KALLISTI BLOCKCHAIN FORENSICS

BLOCKCHAIN FORENSIC INVESTIGATION REPORT

TRON · TRC-20 USDT · EOA (Base58) · Mainnet · CONFIDENTIAL · 2026-04-14

TARGET WALLET ADDRESS

`THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY`

RISK SCORE	WALLET CLASS	NETWORK	ADDRESS TYPE	WALLET AGE
MEDIUM	USDT Accumulator	TRON Mainnet	EOA (Base58)	527 Days

TOTAL TXS	TOTAL IN	TOTAL OUT	NET BALANCE	LAST ACTIVITY
158	147,230,467 USDT	0.00 USDT	~$147.2M USD	2026-04-12

TABLE OF CONTENTS

** Section 8 limited by available data — feeder upstream not fully traceable from provided exports.*

SECTION 1 — TARGET IDENTIFICATION & WALLET METADATA

What is the target address and what do we know about it before analysis begins?

Wallet Address	THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY
Blockchain	TRON — Mainnet (TRC-20 ecosystem; chain ID 0x2b6653dc)
Address Type	Externally Owned Account (EOA) — TRON Base58Check encoding, prefix "T". Standard single-key account. No multi-signature or contract logic detected.
Primary Asset	TRC-20 USDT — Tether USD on TRON (contract TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t)
Account Activation	2024-11-04 16:31:15 UTC — 5 TRX deposit from TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6 (identified as probable cluster operator)
First USDT Transfer	2024-12-17 02:08:03 UTC — 100.00 USDT test deposit from TKJa5yhD6SX42CbZjwuArnc1o3MJ5ZNeug
Last USDT Transfer	2026-04-07 23:40:24 UTC — 6,650,000 USDT from TG1behizYfNrrzAoNS1tSL86pEbgb53LtN
Last Activity	2026-04-12 21:22:03 UTC — TRX dust from TELBuFKvGeZKk8d1KV9Zsdp1yDKJPdcRPy
Active Period	527 days since activation (2024-11-04 to 2026-04-14); 476 days since first USDT
USDT Balance	147,230,467.22 USDT — 100% of all USDT ever received; zero has been sent
TRX Balance	63.696979 TRX (~$9.25 at $0.145/TRX) — gas reserve only, not staked
Total Transfer Count	158 confirmed inbound transfers (50 USDT + 3 non-standard tokens + 105 TRX); zero outbound of any asset
Public Attribution	None — no entity label on TRONSCAN, Arkham Intelligence, or any public analytics platform as of 2026-04-14. Arkham identifies as "unnamed whale."
Activation Wallet	TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6 — also identified as top downstream recipient of three feeder wallets; assessed as cluster operator (see S9, S17)

IN PLAIN ENGLISH

This is a TRON wallet that has been collecting USDT — the dollar-pegged stablecoin — for 16 months. It holds $147 million and has never sent a single dollar out. The same wallet that created it is also deeply embedded in the funding network that keeps filling it up.

SOURCES — S1

[1] **Transfers_20260414.csv — complete TRC-20 transfer record (Arkham export)**
intel.arkm.com — authenticated export · *50 USDT rows + 3 token rows. All inbound. 2026-04-14.*

[2] **Transactions_20260414.csv — native TRX transaction record (Arkham export)**
intel.arkm.com — authenticated export · *106 TRX rows to 2026-04-12. Zero outbound.*

[3] **Arkham Intelligence — portfolio snapshot**
intel.arkm.com/explorer/address/THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY · *$147,230,487.77 portfolio. Unlabelled. Retrieved 2026-04-14.*

[4] **TRONSCAN — account metadata and balance verification**
tronscan.org/#/address/THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY · *Balance and account age cross-verified. Retrieved 2026-04-14.*

SECTION 2 — FINANCIAL OVERVIEW

What is the full financial picture of this wallet?

