USDT Theft Flow Analysis & Exchange Deposit Review

Project Overview

This case study examines the theft of 100,042 USDT on the Ethereum network and the subsequent tracing of the funds through intermediary wallets, layered transaction movement, consolidation behaviour, and final routing into exchange-linked wallet infrastructure.

Unlike cross-chain laundering investigations or mixer-based obfuscation cases, this investigation demonstrates behavioural layering through wallet-to-wallet movement prior to exchange deposit activity.

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	USDT Theft Flow Analysis & Exchange Deposit Review
Network Reviewed	Ethereum (ERC-20)
Asset	Tether USD (USDT)
Total Amount Reviewed	100,042 USDT
Investigation Focus	Layering Behaviour & Exchange Routing Analysis
Observed Final Endpoints	Kraken-Linked Deposit Infrastructure

Key Observations

- Rapid intermediary wallet movement observed
- Structured transaction progression identified
- Validation transfer behaviour detected
- Consolidation routing identified before final exchange-linked movement
- Continuous transaction chain preserved on Ethereum

INVESTIGATION OBJECTIVES & DASHBOARD

Investigation Objectives

- Analyse stolen fund movement
- Review intermediary wallet routing behaviour
- Identify layering and structuring activity
- Assess transaction continuity
- Review consolidation behaviour
- Examine exchange-linked destination activity
- Conduct behavioural transaction analysis
- Demonstrate blockchain investigation methodology

Investigation Dashboard

Initial Theft Event

100,042 USDT transferred from source wallet

Primary Laundering Behaviour

Wallet-to-wallet layering

Key Transaction Indicator

Test transaction before main transfer

Final Observed Behaviour

Exchange-linked routing and aggregation

Core Analytical Indicators

Transaction continuity, timing alignment, consolidation patterns, and exchange clustering

Methodology:

The investigation applied transaction-level blockchain analysis, behavioural assessment, wallet interaction review, and exchange attribution analysis to reconstruct the movement of stolen funds across Ethereum wallet infrastructure.

METHODOLOGY

Methodology Applied

- Forward transaction tracing
- Wallet interaction analysis
- Behavioural pattern assessment
- Transaction continuity review
- Timestamp correlation analysis
- Layering behaviour identification
- Consolidation analysis
- Exchange clustering review
- Destination wallet grouping analysis
- Manual transaction flow reconstruction

Tools & Platforms Referenced

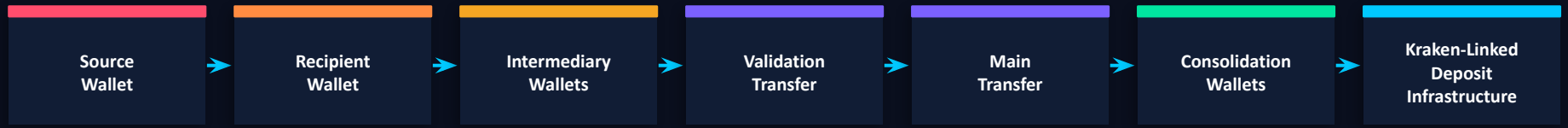
Tools referenced in this investigation varied depending on the transaction structure, wallet behaviour, and analytical requirements of the case.

Platforms Used

- Arkham Intelligence
- Breadcrumbs
- Etherscan
- OKLink
- Ethereum transaction graph visualisation tools

THEFT FLOW RECONSTRUCTION

The reconstructed transaction path begins from the initial theft event before progressing through intermediary wallet routing, layered transaction activity, consolidation stages, and eventual routing into Kraken-linked exchange infrastructure.



Transaction Flow Analysis — Stage Overview

Stage 1 — Initial Theft Event

100,042 USDT transferred from source wallet to recipient wallet on Ethereum. Origin point of the reviewed laundering sequence.

Stage 2 — Intermediary Wallet Routing

Funds rapidly moved through intermediary wallets without prolonged holding, indicating active transaction routing rather than passive storage.

Stage 3 — Structuring & Validation

Small validation transfer observed before larger transfer executed. Associated with destination verification, exchange deposit validation, and operational transfer confirmation.

TRANSACTION FLOW ANALYSIS

Stage 4 — Consolidation Behaviour

The traced funds were subsequently merged with additional inflows through intermediary aggregation wallets prior to final destination routing.

The observed consolidation pattern demonstrated:
· Layered routing behaviour
· Structured transfer sequencing
· Exchange-oriented transaction preparation

Stage 5 — Final Exchange Routing

The final destination wallets demonstrated characteristics commonly associated with centralized exchange-controlled infrastructure, including:
· High-volume aggregated inflows
· Repeated deposit activity
· Cluster-linked routing behaviour
· Structured wallet interaction patterns

The reviewed routing activity supported attribution to Kraken-linked deposit infrastructure.

Evidence Assessment

The analytical conclusion is supported through multiple independent indicators that collectively reinforce transaction continuity and exchange attribution assessment.

