...0000	 +1 #1038161  +1 #1037091	Gas Fee 0.0003ETH(\$1.31)

Using MistTrack with a start time filter set to the theft date of July 21 and filtering transactions above 50 ETH to exclude small phishing transactions, the transfer results showed that the involved ETH was ultimately moved to Uniswap and CowSwap for token swaps. The intermediate addresses were flagged by MistTrack as Vanilla Drainer, indicating that the behind-the-scenes operator was the phishing group Vanilla Drainer.



The complexity of non-standard assets requires investigators to adopt a multi-dimensional perspective. Beyond the on-chain flow of the NFT itself, it is necessary to consider the context of authorization transactions, address labeling, and the inflow and outflow paths of extracted funds to accurately determine the identity of operators and the profit chain behind NFT movements.

## 8. Address Behavior Analysis

Addresses are the most basic unit in on-chain asset tracking. However, a single address often does not represent the real operator. Treating an address merely as a “receiving account” or “transfer node” can overlook underlying control relationships, behavioral patterns, and potential risk characteristics. Address behavior analysis is therefore a key step in transforming fund flows into operator profiles, constructing a “behavioral fingerprint” through each transaction, contract interaction, cross-chain transfer, or mixer attempt, which helps infer operational habits, preferences, and even potential identity.

### (1) Active Behavior Feature Identification

Identifying the basic behavioral features of an address is the starting point of analysis. For example, an address that has been dormant for a long time but suddenly transfers a large

amount of assets, or one that makes frequent small transfers in a short period, may indicate unconventional usage, potentially for money laundering, fund routing, or scripted operations:

- **Dormant Activation:** An address remains inactive for a long period and suddenly performs a large transfer, common in exit or cash-out scenarios.
- **High-Frequency Transfers:** Multiple transfers in a short time, often for dispersing funds or laundering.
- **Fixed Amounts:** Many transfers of similar amounts (e.g., 0.9999 ETH), possibly indicating automated scripts or mixer usage.
- **Short Lifespan:** Newly created addresses quickly receive and transfer funds, typical of temporary wallets.

## (2) Address Clustering Analysis

Attackers rarely use a single address. Behavior clustering involves grouping addresses likely controlled by the same entity. Patterns such as consistent activity time, use of specific platforms, repeated transactions in the same stablecoin, or recurring cross-chain paths can form a distinct on-chain “fingerprint.” Multiple addresses showing similar habits, counterparties, and transaction rhythms can help establish these fingerprints and identify actors:

- **Input Clustering:** In a transaction, if multiple addresses contribute inputs (e.g., BTC UTXO model), they may be controlled by the same operator.
- **Behavioral Synchrony:** Addresses that receive funds from the same source around the same time and react similarly (cross-chain transfers, DEX trades) may be controlled by one operator.
- **Shared Services:** Multiple addresses interacting with the same contract (e.g., Ponzi schemes, black/grey market tokens) and showing similar paths can be grouped as a behavioral cluster.
- **Transaction Parameter Similarity:** Repeated patterns in gas limits, slippage, or fee preferences can be used as clustering features.
- **Address Naming Patterns:** Some groups create addresses following identifiable naming schemes, e.g., in the Nobitex attack, Gonjeshke Darande used addresses with provocative

keywords and repeated structures. (TKFuckiRGCTerroristsNoBiTEXy2r7mNX,  
0xffDead, 1FuckiRGCTerroristsNoBiTEXXXaAovLX)

### (3) Risk Behavior Profiling

Determining if an address is “risky” requires analyzing its overall behavior, not just its interactions:

- Rapid Outflow: Funds are transferred out immediately after receipt, typical for routing or temporary receiving addresses.
- Frequent Mixer Usage: Repeated interactions with Tornado Cash, Railgun, Wasabi, or proxies calling these protocols.
- Cross-Chain Activity: Frequent movement across L2s or non-mainstream chains.
- Suspicious Interactions: Calling failed contract functions, interacting with scam or “airdrop” tokens, or overlapping with known malicious addresses.
- Scripted Operations: Deploying phishing contracts or automatically extracting authorized assets, typical in rug pulls or phishing drainers.

### (4) Address Labels and Off-Chain Identity

While blockchain addresses do not directly correspond to real identities, cross-analysis with off-chain data can gradually reconstruct likely operator profiles. Platforms like MistTrack use extensive address label databases and fund flow analysis, combined with external sources, to build a multi-dimensional identity assessment:

- CEX Interaction Identification: By analyzing interactions with centralized exchanges (CEXs) and combining with KYC or risk logs, addresses can be linked to real-world accounts.
- Label Propagation: Tracing relationships with high-risk addresses (e.g., hacker or OFAC-sanctioned addresses) helps identify associated clusters.
- Social Behavior Cross-Verification: Activities on GitHub, Reddit, Twitter, etc., can be time-correlated with on-chain actions for preliminary association.
- Data Leak Comparison: Leaked emails, phone numbers, or mnemonics can be fuzzily matched with transaction histories to support identity inference.

Attackers often use various anonymity tools off-chain to further hide identity:

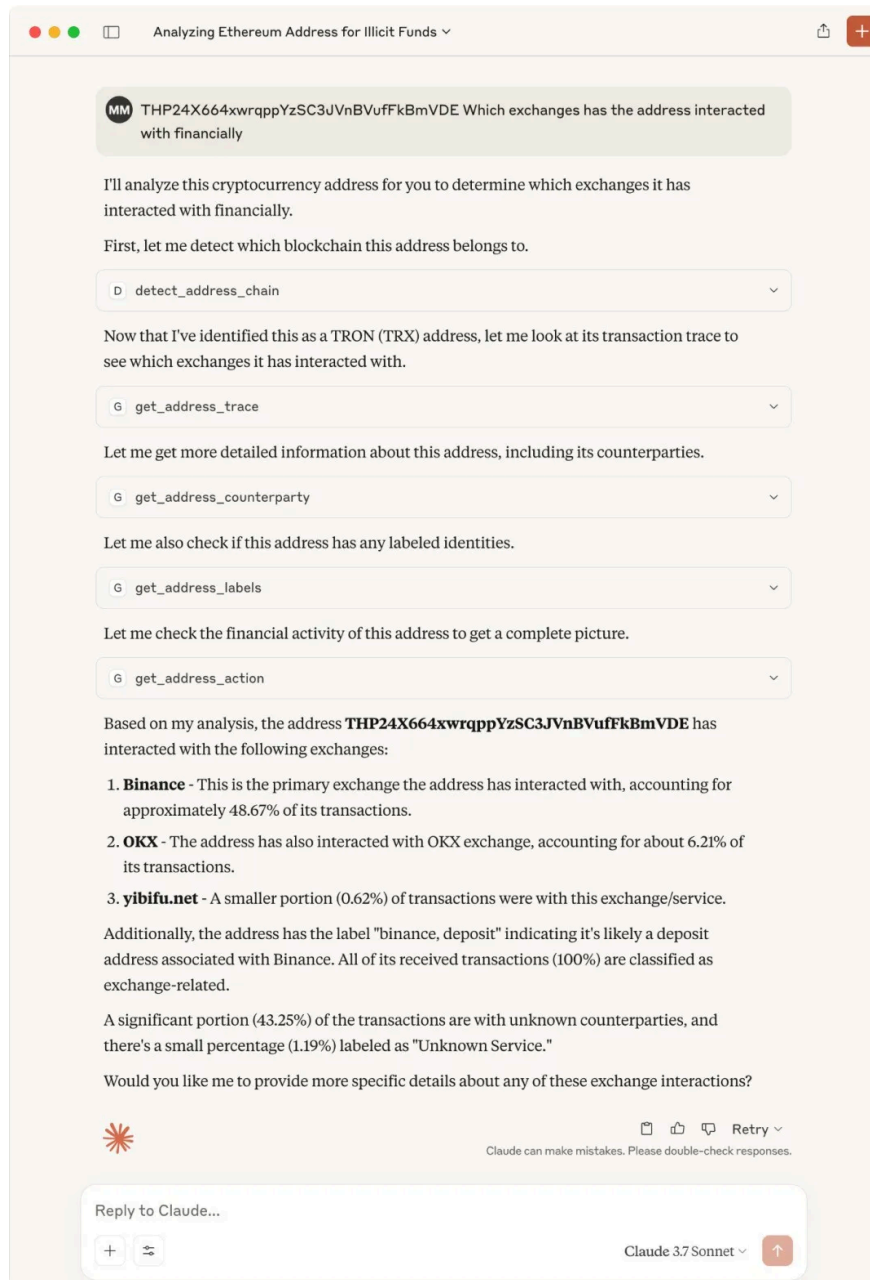
- **Anonymous Network Tools:** Attackers often use tools such as VPNs, the Tor network, and proxy servers to hide their true IP addresses and login locations. Some of these tools are subject to law enforcement investigation.
- **Privacy Messaging and Email Services:** Use end-to-end encrypted email services such as ProtonMail and Tutanota, as well as anonymous chat tools such as Signal, Telegram, and Session, which are widely used for account registration, communication coordination, over-the-counter transactions, and even sharing stolen data.
- **Anonymous Infrastructure:** Attackers may rent VPSs or "bulletproof hosting" services that support cryptocurrency payments and lack real-name verification to set up phishing sites, deploy malicious smart contracts, or automated money laundering scripts. These service providers typically do not retain customer logs, further increasing the difficulty of locating attackers.
- **Fake Identity Generation:** When passing initial Know Your Customer (KYC) checks on some lightly regulated platforms, attackers may use batches of fake identities to register and maintain accounts. These identities often have templated formats, and methods such as device fingerprinting and IP analysis can gradually identify common characteristics.

While these anonymous services don't leave direct on-chain traces themselves, the indirect traces they leave within the attack chain still hold valuable traceability. By combining platform-side login records, operation logs, KYC data, social account activity, and on-chain transfer times, frequency, and tools used, professional researchers can build their own hacker information databases and compare them with anonymous email addresses, VPN accounts, and other information within the database. This provides a powerful off-chain path for identity association and behavior tracing when on-chain tracing is blocked.

## (5) AI Tools and Analysis

Modern on-chain analytics platforms are advancing automation and intelligence in behavioral profiling. [MistTrack MCP](#), for example, allows natural language API calls through clients like Claude or Cursor to generate address profiles, risk scores, and transaction graphs, improving efficiency and accessibility.

Users can request analysis via MCP-enabled AI tools, e.g., “Please track the fund flow between this address and exchanges, with a depth of 2: [ETH\_ADDRESS].” The AI will call MistTrack APIs and return detailed, readable results.



MistTrack MCP currently supports 10+ on-chain analytics tools covering risk identification, address profiling, and transaction graph construction.

- `mcp_misttrack_detect_address_chain` - Detect the blockchain and possible tokens supported by the address
- `mcp_misttrack_get_address_labels` - Get label list for specified address
- `mcp_misttrack_get_address_overview` - Get balance and statistics for specified address
- `mcp_misttrack_get_address_action` - Get transaction operation analysis results for specified address
- `mcp_misttrack_get_address_trace` - Get profile for specified address, including platform interaction list and related threat intelligence data
- `mcp_misttrack_get_address_counterparty` - Get transaction counterparty analysis results for specified address
- `mcp_misttrack_check_malicious_funds` - Check if specified address has malicious funds (like blacklisted USDT)
- `mcp_misttrack_get_risk_score` - Get risk score for specified address or transaction hash
- `mcp_misttrack_get_dashboard_url` - Generate MistTrack dashboard URL based on coin and address
- `mcp_misttrack_get_chain_explorer_url` - Generate blockchain explorer URL based on coin and address
- `mcp_misttrack_get_url_info` - Get comprehensive URL information for specified address, including dashboard URL and blockchain explorer URL
- `analyze_transactions_recursive` - Recursively analyze transaction relationships and build transaction graph for multiple-layer funds tracing

AI integration is expected to increase speed, accuracy, and transform profiles from static labels to dynamic behavior sequences.

Building on-chain identity profiles does not necessarily mean real-world identification. The core goal is to infer organizational control, fund cycles, or structural links with high-risk entities. This method is crucial in addressing complex fraud, layered laundering, and advanced scenarios.

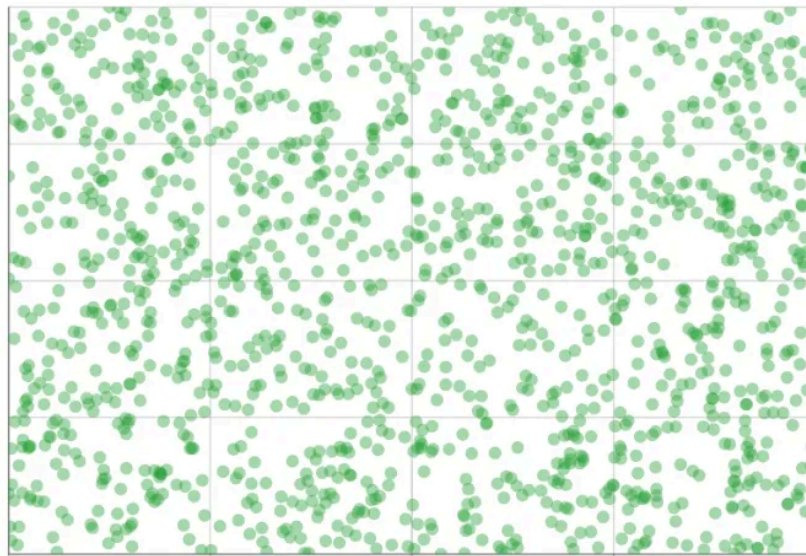
Through continuous analysis of transfers, contract interactions, and cross-chain activity, fragmented wallet addresses can be linked into coherent entity profiles. Just like detectives scrutinize subtle crime scene clues, on-chain analysts must track the logic behind each transfer, authorization, and cross-chain movement to find connections across cases, ultimately building behavioral networks and identity webs. These profiles support tracing paths, reconstructing network structures, and providing reliable evidence for exchanges, project teams, or law enforcement to freeze assets and issue risk warnings.