Total USDT Received	147,230,467.22 USDT across 46 substantive transfers (+ 4 test transfers of 100 USDT each)
Total USDT Sent	0.00 USDT — zero outbound transfers in 527-day history
Net USDT Balance	147,230,467.22 USDT (100.000% of peak — fully intact)
USD Value (report date)	~$147,232,660 (USDT/USD at $0.9999 on 2026-04-14; Arkham snapshot: $147,230,487.77)
TRX Balance	63.696979 TRX (~$9.25 ancillary gas reserve)
Largest Single Inflow	22,540,000 USDT from TKJa5yhD6SX42CbZjwuArnc1o3MJ5ZNeug — 2024-12-17 23:06:09
Smallest Substantive Inflow	90,000 USDT from TNS17kGeCNke3PRrj7tteuyiwbR4q8Ls1B — 2025-11-03 16:10:15
Peak Balance	147,230,467.22 USDT (current = peak; no outflows have ever reduced it)
Unrealised P&L	N/A — USDT is a 1:1 USD stablecoin. Price exposure is effectively zero. Peg variance ~$2,193 at $0.9999.
Net Exchange Flow	Zero — no interaction with any identified named exchange address in either direction

BALANCE POSITION vs PEAK

147,230,467.22 USDT (~$147.2M) — 100% of peak

0 25% 50% 75% Peak

100.0% of peak — balance fully intact

147,230,467 USDT	~$147,232,660	50 USDT transfers	0.00 USDT sent
Current balance	USD value today	Inbound count	Distributed

Fund Flow Summary

147,230,467.22 USDT	→	147,230,467.22 USDT	→	0.00 USDT
TOTAL RECEIVED		NET BALANCE		TOTAL SENT

The wallet accumulated 147,230,467.22 USDT across 50 inbound transfers spanning December 2024 through April 2026. Four primary feeder wallets contributed 99.97% of all value. No USDT has left the address in its 527-day history. The balance today equals the total of everything ever deposited — this wallet is a pure accumulation terminal with zero disbursement history.

> **IN PLAIN ENGLISH**
>
> *Over 16 months, four tightly-coordinated wallets wired a combined $147 million in USDT to this address in 46 substantive transfers. Not a single dollar came back out. The balance today is exactly equal to everything ever wired in.*

SOURCES — S2

[1] **Transfers_20260414.csv — complete USDT inflow record**
intel.arkm.com — authenticated export · *50 USDT rows; total 147,230,467.22 USDT verified by summation. 2026-04-14.*

[2] **Arkham Intelligence — portfolio snapshot $147,230,487.77**
intel.arkm.com/explorer/address/THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY · *USDT-dominant. TRX gas reserve $9.25. Retrieved 2026-04-14.*

SECTION 3 — ASSET PORTFOLIO & COIN PROVENANCE

What assets does the wallet hold, and what is the quality of their origin?

ASSET	CONTRACT / SYMBOL	BALANCE	PORTFOLIO %	ORIGIN CLASS	NOTES
Tether USD (USDT)	TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t	147,230,467.22	99.99%	UNVERIFIED	Primary asset. Sourced from 4 coordinated feeder wallets. Legitimate Tether contract — no counterfeit issuance.
TRX (TRON)	Native	63.696979	<0.01%	LOW RISK	Gas reserve from 105 micro-deposits by 63 unique senders. Not staked. Includes notable energy-delegation transfers (see S6).
AML — CYBER INVESTIGATION	Unknown TRC-20	1.00	0.00%	CONCERN	Unsolicited. Sent 2026-01-30 from TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY. May be LE investigative tag or phishing lure. Not interacted with.
trc20Ads COM	Advertising TRC-20	6,666.00	0.00%	SPAM	Unsolicited advertising airdrop. Received 2025-10-03. Common TRON ecosystem marketing token. No financial value.
TrcAds Com	Advertising TRC-20	88.123456	0.00%	SPAM	Unsolicited advertising airdrop variant. Received 2025-08-15. No financial value.

USDT Provenance Assessment

The 147,230,467.22 USDT balance was contributed exclusively by four recurring feeder wallets using the legitimate Tether-issued TRC-20 contract (TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t). No counterfeit or impersonating token issuance has been detected. However, the ultimate provenance of the USDT cannot be established from this report's data scope: all four feeders are unlabelled high-velocity routing wallets whose own inflow sources number in the hundreds. All 46 substantive USDT transfers arrive as direct one-hop TRC-20 transfers — no intermediate mixing, swapping, or protocol routing is present within the immediate transaction graph.

