Tornado Cash Exposure Analysis & Laundering Flow Investigation

Project Overview

This case study examines Tornado Cash withdrawal activity and the subsequent tracing of laundering behaviour through intermediary wallet routing, clustering analysis, and downstream transaction flow assessment.

The investigation focused on identifying observable transaction continuity, structured withdrawal behaviour, fund dispersion patterns, and downstream routing into decentralized infrastructure following Tornado Cash interaction.

Wallet addresses and transaction identifiers have been partially masked in this public portfolio version for professional presentation and responsible disclosure considerations.

INVESTIGATION SUMMARY

Category	Details
Investigation Type	Tornado Cash Exposure Analysis & Laundering Flow Investigation
Network Reviewed	Ethereum
Primary Asset	ETH
Initial Observed Exposure	200 ETH
Cluster Exposure Reviewed	~7,369 ETH
Investigation Focus	Mixer Exposure & Laundering Flow Analysis
Downstream Routing	Non-Custodial / Decentralized Infrastructure

Key Observations

- Fixed denomination withdrawals identified
- Rapid downstream dispersion observed
- Intermediary wallet layering detected
- Cluster-linked exposure identified
- Decentralized routing behaviour observed

INVESTIGATION OBJECTIVES & DASHBOARD

Investigation Objectives

- Analyse Tornado Cash withdrawal behaviour
- Review intermediary wallet interactions
- Identify laundering flow continuity
- Assess clustering relationships
- Examine downstream routing behaviour
- Review behavioural transaction indicators
- Conduct exposure assessment
- Demonstrate structured blockchain investigation methodology

Investigation Dashboard

Mixer Interaction

Tornado Cash withdrawals identified

Withdrawal Pattern

Fixed-value 100 ETH withdrawals

Laundering Behaviour

Layering and rapid dispersion

Downstream Activity

Routing into decentralized infrastructure

Core Analytical Indicators

Clustering analysis, timing correlation, structured withdrawal behaviour, transaction continuity

Methodology:

The investigation applied transaction-level blockchain analysis, behavioural assessment, wallet clustering review, and downstream transaction tracing to reconstruct laundering behaviour following Tornado Cash interaction.

METHODOLOGY

Methodology Applied

- Tornado Cash withdrawal review
- Wallet interaction analysis
- Transaction continuity assessment
- Behavioural pattern analysis
- Clustering review
- Timing correlation analysis
- Layering behaviour identification
- Fund dispersion analysis
- Exposure assessment
- Manual transaction flow reconstruction

Tools & Platforms Referenced

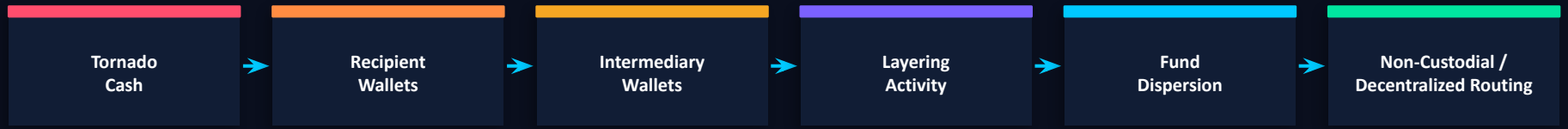
Tools referenced in this investigation varied depending on the transaction structure, clustering behaviour, and analytical requirements of the case.

Platforms Used

- Arkham Intelligence
- Breadcrumbs
- Etherscan
- Tornado Cash transaction review tools
- Ethereum transaction graph visualisation tools

TORNADO CASH EXPOSURE RECONSTRUCTION

The reconstructed transaction path begins from Tornado Cash withdrawal activity before progressing through intermediary wallet routing, layered fund dispersion, and downstream movement into decentralized infrastructure.



Masked Transaction Evidence

Type	Masked TXID	Recipient	Amount
Withdrawal 1	0xddbedd...0fc6ba	0xcfe379...cada0	100 ETH
Withdrawal 2	0xfedade...a51385	0xb86262...bfb03	100 ETH

Deposit Address Samples (Masked)

0x096f31...bb5C9 0x0aC426...3a2B 0x19428B...D723 0x1EeAa9...7F5e 0x2400A0...Bdc7

TRANSACTION FLOW ANALYSIS

Stage 1 — Tornado Cash Withdrawal Activity

Multiple fixed-value Tornado Cash withdrawals were identified involving 100 ETH withdrawal patterns into recipient wallets.

The structured denomination pattern demonstrated behaviour commonly associated with mixer-based laundering workflows.

Stage 2 — Recipient Wallet Activity

Following withdrawal activity, recipient wallets rapidly redistributed funds through intermediary transaction paths without prolonged holding behaviour.

The reviewed routing sequence indicated active laundering progression rather than passive storage activity.

Stage 3 — Layering Behaviour

Funds were dispersed across multiple intermediary wallets in a structured sequence designed to reduce direct transaction linkage visibility.

Observed behavioural indicators included:
· Rapid transaction sequencing
· Repeated routing behaviour
· Multi-wallet dispersion
· Layered transaction movement

TRANSACTION FLOW ANALYSIS (CONTINUED)

Stage 4 — Cluster Exposure Analysis

Additional wallet relationships identified through clustering review expanded the observed exposure from the initially visible 200 ETH to an estimated broader cluster exposure of approximately 7,369 ETH.