## 9. Case Studies

In on-chain tracking practice, different types of fund flow paths exhibit distinct behavioral characteristics. This section presents selected cases to provide readers with reference perspectives for observing on-chain behavior.

### Case 1: Peel Chain Tracking

On August 3, 2016, the well-known cryptocurrency exchange Bitfinex announced a hack that resulted in the theft of approximately 119,755 BTC. At that time, this amounted to roughly \$60 million, or about \$4.5 billion in total value based on contemporary pricing. MistTrack analysis showed that the stolen assets were initially dispersed across 2,072 wallet addresses, which were labeled as follows:



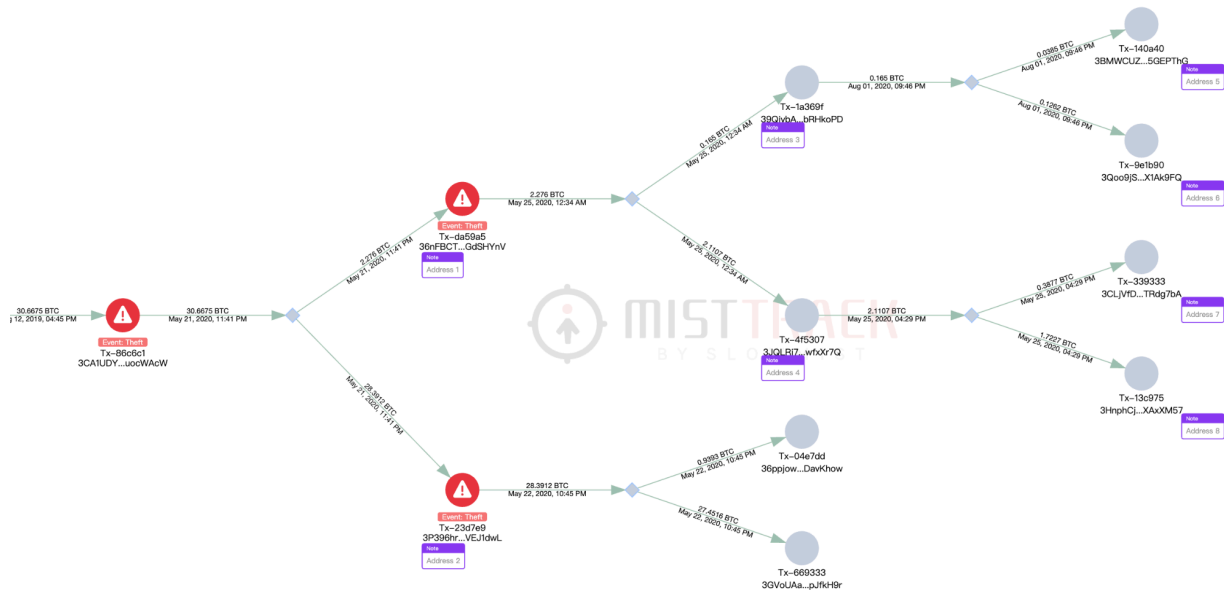
Starting January 2017, the hacker began intensive fund transfers. Analyzing the 2,072 addresses revealed that most funds were moved using a peel chain method. MistTrack tracked approximately 30.6781 BTC from a Bitfinex platform address to the hacker address [19Xs96FQJ5mMbb7Xf7NXMDeHbsHqY1HBDM](https://blockchain.info/address/19Xs96FQJ5mMbb7Xf7NXMDeHbsHqY1HBDM), and then via two straight transfers to 3CA1UDYQy47Z46HKCVqRV8b1XVduocWAcW.



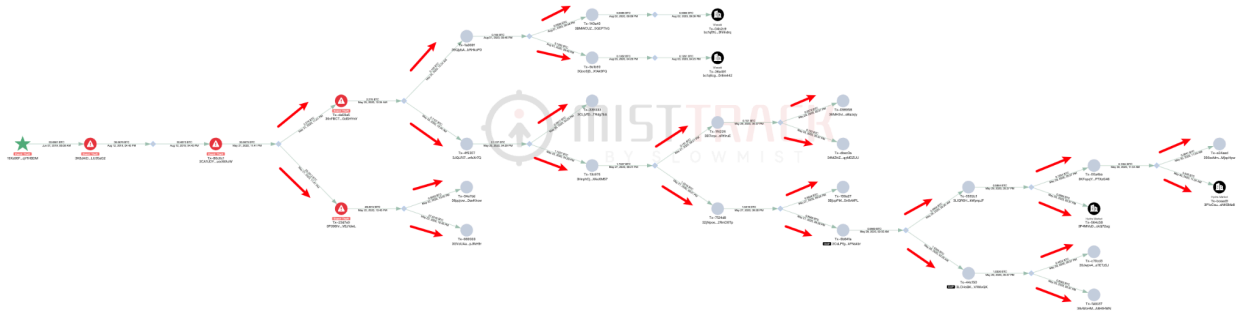


Examining 3CA1UDYQy47Z46HKCVqRV8b1XVduocWAcW's flow:

- 30.6675 BTC was split into 2.27 BTC and 28.39 BTC and sent to addresses 1 and 2.
- Address 1 further split 2.27 BTC into 0.16 BTC and 2.11 BTC to addresses 3 and 4.
- Address 3 repeated the splitting with 0.16 BTC into addresses 5 and 6, and so on.



For a more intuitive presentation, we've captured a portion of the fund flow.



As can be seen in the image above, funds were transferred to two addresses, which were then each transferred to two other addresses. The amounts gradually decreased, and the addresses appeared in increasing numbers, until some funds were eventually transferred out through Wasabi CoinJoin mixers or to the Hydra Market darknet market. Of course, this is only a small portion of the funds, but it's clear that the hackers were very patient in evading tracking. Let's take another hacker address, [1BprR3VRh8AsJVXFR8uNzzZJnyMhF1gyQE](https://misttrack.com/address/1BprR3VRh8AsJVXFR8uNzzZJnyMhF1gyQE), as an example. According to MistTrack, this hacker address stole 271.22 BTC.