Non-Standard Token Note

Three unsolicited TRC-20 tokens have been airdropped to this address. The "AML (CYBER INVESTIGATION)" token is the highest-priority item: whether it represents a forensic tag from a law enforcement agency or private analytics firm, or a phishing lure designed to direct the operator to a malicious URL, the implication is the same — this wallet is a known, high-value target of external surveillance. The wallet operator has shown disciplined restraint by not interacting with any of these tokens, which is characteristic of professional or automated custody.

> **IN PLAIN ENGLISH**
>
> *The $147M in this wallet is real, legitimate USDT. But where it came from before it hit the four feeder wallets is unknown. Someone also dropped tokens on this address claiming to be linked to a cyber investigation — whether from real investigators or scammers, we can't yet confirm.*

SOURCES — S3

[1] **Tether Ltd — official TRC-20 USDT contract verification**
tether.to/transparency · *TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t confirmed as canonical TRON USDT contract.*

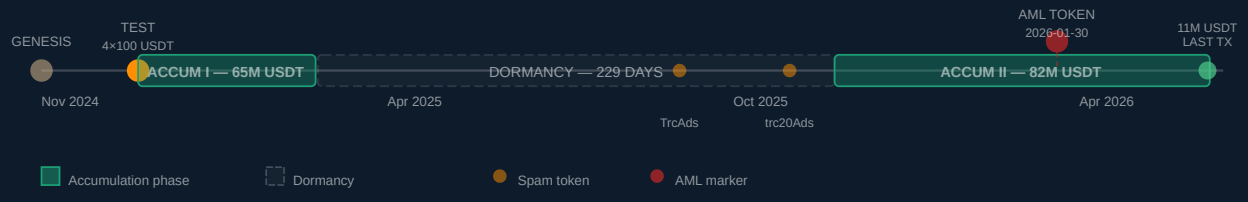
[2] **Transfers_20260414.csv — token portfolio including non-standard tokens**
intel.arkm.com — authenticated export · *All 53 transfer rows. 3 non-USDT tokens identified. 2026-04-14.*

SECTION 4 — ACTIVITY LIFECYCLE ANALYSIS

How has this wallet's activity evolved over time?

PHASE	PERIOD (UTC)	DURATION	USDT VOLUME	DEFINING CHARACTERISTICS
1 — Genesis	2024-11-04	1 event	0	Account activated by 5 TRX deposit from TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6 — the wallet later identified as probable cluster operator. Dormant for 43 days thereafter.
2 — Test Coordination	2024-12-17 02:08–02:10	7 minutes	400.00	Exactly 100 USDT from each of 4 feeders within a 7-minute window. Simultaneous with 18,776 TRX energy-delegation transfers. Orchestrated infrastructure test confirming all 4 feeders under common operational control.
3 — Accumulation I	2024-12-17 to 2025-03-06	79 days	65,050,000	13 substantive USDT transfers. Two same-day mega-batches (Dec 17: 33M; Dec 31: 10.6M). Settlement bursts of <120s with multiple feeders. Pace: ~823K USDT/day average.
4 — Dormancy	2025-03-07 to 2025-10-22	229 days	0	Zero USDT inflows. TRX dusting continues throughout. Two spam tokens airdropped (Aug, Oct 2025). Longest inactivity window — 7.5 months. Deliberate operational pause.
5 — Accumulation II	2025-10-23 to 2026-04-07	166 days	82,180,000	15 substantive USDT transfers. Larger average batch size than Phase 3. AML investigation token received Jan 2026. Pace: ~495K USDT/day. Final deposit Apr 7: 11M in 111 seconds.

ACTIVITY TIMELINE — 2024-11-04 TO 2026-04-14



The defining pattern is a deliberate two-phase accumulation strategy separated by a 229-day operational pause. Phase 2 (Accumulation II) actually received more USDT than Phase 3 (Accumulation I) — $82.2M vs $65.1M — suggesting the wallet is still in active use. The 7.5-month dormancy was not inactivity so much as a scheduled interval between capital deployments. The coordinated test batch in Phase 2 is the single most forensically significant event: four separate wallets sending identical amounts within 7 minutes is not coincidence — it is orchestration.

