Private Key Compromise & Multi-Chain Fund Flow Investigation

Project Overview

This case study examines a private key compromise incident involving unauthorized asset transfers across multiple blockchain environments, including BNB Chain, TRON, and Bitcoin network infrastructure.

The investigation reconstructed transaction continuity from the initial unauthorized wallet access through intermediary wallet movement, cross-chain conversion behaviour, stablecoin routing, aggregation activity, bridge interaction, and downstream Bitcoin peeling-chain movement.

The case demonstrates practical blockchain investigation methodology involving compromise-response tracing, cross-chain analysis, behavioural transaction assessment, and Bitcoin UTXO reconstruction.

Wallet addresses, transaction hashes, screenshots, bridge identifiers, and visual references have been partially masked in this public portfolio version for professional presentation and responsible disclosure considerations.

INVESTIGATION SUMMARY

Category	Details
Investigation Type	Private Key Compromise & Multi-Chain Fund Flow Investigation
Networks Reviewed	BNB Chain → TRON → Bitcoin
Assets Reviewed	BNB, USDT, BTC
Investigation Focus	Unauthorized Fund Movement & Cross-Chain Laundering Analysis
Observed Behaviour	Layering, bridge routing, aggregation, peeling-chain, Lightning Network, OKX consolidation
Final Status	Funds traced to OKX-associated hot wallet via Lightning Network & peel-chain routing

Key Observations

- Rapid wallet-draining activity identified
- Newly created intermediary wallets observed
- Cross-chain bridge interaction detected (BNB → TRON via Bridgers)
- Stablecoin conversion and aggregation behaviour identified (40,552 USDT consolidated)
- Bitcoin peeling-chain structure reconstructed (0.16777215 BTC repeated denomination outputs)
- Lightning Network interaction identified — Channel ID: 1042853793660534786 (LNBiG & Binance nodes)
- OKX-associated hot wallet consolidation identified — 8.78418058 BTC batch inflow

INVESTIGATION OBJECTIVES & DASHBOARD

Investigation Objectives

- Analyse unauthorized transaction movement following wallet compromise
- Review intermediary wallet forwarding behaviour
- Assess cross-chain bridge interaction activity (Bridgers infrastructure)
- Examine stablecoin conversion and TRON routing behaviour
- Analyse aggregation and consolidation patterns (Near Intent)
- Conduct Bitcoin peeling-chain analysis (UTXO reconstruction)
- Identify Lightning Network interaction and channel attribution
- Identify downstream exchange consolidation (OKX hot wallet exposure)
- Demonstrate structured blockchain investigation methodology

Investigation Dashboard

Initial Incident
Private key compromise suspected

Unauthorized Activity
Immediate outbound wallet draining identified

Layering Behaviour
Intermediary forwarding wallets observed

Cross-Chain Activity
BNB → TRON bridge routing identified (Bridgers)

TRON Aggregation
USDT consolidated — 40,552 USDT (Near Intent swap)

Bitcoin Activity
Structured BTC peeling-chain behaviour identified

Lightning Network
Channel 1042853793660534786 — LNBiG [Hub-2] & Binance

Final Destination
OKX hot wallet consolidation — 8.78418058 BTC batch

Methodology: Blockchain tracing, bridge analysis, wallet interaction review, stablecoin flow, Bitcoin UTXO, Lightning Network & exchange exposure analysis.

METHODOLOGY

Methodology Applied

- Unauthorized transaction tracing
- Wallet interaction analysis
- Cross-chain bridge review
- Stablecoin routing analysis
- Fund consolidation assessment
- Timestamp correlation
- Behavioural transaction analysis
- Bitcoin UTXO tracing
- Peeling-chain analysis
- Aggregation behaviour review
- Manual transaction flow reconstruction

Tools & Platforms Referenced

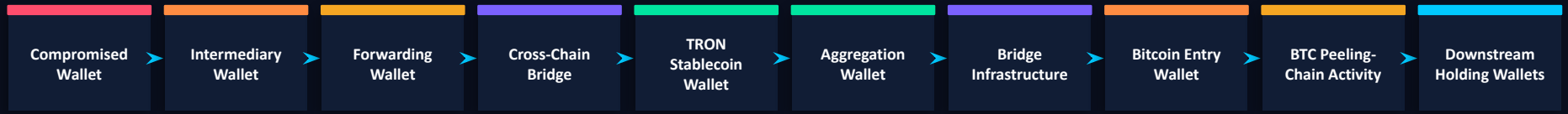
Tools referenced in this investigation varied depending on the blockchain network and analytical requirements of the case.