The clustering analysis demonstrated:
· Related wallet interaction behaviour
· Repeated transaction relationships
· Common downstream routing patterns
· Structured laundering continuity

Stage 5 — Downstream Decentralized Routing

Following intermediary layering activity, funds were routed into decentralized and non-custodial infrastructure rather than directly into centralized exchange deposit paths.

The reviewed routing behaviour demonstrated characteristics associated with:
· Decentralized transaction routing
· Non-custodial interaction
· Continued laundering dispersion activity

EVIDENCE ASSESSMENT — CORE EVIDENCE PILLARS

The analytical conclusion is supported through multiple independent indicators that collectively reinforce the laundering flow assessment.

Tornado Cash Interaction

Direct Tornado Cash withdrawal activity was identified as the initial laundering entry point.

Fixed Withdrawal Behaviour

Repeated fixed-value 100 ETH withdrawals demonstrated structured mixer withdrawal behaviour.

Rapid Fund Dispersion

Funds were redistributed rapidly following withdrawal activity, reducing direct trace continuity between recipient wallets.

Clustering Relationships

Wallet clustering analysis identified broader exposure relationships extending beyond the initially visible withdrawal amounts.

Decentralized Routing Behaviour

The downstream movement pattern demonstrated routing into decentralized infrastructure rather than immediate centralized exchange cash-out behaviour.

SCREENING & EXPOSURE REVIEW

Screening Observations

- Tornado Cash interaction confirmed
- Structured withdrawal behaviour observed
- Layered intermediary routing identified
- Decentralized routing activity detected
- Expanded cluster exposure identified

Behavioural Risk Indicators

Risk Indicator	Assessment
Tornado Cash Exposure	High
Fixed-Value Withdrawal Pattern	High
Layering Behaviour	High
Rapid Fund Dispersion	High
Decentralized Routing Activity	Medium
Cluster Exposure	High

Screenshots & Visual Evidence — Included Evidence Types

Blockchain explorer screenshots · Tornado Cash withdrawal visuals · Transaction flow graphs · Wallet interaction diagrams · Clustering analysis visuals · Layering flow mapping

Portfolio Safety Controls: masked wallet addresses · masked TXIDs · shortened visual identifiers · cropped screenshots where appropriate · reduced exposure of sensitive identifiers

INVESTIGATION SCOPE, LIMITATIONS & ANALYTICAL ASSESSMENT

Investigation Scope & Limitations

This investigation was conducted using publicly accessible blockchain data, wallet clustering analysis, transaction flow review, and open-source analytical techniques.

Wallet ownership, beneficial ownership, and downstream identity attribution could not be independently verified using public blockchain data alone.

No privileged exchange records, KYC-linked account information, or law-enforcement investigative access were available during the review.

Analytical findings are therefore based on:

- Observable transaction behaviour
- Tornado Cash interaction review
- Wallet clustering analysis
- Transaction continuity assessment
- Behavioural laundering indicators
- Downstream routing analysis

Analytical Assessment

The reviewed transaction behaviour demonstrated observable characteristics associated with structured laundering activity involving Tornado Cash withdrawals, intermediary wallet layering, fund dispersion, and decentralized routing behaviour.

The structured withdrawal denomination pattern, combined with rapid redistribution and cluster-linked transaction relationships, supports the analytical assessment that the reviewed wallets formed part of a broader laundering sequence rather than isolated unrelated activity.

CONCLUSION

Conclusion

The investigation supports a coherent linkage between Tornado Cash withdrawal activity, intermediary wallet layering behaviour, expanded cluster exposure, and downstream decentralized routing activity.

The reviewed transaction behaviour demonstrates structured laundering methodology involving Tornado Cash exposure followed by layered routing and downstream decentralized infrastructure interaction.

The case is strengthened through multiple analytical indicators, including:

- **Fixed-Value Withdrawal Behaviour**
- **Transaction Continuity**
- **Rapid Fund Dispersion**
- **Wallet Clustering Relationships**
- **Intermediary Routing Behaviour**
- **Decentralized Transaction Movement**

Recommended Next Steps

Based on the reconstructed transaction flow and identified clustering relationships, continued monitoring of the traced wallets and related intermediary addresses is recommended to identify any subsequent movement or additional linked transactions.

- Expansion of wallet cluster analysis
- Continued monitoring for centralized exchange interaction
- Review of additional downstream routing behaviour
- Preservation of transaction evidence and timeline records
- Sanctions and exposure screening updates
- Monitoring for re-entry into exchange infrastructure

Final Project Summary

This project demonstrates practical blockchain investigation methodology involving:

- **Tornado Cash Exposure Analysis**
- **Wallet Clustering Review**
- **Laundering Flow Reconstruction**
- **Intermediary Wallet Analysis**
- **Behavioural Transaction Assessment**
- **Decentralized Routing Review**
- **Structured AML-Focused Reporting**

The investigation combined blockchain analysis, clustering techniques, behavioural assessment, and transaction continuity review to reconstruct laundering activity following Tornado Cash interaction.