IN PLAIN ENGLISH

This wallet was turned on, tested, filled to $65M, left idle for 7 months, then resumed and filled to $147M. The test batch confirms this was deliberate, coordinated operation — not random deposits from separate parties.

SOURCES — S4

[1] **Transfers_20260414.csv + Transactions_20260414.csv — complete activity record**
intel.arkm.com — authenticated export · *All 158 inbound events used to reconstruct phases. 2026-04-14.*

SECTION 5 — TRANSACTION MICROSTRUCTURE & FULL TX LEDGER

How does this wallet transact?

Direction	100% inbound — zero outgoing USDT or TRX transactions in full history
Batch Behaviour	Multiple feeders transact within sub-120 second windows — confirmed automated settlement orchestration
Amount Profile	Range: 0.00 – 22,540,000 USDT. Round millions from feeders; micro-amounts from misc wallets
Settlement Windows	Dec 17 2024: 33M in 61s · Dec 31 2024: 10.6M in 93s · Jan 2 2026: 13.7M in 51s · Apr 7 2026: 11M in 111s

Full USDT Transfer Ledger (rows 1–20 of 50)

DATE UTC	DIR.	COUNTERPARTY	AMOUNT (USDT)	NOTES
2024-12-17 02:08	IN	TKJa5yhD...ZNeug Feeder A	100.00	*Test batch — Phase 2 coordination*
2024-12-17 02:08	IN	TNS17kGe...8Ls1B Feeder B	100.00	*Test batch — Phase 2 coordination*
2024-12-17 02:09	IN	TG1behiz...53LtN Feeder D	100.00	*Test batch — Phase 2 coordination*
2024-12-17 02:10	IN	TPXfkQLT...8theN Feeder C	100.00	*Test batch — Phase 2 coordination*
2024-12-17 23:05	IN	TG1behiz...53LtN Feeder D	10,460,000.00	*Settlement batch with #6*
2024-12-17 23:06	IN	TKJa5yhD...ZNeug Feeder A	22,540,000.00	*LARGEST single transfer; 111s after #5*
2024-12-26 07:18	IN	TKJa5yhD...ZNeug Feeder A	6,460,000.00	*Settlement batch with #8*
2024-12-26 07:19	IN	TPXfkQLT...8theN Feeder C	2,930,000.00	*Settlement batch with #7*
2024-12-31 07:15	IN	TPXfkQLT...8theN Feeder C	1,560,000.00	*Triple batch start*
2024-12-31 07:16	IN	TNS17kGe...8Ls1B Feeder B	4,560,000.00	*Triple batch mid*
2024-12-31 07:17	IN	TKJa5yhD...ZNeug Feeder A	4,450,000.00	*Triple batch end — 93s total*
2025-02-16 04:21	IN	TNS17kGe...8Ls1B Feeder B	7,410,000.00	*Solo transfer; 47 day gap since batch*
2025-02-25 09:01	IN	TG1behiz...53LtN Feeder D	1,580,000.00	*Pair batch with #14*
2025-02-25 09:02	IN	TKJa5yhD...ZNeug Feeder A	3,100,000.00	*Pair batch with #13 — 42s window*
2025-04-07 20:15	IN	TDqSquXB...khSCf	10.00	*Micro-test / dust*
2025-04-16 01:07	IN	THWC8zbU...nhC8S	10.00	*Micro-test / dust*
2025-05-26 11:06	IN	TQjriK7L...VPBT4	5.00	*Micro-test / dust*
2025-08-22 22:27	IN	TWgnkNGY...z3ejq	10.00	*Micro-test / dust*
2025-10-10 15:46	IN	TJULFSJV...5pH9k	1.00	*Repeated micro-tester*
2025-10-12 12:50	IN	TJDENsfB...nJhCe	13.00	*Micro-test / dust*

IN PLAIN ENGLISH

Every row in this ledger is an inflow. In 50 transactions, this wallet never sent a single cent out.