**BTC** | P2PKH

1BprR3VRh8AsJVXFR8uNzzZJnyMhF1gyQE Copy Report Favorites

Portfolio ▾

Explorer ▾

---

**AML Risk Score** ⓘ Risk Report

Risk Score: 85

Risk Level: High

- Theft
- Suspected malicious address
- Involved in illicit activity
- Interact with high-risk tag address

Detail >

**Overview** B \$ Data updated seconds ago ↻

<p>Balance 0.0 BTC</p> <p>First seen (UTC) Aug 02, 2016, 09:02 AM</p> <p>Total received 271.2278 BTC</p> <p>Incoming txn 4</p>	<p>Txs count 5</p> <p>Last seen (UTC) Jul 24, 2020, 04:48 PM</p> <p>Total spent 271.2278 BTC</p> <p>Outgoing txn 1</p>
--	--

We then tracked the large transfer addresses:

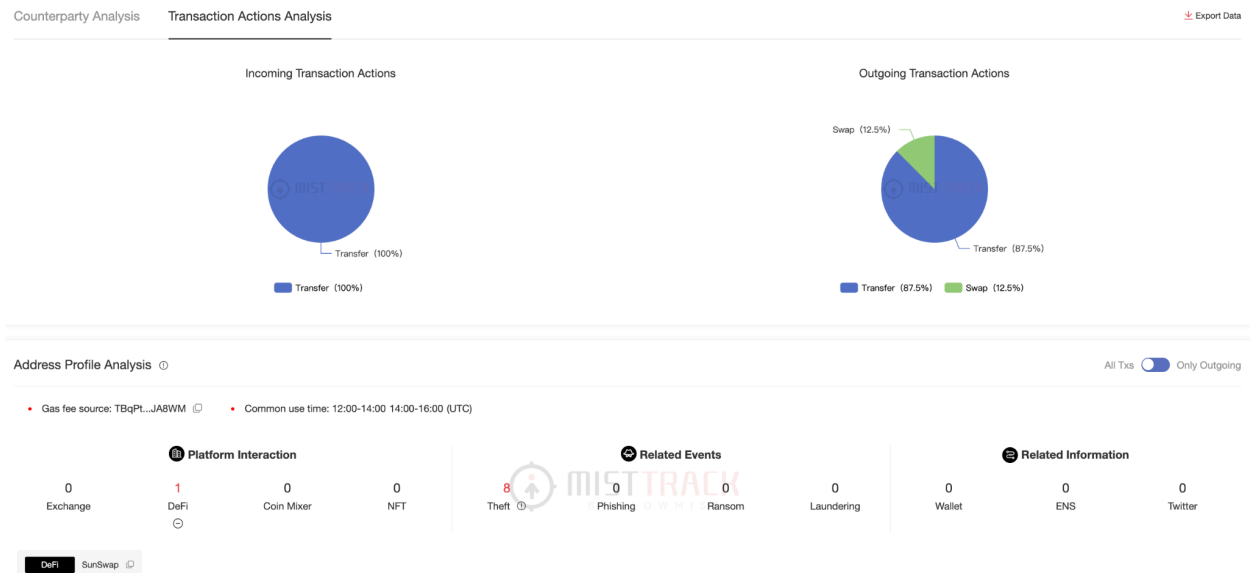


Although the transfer of small amounts of funds is omitted, we can still clearly see the characteristics of the Peel Chain technique:

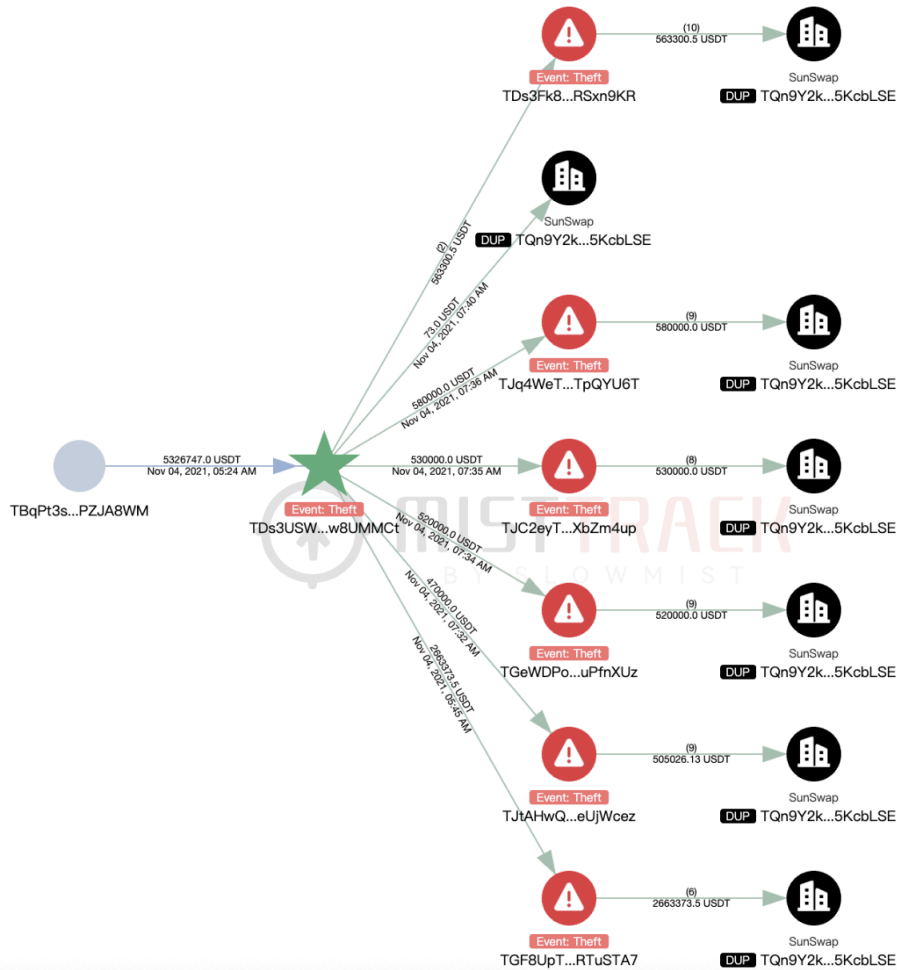
- Generally starts with a single "dirty" address;
- Usually continuously split into two addresses;
- Split into large and small amounts;
- Funds are parked or mixed or enter exchanges/darknet platforms.

### Case 2: TRON Network Tracking

A victim who imported their private key into a fake wallet app lost 5,326,747 USDT (over 5.3 million USD). Using the MistTrack anti-money laundering (AML) tracking system, we first analyzed the hacker’s initial address: [TDs3USWcG5ua4jkGNMGgNZrXrPgw8UMMCt](https://tronscan.org/#/address/TDs3USWcG5ua4jkGNMGgNZrXrPgw8UMMCt).



From the analysis, the hacker’s transactions were mostly Transfers and Swaps. By examining the timing of these transactions, we can also infer the hacker’s active time periods. The stolen USDT was then moved to six addresses and exchanged using SunSwap.



For example, the initial hacker address TDs3USWcG5ua4jkGNMGgNZrXrPgW8UMMCt [swapped](#) 73 USDT for 684.76 TRX.