EVIDENCE ASSESSMENT — CORE EVIDENCE PILLARS

Continuous Transaction Chain

Funds remained traceable from the initial theft event through intermediary wallets into the final exchange-linked destination without transaction continuity breaks.

Validation Transfer Behaviour

A small transfer preceding the larger movement demonstrated behaviour commonly associated with exchange deposit testing or operational verification.

Consolidation Activity

The reviewed wallets demonstrated aggregation behaviour involving multiple inflows prior to final routing activity.

Exchange Clustering Indicators

Destination wallet behaviour demonstrated characteristics commonly associated with centralized exchange infrastructure rather than isolated personal wallet usage.

No Cross-Chain or Mixer Interaction

No bridge activity, mixer usage, or DeFi routing behaviour was identified during the reviewed transaction path. This preserved strong transaction continuity and evidentiary linkage throughout the investigation.

SCREENING & EXPOSURE REVIEW

Screening Observations

- No direct sanctions exposure identified during reviewed transaction flow
- Exchange-linked deposit behaviour observed
- Structured intermediary wallet movement identified
- Rapid sequential routing behaviour observed
- Consolidation activity identified prior to final deposit routing

Behavioural Risk Indicators

Risk Indicator	Assessment
Theft-Origin Transaction	High
Rapid Layering Behaviour	High
Validation Transfer Pattern	Medium
Exchange Deposit Routing	High
Consolidation Activity	Medium
Trace Continuity Strength	Low Analytical Uncertainty

Screenshots & Visual Evidence — Included Evidence Types

Blockchain explorer screenshots · Transaction flow graphs · Wallet interaction visuals · Layering sequence diagrams · Timeline evidence · Consolidation flow mapping

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

EXCHANGE ATTRIBUTION ANALYSIS

The final destination wallet cluster demonstrated several characteristics commonly associated with centralized exchange infrastructure.

High-Volume Aggregated Inflows

The destination wallets received multiple inflows consistent with exchange aggregation behaviour.

Structured Deposit Behaviour

The transaction sequence demonstrated operational patterns aligned with exchange deposit workflows.

Cluster Relationship Analysis

The reviewed wallets demonstrated linkage to broader exchange-controlled transaction infrastructure through repeated routing relationships.

Behavioural Consistency

The routing sequence aligned with observable exchange cash-out behaviour following intermediary laundering activity.

Based on transaction continuity, behavioural analysis, consolidation review, and wallet clustering observations, the reviewed destination infrastructure was attributed to Kraken-linked exchange activity.

INVESTIGATION SCOPE, LIMITATIONS & ANALYTICAL ASSESSMENT

Investigation Scope & Limitations

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

Wallet ownership, beneficial ownership, and custodial exchange account ownership 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
- Transaction continuity
- Wallet interaction analysis
- Exchange clustering indicators
- Consolidation behaviour
- Timing correlation
- Behavioural transaction assessment

Analytical Assessment

The reviewed transaction behaviour demonstrated observable characteristics associated with structured laundering activity involving intermediary wallet routing, rapid transaction sequencing, consolidation behaviour, and exchange-linked destination movement.

Although no mixer protocols or bridge infrastructure were used, the wallet-to-wallet layering behaviour created a form of behavioural obfuscation prior to final exchange routing.

The continuous Ethereum-based transaction chain preserved strong analytical linkage between:

- The initial theft event
- Intermediary wallet activity
- Consolidation stages
- Final exchange-linked deposits

CONCLUSION

Conclusion

The investigation supports a coherent end-to-end linkage between the initial theft event, intermediary wallet routing, consolidation behaviour, and the final Kraken-linked exchange deposit infrastructure.

The reviewed transaction behaviour demonstrates how layered wallet movement and consolidation can be used to obscure transaction origin even without mixer protocols, bridge infrastructure, or DeFi routing activity.

The case is strengthened through multiple analytical indicators, including:

- **Continuous Transaction Tracing**
- **Rapid Transfer Sequencing**
- **Validation Transfer Behaviour**
- **Consolidation Activity**
- **Exchange Clustering Indicators**
- **Uninterrupted Transaction Continuity**

Recommended Next Steps

Continued monitoring of traced wallets · Exchange outreach / lawful information requests · Wallet cluster analysis expansion · Screening against sanctions databases · Preservation of transaction evidence · Compliance review, legal escalation, or law-enforcement referral as appropriate

Final Project Summary

This project demonstrates practical blockchain investigation methodology involving:

- **Theft Flow Tracing**
- **Wallet Interaction Analysis**
- **Layering Behaviour Assessment**
- **Consolidation Review**
- **Exchange Attribution Analysis**
- **Behavioural Transaction Analysis**
- **Structured AML-Focused Reporting**

The investigation combined blockchain analysis, behavioural assessment, transaction continuity review, and evidence-based analytical techniques to reconstruct the laundering sequence from the initial theft event through exchange-linked destination routing.