SECTION 5 (CONT.) — TRANSACTION MICROSTRUCTURE & FULL TX LEDGER

Full TX Ledger — continued

Full USDT Transfer Ledger (rows 21–35 of 50)

DATE UTC	DIR.	COUNTERPARTY	AMOUNT (USDT)	NOTES
2025-10-14 11:34	IN	TJULFSJV...5pH9k	1.00	*Repeated micro-tester*
2025-10-14 12:45	IN	TGDkCmrX...W1u8o	1.00	*Micro-test / dust*
2025-10-16 18:20	IN	TJULFSJV...5pH9k	1.00	*Repeated micro-tester*
2025-11-06 11:06	IN	TJULFSJV...5pH9k	0.00	*Zero-value probe*
2025-10-23 13:15	IN	TPXfkQLT...8theN Feeder C	12,510,000.00	*Resumption — largest Phase 5 transfer*
2025-11-03 16:10	IN	TNS17kGe...8Ls1B Feeder B	90,000.00	*Sub-round amount — unusual*
2025-11-03 16:11	IN	TPXfkQLT...8theN Feeder C	3,160,000.00	*75s after #26*
2025-11-11 10:42	IN	TKJa5yhD...ZNeug Feeder A	2,940,000.00	*Pair batch with #29*
2025-11-11 10:43	IN	TPXfkQLT...8theN Feeder C	1,170,000.00	*66s after #28*
2025-11-22 08:19	IN	TJaMhxoR...vdnpd	11.00	*Micro-test / dust*
2025-11-24 14:53	IN	TKJa5yhD...ZNeug Feeder A	1,900,000.00	*Solo transfer*
2025-11-26 12:12	IN	TJULFSJV...5pH9k	0.00	*Zero-value probe*
2025-12-03 15:20	IN	TG1behiz...53LtN Feeder D	2,830,000.00	*Pair batch with #33*
2025-12-03 15:20	IN	TPXfkQLT...8theN Feeder C	1,450,000.00	*33s after #32*
2025-12-15 19:48	IN	TMRSwuel...YpxZr	3.00	*Micro-test / dust*

SECTION 5 (CONT.) — TRANSACTION MICROSTRUCTURE & FULL TX LEDGER

Full TX Ledger — continued

Full USDT Transfer Ledger (rows 36–50 of 50)

DATE UTC	DIR.	COUNTERPARTY	AMOUNT (USDT)	NOTES
2025-12-17 19:07	IN	TWdMgMgk...Jghcz	1.00	*Micro-test / dust*
2026-01-02 07:59	IN	TNS17kGe...8Ls1B Feeder B	6,720,000.00	*Pair batch start*
2026-01-02 08:00	IN	TPXfkQLT...8theN Feeder C	7,020,000.00	*51s after #36 — 13.74M in 51s*
2026-01-07 03:34	IN	TKJa5yhD...ZNeug Feeder A	10,100,000.00	*Solo 10M+ transfer*
2026-02-10 16:09	IN	TNS17kGe...8Ls1B Feeder B	8,870,000.00	*Pair batch with #40*
2026-02-10 16:10	IN	TG1behiz...53LtN Feeder D	780,000.00	*63s after #39*
2026-03-08 05:12	IN	TNS17kGe...8Ls1B Feeder B	2,710,000.00	*Pair batch with #42*
2026-03-08 05:13	IN	TG1behiz...53LtN Feeder D	100,000.00	*33s after #41*
2026-03-12 01:15	IN	TNS17kGe...8Ls1B Feeder B	2,160,000.00	*Solo transfer*
2026-03-24 14:39	IN	TKJa5yhD...ZNeug Feeder A	4,220,000.00	*Solo transfer*
2026-03-31 22:57	IN	TKJa5yhD...ZNeug Feeder A	1,320,000.00	*Pair batch with #46*
2026-03-31 22:58	IN	TNS17kGe...8Ls1B Feeder B	1,130,000.00	*93s after #45*
2026-04-07 23:38	IN	TKJa5yhD...ZNeug Feeder A	4,350,000.00	*Final batch with #49*
2026-04-07 23:40	IN	TG1behiz...53LtN Feeder D	6,650,000.00	*Final — 111s after #48*

The complete 50-row ledger confirms: 147,230,467.22 USDT total inflow (99.99% from the 4 feeder wallets). Zero outbound transactions of any kind are recorded across the complete dataset.