**Transaction Details** < >

TDs3USWcG5ua4jkGNMGgNZrXrPgw8UMMCt swapped 73 USDT for 684.76857 TRX on SunSwap

Hash: 54c40fa344f5c301c292b0d9f104886735347efd466d762ba7dc7137725125e5

Result: **SUCCESSFUL**

Block & Time: 35164765 | 1361 days ago | 2021-11-04 07:40:06 (UTC)

Status: **CONFIRMED** Confirmed by over 200 blocks

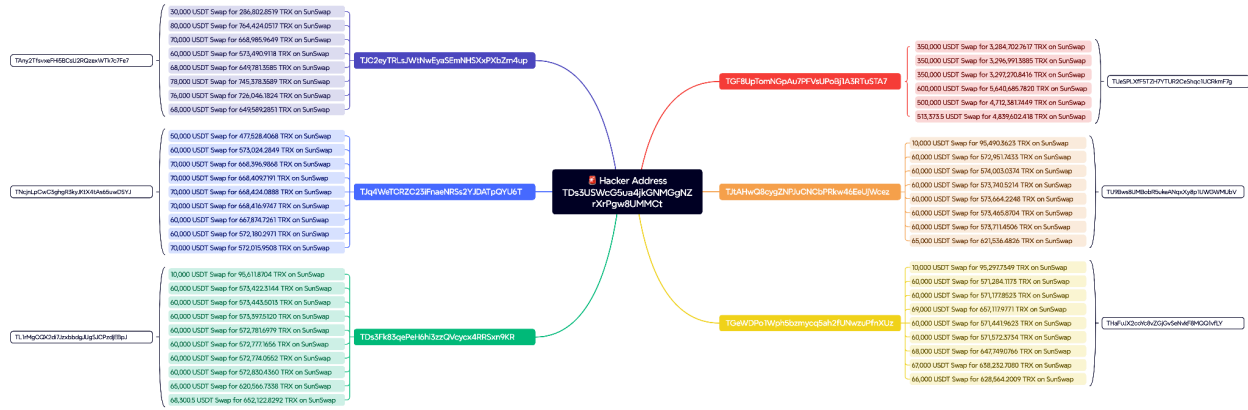
Confirmed SRs: 19 TRONLink Ant Investment Group BitGuild TRONALLIANCE

Resources Consumed & Fee: 11.73844 TRX  
Energy Fee Limit: 100 TRX

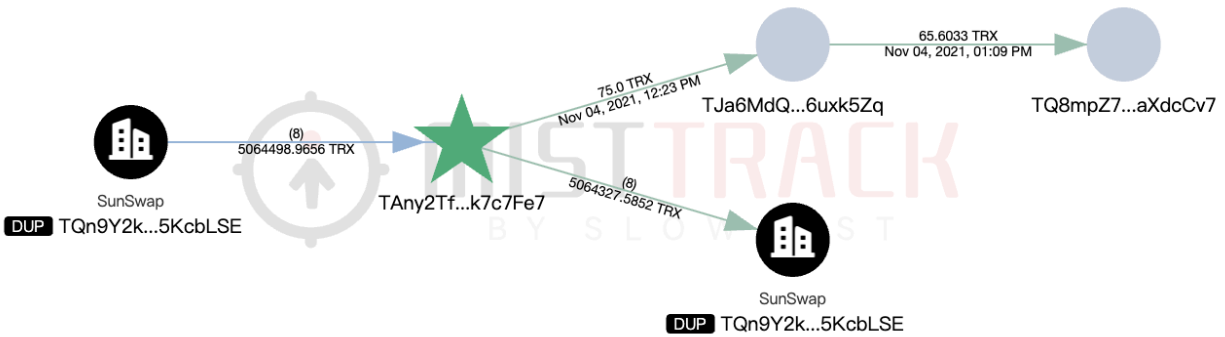
Looking at one of the six addresses, TGF8UpTomNGpAu7PFVsUPoBj1A3RTuSTA7, it swapped a total of 2,663,373.5 USDT into TRX via six [transactions](#) and sent them to the same address TUEs...mF7g.

Token Transfer: 2	From SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	To TUEsPLXIF5TZH7YTUR2CeShqc1UCRkmF7g	3,284,702.761741 TRX
	From TGF8UpTomNGpAu7PFVsUPoBj1A3RTuSTA7	To SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	350,000 USDT
Token Transfer: 2	From SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	To TUEsPLXIF5TZH7YTUR2CeShqc1UCRkmF7g	3,296,991.388533 TRX
	From TGF8UpTomNGpAu7PFVsUPoBj1A3RTuSTA7	To SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	350,000 USDT
Token Transfer: 2	From SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	To TUEsPLXIF5TZH7YTUR2CeShqc1UCRkmF7g	3,297,270.841694 TRX
	From TGF8UpTomNGpAu7PFVsUPoBj1A3RTuSTA7	To SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	350,000 USDT
Token Transfer: 2	From SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	To TUEsPLXIF5TZH7YTUR2CeShqc1UCRkmF7g	5,640,685.782043 TRX
	From TGF8UpTomNGpAu7PFVsUPoBj1A3RTuSTA7	To SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	600,000 USDT
Token Transfer: 2	From SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	To TUEsPLXIF5TZH7YTUR2CeShqc1UCRkmF7g	4,712,381.744991 TRX
	From TGF8UpTomNGpAu7PFVsUPoBj1A3RTuSTA7	To SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	500,000 USDT
Token Transfer: 2	From SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	To TUEsPLXIF5TZH7YTUR2CeShqc1UCRkmF7g	4,839,602.418044 TRX
	From TGF8UpTomNGpAu7PFVsUPoBj1A3RTuSTA7	To SC TQn9Y2khEsLJW1ChVW...5KcbLSE S-USDT-TRX Token	513,373.5 USDT

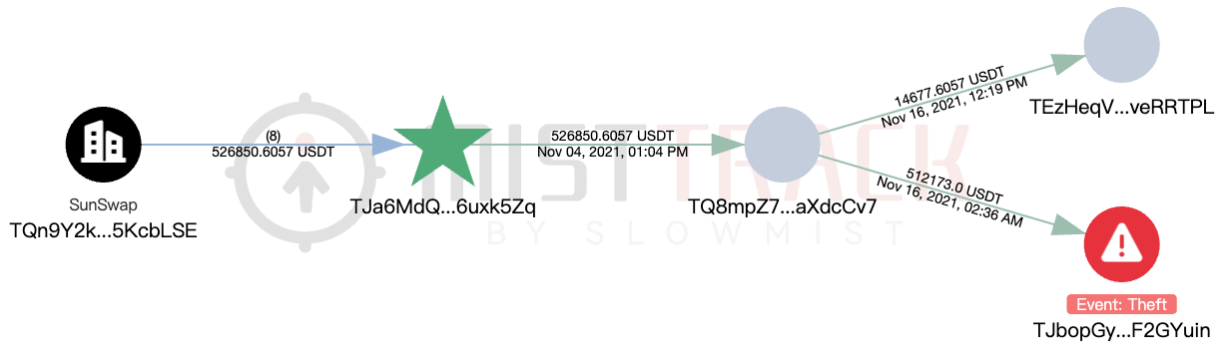
The other five addresses followed the same pattern.