Platforms Used

- BscScan
- TronScan
- Blockchain.com Explorer
- Mempool.space
- Bridge transaction explorers
- Arkham Intelligence
- Breadcrumbs
- OKLink
- Bitcoin transaction graph visualisation tools

MULTI-CHAIN TRANSACTION RECONSTRUCTION

The reconstructed transaction sequence begins from the compromised wallet before progressing through intermediary wallets, bridge infrastructure, TRON-based stablecoin routing, aggregation behaviour, and downstream Bitcoin peeling-chain movement.



Masked Transaction References

Type	Masked TXID	Status
Initial Unauthorized Transfer	`0x91ab3d...f72c81`	Confirmed
Bridge Transaction	`0x4ec7a1...91dd52`	Confirmed
Stablecoin Routing	`7f3ad8...d119e0`	Confirmed
BTC Transfer	`a91d72...4e88bc`	Confirmed

Masked Wallet References

Wallet Type	Masked Address
Compromised Wallet	`0x8d20Eb...E0D479`
Intermediary Wallet	`0x41fd82...9f7A12`
TRON Wallet	`TNac9nV...HemJ`
BTC Wallet	`bc1qxy2k...f4k9`

TRANSACTION FLOW ANALYSIS — STAGES 1–4

Stage 1 — Initial Unauthorized Wallet Activity

The investigation identified unauthorized outbound transfers originating from the compromised wallet shortly after the suspected private key exposure event.

Key Findings

- Immediate wallet-draining behaviour observed
- Newly created recipient wallets identified
- No prior meaningful wallet history detected

Assessment: The rapid outbound transaction behaviour demonstrated characteristics commonly associated with automated compromise exploitation and operational laundering preparation.

Stage 2 — Intermediary Forwarding Activity

The compromised funds were subsequently forwarded through additional intermediary wallets before cross-chain routing activity.

Key Findings

- Sequential forwarding behaviour observed
- Minimal holding duration identified
- Layered transaction routing detected

Assessment: The reviewed forwarding sequence demonstrated structured intermediary separation designed to reduce direct trace continuity from the compromised source wallet.

Stage 3 — Cross-Chain Bridge Interaction

The investigation identified bridge activity converting BNB-chain assets into TRON-based stablecoin infrastructure.

Key Findings

- BNB routed into bridge infrastructure
- Stablecoin conversion identified
- TRON destination wallet activity observed

Assessment: The bridge interaction represented a laundering transition point enabling movement between blockchain ecosystems and increasing tracing complexity.

Stage 4 — TRON Stablecoin Routing

Following bridge conversion, the funds were routed through TRON-based stablecoin wallets before further downstream movement.

Key Findings

- Stablecoin receipt activity identified
- Structured routing behaviour observed
- Additional intermediary movement detected

Assessment: The use of TRON stablecoin routing supported rapid low-cost movement and subsequent aggregation behaviour.

TRANSACTION FLOW ANALYSIS — STAGES 5–8

Stage 5 — Aggregation & Consolidation Behaviour

The investigation identified consolidation behaviour involving aggregation of multiple inflows into centralized wallet infrastructure.

Key Findings

- Multi-inflow aggregation identified
- Consolidated balances observed
- Structured routing sequence detected

Assessment: The reviewed aggregation behaviour demonstrated operational consolidation patterns commonly associated with laundering workflows involving staged routing and pooled liquidity handling.

Stage 6 — Bitcoin Entry Routing

Following stablecoin routing activity, the funds were bridged into Bitcoin network infrastructure.

Key Findings

- Bitcoin entry wallet identified
- Stablecoin-to-BTC conversion behaviour observed
- Downstream UTXO routing initiated

Assessment: The Bitcoin transition introduced a UTXO-based tracing environment involving peeling-chain reconstruction and downstream transaction analysis.

Stage 7 — Bitcoin Peeling-Chain Analysis

The investigation identified structured Bitcoin peeling-chain behaviour involving sequential partial transfers across multiple wallets.

Key Findings

- Repeated output splitting observed
- Sequential downstream transfers identified
- Residual balance retention behaviour observed
- Multiple intermediary UTXO transitions detected

Assessment: The observed Bitcoin transaction structure demonstrated characteristics commonly associated with peeling-chain laundering methodology designed to incrementally distribute and obscure transaction flow continuity.

Stage 8 — Final Holding Wallets

The final observed routing stage involved multiple downstream Bitcoin holding wallets retaining unspent balances.