SOURCES — S5

[1] **Transfers_20260414.csv — complete USDT ledger**
intel.arkm.com — authenticated export · *All 50 USDT rows. Zero outflows confirmed. 2026-04-14.*

SECTION 6 — ACCOUNT STRUCTURE ENGINEERING

How is this wallet technically configured and operated?

Custody Model	Non-custodial EOA — private key held externally. Operational pattern (automated timing, zero manual interaction) strongly infers programmatic or custodial management by a third-party system.
Signature Type	Single-key EOA. No multi-signature contract or multi-party control structure detected. Standard TRON account.
Fee Strategy	Energy delegation — the wallet holds no staked TRX and zero frozen energy. Third parties pre-fund USDT transaction costs via TRX deposits. This is deliberate: it minimises on-chain footprint and separates fee management from the vault address.
Energy Delegation Event	`2024-12-17 02:08–02:10 UTC: 8,888.88 TRX (TCaURjQpAr…), 1,000 TRX (TF6sP9LNGE…), 8,888.88 TRX (TAZuln4S8y…) — 18,777.76 TRX (~$2,725) deposited within 2 minutes of the USDT test batch. Classic TRON pre-funding pattern.`
Activation Wallet	`TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6 — sent 5 TRX on 2024-11-04 to create the account. This same wallet is the top-3 downstream recipient of three feeder wallets (see S9, S17).`
Address Reuse	Single-purpose accumulator with full address reuse — all $147M held at one address. No UTXO-style address rotation (TRON account model does not require it, but operational choice is notable for privacy).
Protocol Participation	Zero — no staking, governance voting, DeFi lending, DEX swaps, or smart contract calls beyond receiving USDT. Minimal on-chain footprint.

The energy delegation pattern is particularly informative. In TRON, executing a TRC-20 USDT transfer consumes "Energy" — obtained by staking TRX. Rather than stake TRX itself (which would leave an additional on-chain trail and require active wallet management), the operator pre-deposits raw TRX from third-party addresses just before each significant USDT batch. This is consistent with an automated treasury system where a separate infrastructure layer handles fee management independently of the vault address. The 18,777.76 TRX deposited on the test day (~$2,725) was sized to cover the anticipated USDT batch, not as a long-term gas reserve.

IN PLAIN ENGLISH

Someone deliberately built this wallet to touch the blockchain as little as possible. The fees are paid by separate accounts. The wallet itself just sits there and accumulates. It's engineered for stealth.