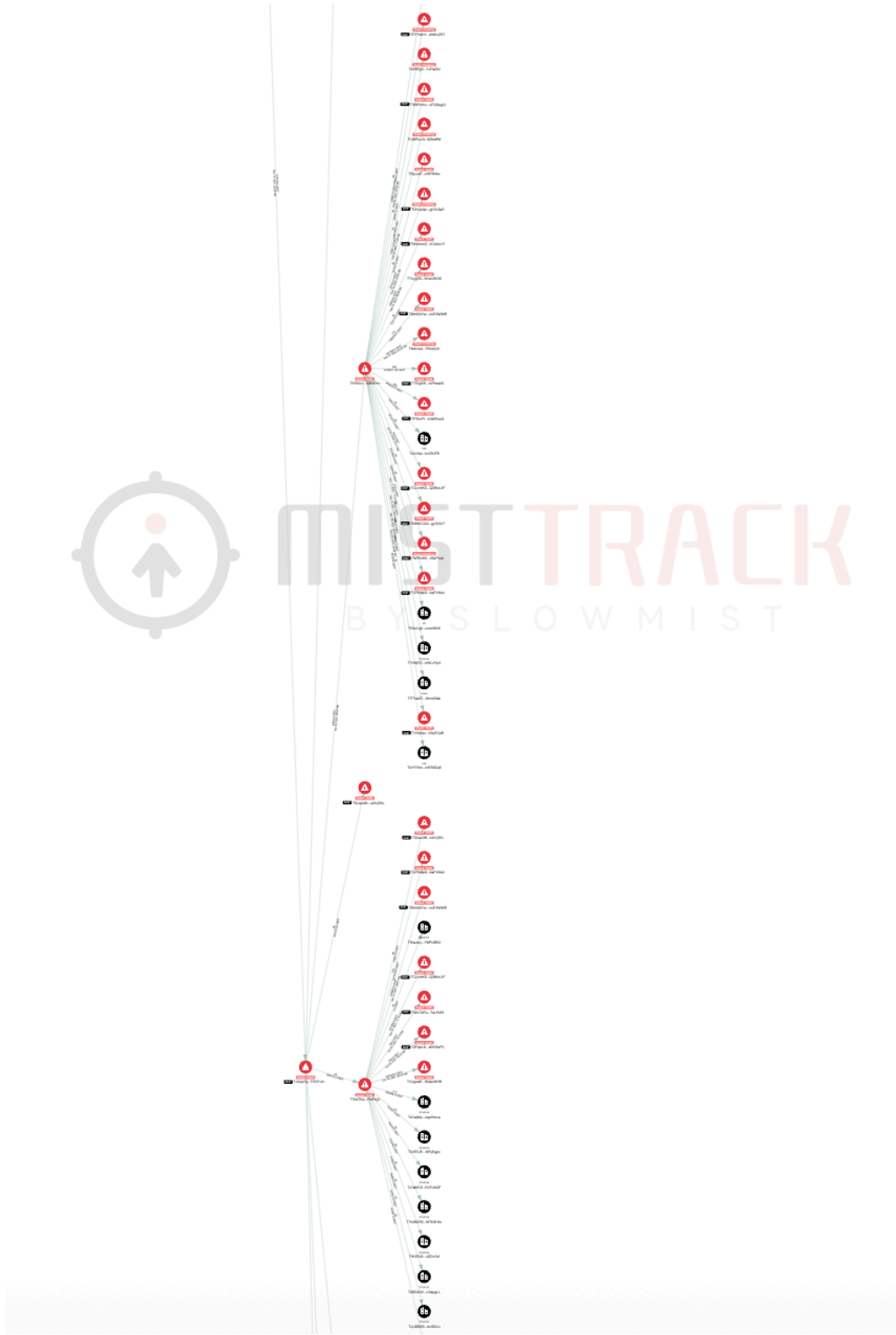
Tracking the new six addresses (leftmost and rightmost in the flow), for instance TAny2TfsvxeFHI5BCsU2RQzexWTK7c7Fe7, the hacker transferred 75 TRX to TQ8mpZ7RnDmz7nhmVNPk3dFdhjYaXdcCv7, leaving 57.41 TRX untransferred.



The remaining 5,064,327.5852 TRX was swapped back into 526,850.6057 USD via SunSwap and moved to TJa6MdQVDH3bvMCYiJpSPy9PTJF6uxk5Zq. That address then sent the USD to the same large address TQ8mpZ7RnDmz7nhmVNPk3dFdhjYaXdcCv7, which further distributed funds to two new addresses.



A shallow tracking of these two new addresses revealed “large addresses” (high balances + numerous transactions) eventually moving funds to multiple exchange addresses or addresses flagged as “Theft” by MistTrack – a pattern consistent with professional money laundering networks.



Interestingly, while five of the six addresses followed the same laundering method, the last address TUEsplxf5tzh7ytur2ceshq1ucrkmf7g slightly altered its method. Instead of



consolidating TRX into USDT and sending to one address, it split into 17 transactions, sending funds to different addresses. Here are the five largest transactions as an example:

Transaction 1: swapped 5,640,672.204843 TRX for 594,394.826963 USDT on SunSwap. Recipient: THrgSieejowjuCEyH8VtyTwhgRm1ojiAUM

Transaction 2: swapped 4,839,588.454844 TRX for 509,481.217226 USDT on SunSwap. Recipient: TBq5KQ74ATdoSsPo24R53QDe29S9jHeKvE

Transaction 3: swapped 4,712,367.781791 TRX for 496,144.129103 USDT on SunSwap. Recipient: TBBFsH9TqGVa7GHZPTHKGCbH5MekLuuk5r

Transaction 4: swapped 3,297,257.264494 TRX for 347,819.714254 USDT on SunSwap. Recipient: TQ7jaebLrj6EDpXT6WX49zo2V9Evzw5wFI

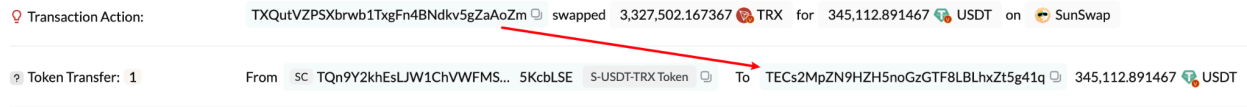
Transaction 5: swapped 3,296,977.811333 TRX for 347,881.638249 USDT on SunSwap. Recipient: TWz8ALaP9B9JszQ3a7JJSWQ25mHjhBPYyN

For example, the first recipient THrgSieejowjuCEyH8VtyTwhgRm1ojiAUM swapped USDT back to TRX twice, both times sending to TXQutVZPSXbrwb1TxgFn4BNdkv5gZaAoZm, resembling earlier patterns.