Key Findings

- Multiple downstream holding wallets identified
- Residual BTC balances remained unspent
- No confirmed centralized exchange interaction observed during reviewed flow

Assessment: The retained balances suggest temporary storage or delayed cash-out behaviour pending future movement.

TRANSACTION FLOW ANALYSIS — STAGES 9–10

Stage 9 — Lightning Network Interaction

One downstream BTC output (from peel-chain wallet bc1p8sf...r9x6j) was routed into active Lightning Network infrastructure on 08 May 2026.

Transaction Detail

TXID (masked): 6dba3b...0ac7f
Timestamp: 08 May 2026, 14:51:50 UTC
From (masked): bc1p8s...rr9x6j
To: Channel ID: 1042853793660534786
Amount: 0.16339151 BTC (~$13,010)
Channel Status: Active / Open

Lightning Channel Nodes

Node 1: LNBiG [Hub-2]
PubKey (masked): 033e9c...15b9c7
Node 2: Binance
PubKey (masked): 03a1f3...d6a72f
Channel ID: 1042853793660534786
Explorer: lightningnetwork.plus

Assessment:
Interaction with LNBiG [Hub-2] / Binance routing infrastructure indicates potential attempt to obscure final settlement destination.

Stage 10 — OKX Exchange Consolidation

A traced BTC input was identified within a larger OKX-associated consolidation batch on 12 May 2026, indicating likely exchange deposit activity.

Transaction Detail

TXID (masked): db91d4...d5a0a
Timestamp: 12 May 2026, 03:55:06 UTC
From (masked): bc1pp8...qsnqe9
To (masked): bc1quh...0r8l2d
Amount: 0.15603931 BTC (~$12,400)
Batch Total Inflow: 8.78418058 BTC (multiple inputs)

Key Findings

- Traced input consolidated into OKX-associated hot wallet
- Batch of 8.78 BTC collected from multiple wallets
- Transaction pattern and amounts suggest common controller
- High probability all upstream wallets operated by same actor
- Exchange deposit behaviour suggests imminent cash-out attempt
- OKLink explorer confirms OKX wallet attribution

Assessment:
OKX consolidation batch represents the strongest identified exchange exposure — transaction structuring implies coordinated multi-wallet control.

COMPLETE TRANSACTION REFERENCE — STAGES 9–10

Detailed transaction records for Lightning Network interaction and OKX consolidation stages. All wallet addresses partially masked.

Stage	Timestamp (UTC)	From (Masked)	To (Masked)	Asset	Amount (BTC / USD)	Notes
S9	08 May 2026 14:51:50 UTC	bc1p8s...rr9x6j	Channel ID: 1042853793660534786	BTC	0.16339151 ~$13,010	Lightning ch. Active/Open; LNBiG [Hub-2] & Binance routing
S10a	08 May 2026 06:37:16 UTC	bc1qfw...lekkjg	bc1q8m...lf6de3	BTC	0.15604055 ~$12,400	Intermediate hop — pre-OKX routing wallet
S10b	08 May 2026 06:40:20 UTC	bc1q8m...lf6de3	bc1pp8...qsnqe9	BTC	0.15603931 ~$12,400	Direct pre-OKX wallet; confirmed via OKLink
S10c	12 May 2026 03:55:06 UTC	bc1pp8...qsnqe9	bc1quh...0r8l2d	BTC	0.15603931 ~$12,400	OKX Hot Wallet — batch inflow 8.78418058 BTC (multi-input)

OKX Consolidation Exposure Note:

The OKX-associated destination wallet received 8.78418058 BTC from multiple inputs. Transaction structuring and amounts strongly suggest common operational control across upstream wallets. Further exchange cooperation may confirm identity attribution.

EVIDENCE ASSESSMENT — CORE EVIDENCE PILLARS

The analytical conclusions are supported through multiple independent indicators identified across all reviewed blockchain environments.

Continuous Multi-Chain Transaction Flow

Transaction continuity was preserved across: BNB Chain, bridge infrastructure, TRON stablecoin routing, and Bitcoin network movement.

Layered Routing Behaviour

Multiple intermediary wallets introduced operational separation between: compromised wallet activity, bridge routing, aggregation behaviour, and Bitcoin movement.

Stablecoin Aggregation Activity

TRON-based stablecoin routing demonstrated structured consolidation and pooled transaction behaviour prior to Bitcoin conversion.

Bitcoin Peeling-Chain Behaviour

The Bitcoin transaction structure demonstrated sequential UTXO peeling patterns involving: repeated transfers, partial residual retention, and downstream wallet propagation.