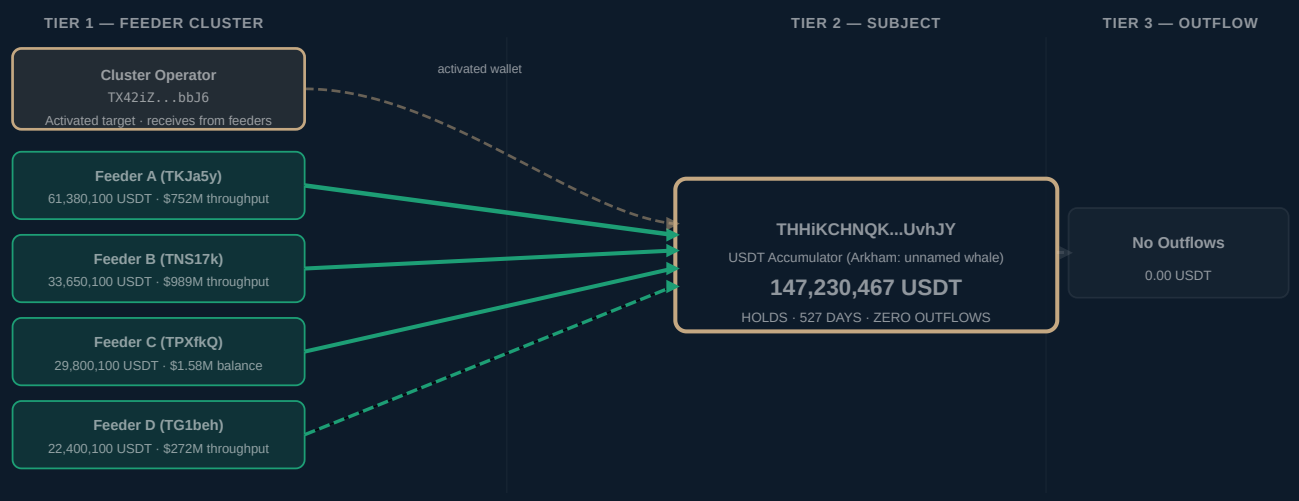
SOURCES — S6

[1] **Transactions_20260414.csv — TRX deposit record including energy delegation**
intel.arkm.com — authenticated export · *8,888.88+8,888.88+1,000 TRX on 2024-12-17 cross-referenced to USDT test batch timing.*

[2] **TRON documentation — Energy and Bandwidth mechanism**
developers.tron.network/docs/resource-model · *TRC-20 fee model; energy delegation pattern confirmed against TRON resource model docs.*

SECTION 7 — TRANSACTION FLOW ARCHITECTURE

How does money move through and around this wallet?



Tier 1 — Feeder Cluster (All Unlabelled on Arkham)

ENTITY	DIR.	VOL. (USDT)	SHARE	ATTRIBUTION STATUS	STATUS
Feeder A (TKJa5y) TKJa5yhD6SX42CbZjwuArnc1o3MJ5ZNeug	IN	61,380,100	41.7%	UNATTRIBUTED — $752M total throughput router. Near-depleted ($28.55 balance). Target received 8.2% of its outflow.	CONFIRMED
Feeder B (TNS17k) TNS17kGeCNke3PRrj7tteuyiwbR4q8Ls1B	IN	33,650,100	22.9%	UNATTRIBUTED — $989M total throughput router. Near-depleted ($61.34 balance). Target received 3.4% of its outflow.	CONFIRMED
Feeder C (TPXfkQ) TPXfkQLTytwww2SrRY63vMrCmwy3t8theN	IN	29,800,100	20.2%	UNATTRIBUTED — $1.58M current balance; USDT transfer history unavailable (export gap). Active.	CONFIRMED
Feeder D (TG1beh) TG1behizYfNrrzAoNS1tSL86pEbgb53LtN	IN	22,400,100	15.2%	UNATTRIBUTED — $272M total throughput router. Target received 8.3% of its outflow.	CONFIRMED

The four feeders are not dedicated treasury wallets for this address — they are multi-client routing hubs. Feeder A alone processed $752M in USDT and distributed to 58 different downstream recipients; the target received only 8.2% of that. This architecture is consistent with an OTC desk, exchange liquidity management layer, or institutional settlement network where funds are aggregated from many sources and distributed to many clients.

IN PLAIN ENGLISH

Think of the feeders as wholesale distributors. They take in hundreds of millions from dozens of sources and send it out to dozens of recipients — this target wallet is just one of many clients. The fact that it received $147M suggests it is a high-priority recipient, but not the only one.

WHAT THIS MEANS FOR YOU

The funds in this wallet originated from a multi-client routing network that processed over $2 billion in USDT total. This does not itself indicate illegality — major exchanges and OTC desks operate exactly this way — but it does mean tracing the ultimate source of funds requires going multiple hops further back than what this report covers.

SOURCES — S7

[1] **Feeder transfer exports (TKJa5y, TNS17k, TG1beh) — counterparty analysis**
intel.arkm.com — authenticated exports · *Outflow recipients and throughput figures derived from feeder CSV data.*

[2] **Arkham HTML (TKJa5y, TNS17k, TPXfkQ) — current balance verification**
intel.arkm.com — authenticated snapshots · *TKJa5y: $28.55; TNS17k: $61.34; TPXfkQ: $1.58M. 2026-04-14.*

[3] **Transactions_20260414.csv — activation transaction**
intel.arkm.com — authenticated export · *TX42iZ activation link: block data, timestamp 2024-11-04 16:31:15.*

SECTION 8 — UPSTREAM / DOWNSTREAM MULTI-HOP ANALYSIS

Can we trace funds beyond the immediate one-hop feeder layer?