Transaction Details					
<input checked="" type="checkbox"/>	Time (UTC) ⌵	Sender	Recipient	Amount ⌵	TXID
<input checked="" type="checkbox"/>	Nov 05, 2021, 09:27 AM	THrgSiee...m1ojiAUM	TQn9Y2kh...w5KcblSE (SunSwap)	300,000 USDT	c30a37d3...6fa14c88
<input checked="" type="checkbox"/>	Nov 05, 2021, 09:28 AM	THrgSiee...m1ojiAUM	TQn9Y2kh...w5KcblSE (SunSwap)	294,394.827 USDT	60e5b0a9...aa21f275

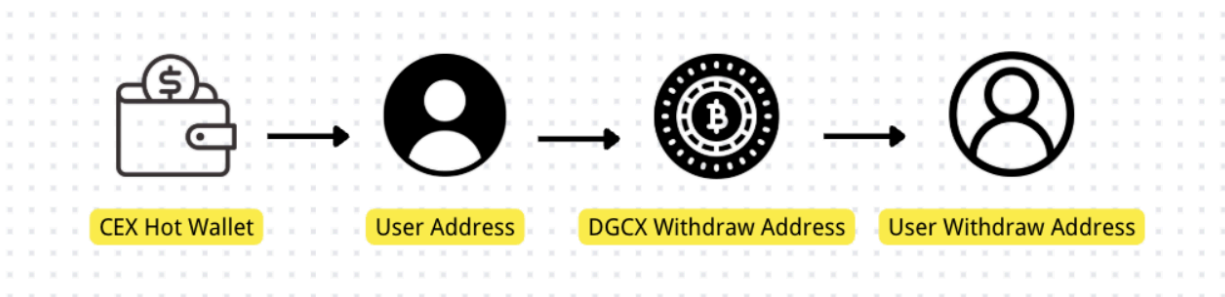
Export

That address then swapped TRX back into USDT to TECs2MpZN9HZH5noGzGTF8LBLhxZt5g41q via SunSwap, ultimately moving USDT to the "large address." Other addresses followed similar patterns.



In summary, the hackers repeatedly exchanged the stolen USDT back and forth to evade tracking. Despite the hackers' best efforts, we can still trace the hacker accounts through the exchange addresses involved, which we will not elaborate on here.

It's worth noting that, compared to these exchange-based money laundering schemes, some Ponzi schemes employ more crude methods. For example, typical Ponzi scheme platforms like Xinkangjia DGCX display a unique deposit address for each user on their user interface, but in reality, all addresses are managed by the platform. Once a user deposits, the funds first enter an intermediate address, undergo one or two simple transfers, and are then aggregated into the platform's "fund pool" address. From there, they are transferred to external, suspicious addresses through a series of frequently switching intermediate wallets. This type of absconding scheme is characterized by its uncomplicated structure, deliberately simplifying the process to quickly liquidate assets.



Phishing scenarios are somewhat different. Most phishing websites disguise themselves as official DApp or wallet authorization pages to trick users into authorizing transactions. Funds don't flow out through user transfers, but rather through the phishing contract itself. A common path

follows: the user authorizes an ERC20 contract, the phishing contract initiates operations like "transferFrom" to transfer funds to the attacker's wallet, the attacker rapidly withdraws the funds through multiple forwarding addresses, and the funds are laundered using a mixer or cross-chain bridge. When tracking this path, it's important to identify the authorization contract's permission boundaries, the transaction caller's address, and the subsequent flow of funds.

Attack paths in the DeFi context are even more complex, often combining smart contract vulnerabilities and flash loans to achieve arbitrage or manipulate market prices. For example, a project suffered a flash loan attack, where the attacker constructed multiple on-chain interactions, completing a series of on-chain operations—including borrowing, price manipulation, asset arbitrage, and liquidation arbitrage—in a very short period of time. Once the attack was complete, the assets were quickly transferred to a wallet controlled by the attacker, then converted to a mainstream stablecoin via a decentralized exchange (DEX) before ultimately being transferred across chains or to an exchange. These cases involve dense on-chain activity and complex contract calls, requiring the use of graphical tracking tools and attention to technical details such as contract vulnerabilities underlying the attack logic.

Regardless of the scenario, reviewing transactions isn't just about looking at transfer charts; it's about identifying key nodes: At what point does control transfer? When do suspicious authorizations or contract interactions occur? Is there any involvement from a centralized platform? These insights not only influence the depth of the tracing process but also the likelihood of subsequent freezing and further investigations involving law enforcement agencies.

## 10. Recommendations for Asset Freezing and Recovery

When on-chain tracking confirms that a portion of stolen or fraudulent funds has entered centralized exchanges (CEXs), asset freezing and recovery become the next critical steps. However, in practice, this process is far more complex than it might appear, involving multiple factors such as legal procedures, the willingness of exchanges to cooperate, and cross-border enforcement mechanisms.

The first step is to identify inflows to exchanges. Using tools like MistTrack or blockchain explorers, analysts examine whether suspicious funds have ultimately entered CEX addresses,

typically relying on address labeling. Major exchanges such as Binance and Coinbase usually have distinctive deposit addresses, and their fund aggregation patterns tend to follow predictable behaviors. Analysts must consider upstream and downstream fund flows to avoid false positives from funds temporarily held in intermediary or OTC addresses.

If inflows to a CEX are confirmed, the next step is to initiate a freeze request. Most top-tier exchanges have security/compliance departments that handle freeze requests, but these usually must be submitted by a compliant entity, such as law enforcement with a case filing receipt and investigation letter, or a law firm submitting legal documentation on behalf of a client. Individual victims rarely have direct access to the exchange. It is recommended to prepare early, including evidence of the incident (transaction records, communication screenshots, details of affected amounts and addresses), on-chain tracking paths (annotated tracking diagrams), and proof of police reports. Cooperation with professional security firms (e.g., SlowMist) and law firms (e.g., JunHe, WINTAO, DENTONS, Man Kun, etc.) can facilitate communication with exchanges and increase the likelihood of a successful freeze.

It is important to emphasize that even if an exchange assists with freezing, this is only a temporary measure. Whether frozen assets can ultimately be recovered depends on subsequent legal processes, such as civil judgments, criminal investigations, or asset restitution procedures. These processes involve complex issues such as jurisdiction, asset identification, and compensation allocation. Therefore, “recovery” is not a direct extension of on-chain analysis but the result of coordinated action among legal, technical, and platform entities.

At the international level, freezing is even more challenging. On one hand, different countries/regions have vastly different legal interpretations regarding crypto assets; on the other hand, many funds eventually enter gray-market platforms that are either unregulated or uncooperative. Some exchanges operate in jurisdictions with lenient regulations and may not comply with freeze requests even if they hold the assets.