SCREENING & EXPOSURE REVIEW

Screening Observations

- Cross-chain bridge interaction identified (BNB → TRON via Bridgers)
- Stablecoin aggregation behaviour observed (40,552 USDT consolidated)
- Multi-stage layering activity detected across BSC, TRON and Bitcoin
- Bitcoin peeling-chain methodology identified (0.16777215 BTC denominations)
- Multiple downstream holding-wallet relationships observed
- Lightning Network interaction identified — Channel ID: 1042853793660534786
- OKX-associated hot wallet consolidation identified (8.78418058 BTC batch)

Behavioural Risk Indicators

Risk Indicator	Assessment
Private Key Compromise Behaviour	High
Intermediary Wallet Layering	High
Cross-Chain Laundering Activity	High
Bridge Infrastructure Usage	High
Bitcoin Peeling-Chain Behaviour	High
Lightning Network Interaction	High
OKX Exchange Consolidation	High
Residual Holding Wallet Structure	Medium

Screenshots & Visual Evidence — Included Evidence Types

Blockchain explorer screenshots · Cross-chain bridge confirmations · Wallet interaction diagrams · Transaction timeline visuals
Bitcoin UTXO flow diagrams · Peeling-chain mapping visuals · Aggregation flow structures · Lightning channel interaction evidence

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

INVESTIGATION SCOPE, LIMITATIONS & ANALYTICAL ASSESSMENT

Investigation Scope & Limitations

This investigation was conducted using publicly accessible blockchain data, bridge transaction analysis, wallet interaction 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
- Transaction continuity across all networks
- Cross-chain routing analysis
- Bridge interaction review
- Stablecoin aggregation behaviour
- Bitcoin UTXO analysis
- Peeling-chain assessment
- Lightning Network channel analysis
- Exchange consolidation exposure review

Analytical Assessment

The reviewed activity demonstrated a structured multi-chain laundering sequence following a suspected private key compromise involving:

- Intermediary wallet layering
- Bridge infrastructure usage (Bridgers — BNB to TRON)
- Stablecoin routing and TRON-based aggregation
- Aggregation behaviour (40,552 USDT consolidated)
- Bitcoin peeling-chain movement (0.16777215 BTC denominations)
- Downstream holding-wallet retention
- Lightning Network interaction (Channel ID: 1042853793660534786)
- OKX-associated exchange consolidation (8.78418058 BTC batch)

The cross-chain transitions significantly increased tracing complexity while preserving sufficient transaction continuity for behavioural reconstruction across all networks.

The OKX exchange consolidation represents the strongest identified cash-out exposure indicator identified during the investigation.

CONCLUSION

Conclusion

The investigation successfully reconstructed transaction continuity across multiple blockchain networks and identified behavioural indicators associated with layered laundering activity and structured fund movement following a suspected private key compromise.

The case demonstrates how compromised digital assets can be routed through multiple blockchain ecosystems and structured transaction methodologies to increase tracing complexity while preserving operational liquidity movement.

The reviewed activity demonstrated:

- Rapid Wallet-Draining Behaviour
- Intermediary Wallet Separation
- Bridge-Enabled Cross-Chain Routing
- Stablecoin Aggregation Behaviour
- Bitcoin Peeling-Chain Methodology
- Lightning Network Interaction
- OKX Exchange Consolidation Exposure
- Downstream Holding-Wallet Retention

Recommended Next Steps

Based on the reconstructed transaction flow, continued monitoring of associated wallets and intermediary infrastructure is recommended.

- Ongoing Bitcoin wallet monitoring
- Expansion of peeling-chain analysis
- Monitoring for further Lightning Network channel activity
- Review of future bridge-routing behaviour
- Submit exchange cooperation request to OKX for KYC attribution
- Preservation of transaction evidence and timeline records
- Continued sanctions and exposure screening

Final Project Summary

This project demonstrates practical blockchain investigation methodology involving:

- Compromise-Response Tracing
- Multi-Chain Analysis
- Bridge Transaction Review
- Stablecoin Routing Assessment
- Wallet Interaction Analysis
- Bitcoin UTXO Tracing
- Peeling-Chain Reconstruction
- Behavioural Transaction Analysis
- Structured AML-Focused Reporting

The investigation combined blockchain analysis, cross-chain tracing, behavioural assessment, and Bitcoin transaction reconstruction techniques to map the movement of compromised funds across multiple blockchain ecosystems.