Therefore, we repeatedly emphasize: the role of on-chain tracking is to provide visibility, determine asset destinations, and assist in subsequent actions, but it cannot replace legal freezes nor guarantee fund recoverability. The key to freezing and recovery lies in early identification of fund

paths, possession of a complete evidence chain, and obtaining support from professional institutions and law enforcement.

SlowMist Case Experience: Freezing ≠ the endpoint; collaboration is key. In 2024, with strong support from InMist intelligence network partners, SlowMist assisted clients, partners, and publicly disclosed hack incidents in freezing over USD 112 million in funds. In 2025, SlowMist supported attorney Xiao Sa's team in successfully advancing the unfreezing process of an overseas freeze case, recovering approximately RMB 10 million in USDT for the client. In this case, the critical factor was the collaboration between the legal team and the security company, providing on-chain path analysis, comprehensive evidence chains, and multiple rounds of communication with foreign law enforcement agencies, ultimately facilitating asset restitution.

On-chain tracking is the foundation for identifying problems and clarifying direction, but true asset recovery requires a complete closed-loop of on-chain data analysis, offline legal procedures, and coordinated platform mechanisms. On-chain visibility ≠ controllability, much less recoverability; compliance-driven collaboration is the key. Recognizing this is a consensus every tracker must internalize.

## Conclusion

Throughout the tracking process, we have come to deeply understand that on-chain security is never a one-off task but a long-term and ongoing tug-of-war. Attackers continuously evolve their methods, from early simple on-chain transfers to today's multi-chain strategies leveraging mixers, flash loans, cross-chain bridges, automated arbitrage contracts, and even AI tools to disguise fund flows. The more sophisticated the adversary, the more complex the technology, experience, and tools required. True security depends on having enough analysts, researchers, media, and judicial personnel who continuously monitor, learn, and are willing to delve into cases to reconstruct complex paths and bridge the gap to the truth.

More importantly, we firmly believe that tracking is not merely for judicial service but also to raise public awareness — every exposure of fund flows undermines fraudsters' trust networks. Every readable and reusable case analysis serves as a shield for the community against the next scam.

Too often, victims lose not only technically but also due to information asymmetry. A clear, practical, and accessible tracking handbook may be the first step in addressing this asymmetry.

These contents represent the accumulated insights of the SlowMist team, based on years of on-chain tracking, practical experience, cross-chain monitoring, and case reconstruction. If this handbook helps even a single user avoid being scammed, guides a victim toward a solution, or accelerates the preparation of a case report, its value is fulfilled.

## Disclaimer

This handbook is intended for informational and educational purposes only, aimed at helping readers understand basic concepts, common techniques, and response strategies for crypto asset tracking. It does not constitute legal, investment, or enforcement advice. Tools, platforms, and protocols mentioned are provided solely for case analysis and technical illustration and are not endorsements or recommendations. All examples, scenarios, addresses, and behavioral analyses are based on publicly available information or simulations and are not targeted at any individual or organization, nor do they imply judgment or stance by the authors.

The crypto asset field is highly risky, and on-chain activity is complex and dynamic; tracking and analysis carry technical barriers and uncertainties. In practice, readers should exercise judgment based on their circumstances and seek professional legal, security, or compliance support as necessary. The authors of this handbook assume no responsibility for any direct or indirect losses resulting from the use of or reliance on the content herein.

## About SlowMist



SlowMist is a threat intelligence company focused on blockchain ecosystem security. Founded in January 2018, it was started by a team with over ten years of network security experience to become a global force. Our goal is to make the blockchain ecosystem as secure as possible for everyone. We are now a renowned international blockchain security firm that has worked on various well-known projects such as HashKey Exchange, OSL, MEEEX, BGE, BTCBOX, Bitget, BHEX.SG, OKX, Binance, HTX, Amber Group, Crypto.com, etc.

SlowMist offers a variety of services that include but are not limited to security audits, threat information, defense deployment, security consultants, and other security-related services. We also offer AML (Anti-money laundering) software, MistEye (Security Monitoring) , SlowMist Hacked (Crypto hack archives), FireWall.x (Smart contract firewall) and other SaaS products. We have partnerships with domestic and international firms such as Akamai, BitDefender, RC<sup>2</sup>, TianJi Partners, IPIP, etc. Our extensive work in cryptocurrency crime investigations has been cited by international organizations and government bodies, including the United Nations Security Council and the United Nations Office on Drugs and Crime.

By delivering a comprehensive security solution customized to individual projects, we can identify risks and prevent them from occurring. Our team was able to find and publish several high-risk blockchain security flaws. By doing so, we could spread awareness and raise the security standards in the blockchain ecosystem.

## SlowMist Security Solutions

### Security Services



#### **Exchange Security Audits**

Full range of black box and gray box security audits, going beyond penetration testing



#### **Wallet Security Audits**

Full range of black box and gray box security audits, going beyond penetration testing



#### **Blockchain Security Audits**

Comprehensive audit of key vulnerabilities in Blockchain and consensus security



#### **Smart Contract Audits**

comprehensive white box security audit of source code related to smart contracts



#### **Consortium Blockchain Security Solutions**

Services include but not limited to security design, audits, monitoring and management



#### **Red Teaming**

Penetration testing and evaluating vulnerable points



#### **Security Monitoring**

Dynamic security monitoring for all possible vulnerabilities



#### **Blockchain Threat Intelligence**

Joint defense system with integrated on-chain and off-chain security governance



#### **Defense Deployment**

Deploying Defense Solutions Tailored to Local Conditions, Implementing Hot Wallet Security Strengthening



#### **MistTrack Tracking Service**

Digital assets were unfortunately stolen, MistTrack saves a glimmer of hope





### **Incident Response Service**

Aiming to help Web3 projects quickly and effectively respond to security incidents and threats



### **Security Consulting**

Provide technical, risk management, and emergency response support as well as providing recommendations to improve them



### **Hacking Time**

Annual close-door training focusing on blockchain security



### **Digital Asset Security Solution**

Open source digital asset security solutions

## Security Products



### **SlowMist AML**

Promoting the compliance, security, and healthy development of the web3 industry



### **MistTrack**

A crypto tracking and compliance platform for everyone



### **MistEye**

Provide comprehensive web3 threat intelligence and dynamic security monitoring services for everyone



### **SlowMist Hack**

A comprehensive repository of blockchain incidents



### **False Deposit Vulnerability Scanner**

Creating safe deposit and withdrawals for trading platforms



### **Website**

<https://slowmist.com>

### **X**

[https://x.com/SlowMist\\_Team](https://x.com/SlowMist_Team)

### **Github**

<https://github.com/slowmist>

### **Medium**

<https://slowmist.medium.com>

### **Email**

[team@slowmist.com](mailto:team@slowmist.com)

### **Wechat**





Focusing on Blockchain Ecosystem Security