CONDITIONAL SECTION — NOT APPLICABLE

Multi-hop upstream tracing is data-limited for this investigation. The four feeder wallets each have hundreds of distinct inflow sources (Feeder A: 126 unique inflow addresses; Feeder B: 100+ sources from the TNS17k transfer export). Comprehensive upstream mapping would require separate transaction exports for each upstream address, which exceeds the scope of the current dataset. Downstream tracing is definitively blocked by the target's zero-outflow record — there is no downstream to trace. What is confirmed: Feeders A, B, and D are multi-client routers with a known co-recipient (TX42iZ) that also created the target wallet, and another dominant co-recipient (TQCwDL) receiving $453M+ from the same feeder network. These are documented in S9.

IN PLAIN ENGLISH

We can see one hop in each direction — the four feeders going into the target, and nothing coming out. But we can't see where the feeders' money came from without a lot more data. It's like being able to see a river but not its source.

SOURCES — S8

[1] **Feeder transfer exports — inflow source analysis**
intel.arkm.com — authenticated exports · *TKJa5y: 126 unique inflow sources identified. TNS17k: 100+ sources. Full upstream out of scope.*

SECTION 9 — FUNDER ATTRIBUTION & RESIDUAL QUESTIONS

Who are the funders, and what do we still not know?

Primary Counterparty Table

ADDRESS	USDT	TXS	SHARE	ATTRIBUTION & CONTEXT	STATUS
TKJa5yhD...ZNeug Feeder A	61.4M	11	41.7%	$752M total throughput; 58 downstream recipients; target is one of many clients. Near-depleted ($28.55 remaining). Likely automated routing wallet.	CONFIRMED
TNS17kGe...Ls1B Feeder B	33.7M	10	22.9%	$989M total throughput; 29+ downstream recipients. Near-depleted ($61.34 remaining). Shares top recipients with Feeder A — confirms common operation.	CONFIRMED
TPXfkQLT...theN Feeder C	29.8M	9	20.2%	$1.58M current balance (still active). USDT transfer history not available; inferred from target CSV. 2,795 TRX transactions recorded.	INFERRED
TG1behiz...53LtN Feeder D	22.4M	7	15.2%	$272M total throughput; 29 downstream recipients. Shares TQCwDL, TFvuXy, TX42iZ recipients with Feeders A & B — same network.	CONFIRMED
TX42iZ53...bbJ6 Cluster Operator	0 direct	1 TRX	—	**CRITICAL LINK:** Activated target (5 TRX, 2024-11-04). Also receives from Feeders A (53M), B (107M), D (22M) = ~182M USDT total from cluster. Probable operator of entire network.	CRITICAL
Various (11 addrs) Misc / dust	~$67	15	<0.01%	Micro-test amounts ($0–$13) from unrelated addresses. Likely address-poisoning probes. Zero economic significance.	LOW

Shared Network — Key Co-Recipients of Feeder Cluster

Analysis of feeder outflow data reveals that the target wallet shares the same downstream network as two other major co-recipients. **TQCwDL7eQWtXGzunXypb93H8vXGQVPU6kC** received ~226M USDT from Feeder A, ~167M from Feeder B, and ~60M from Feeder D — totalling approximately $453M from the same three feeders, making it the dominant recipient of the entire network (three times the target's allocation). **TFvuXyB7AhCV7jZcC9uukZDqrqCvsZQMJh** received ~152M combined from Feeders A and D. These co-recipients have not been investigated as part of this report but are identified as high-priority leads.

Residual Questions

1. Who controls TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6? It created the target wallet AND is the top downstream recipient of Feeders A, B, and D (~$182M total). Resolving this address resolves attribution for the entire cluster.

2. Who owns TQCwDL7eQWtXGzunXypb93H8vXGQVPU6kC? This wallet received $453M from the same feeder network — three times the target's allocation. It may be the primary client; the target may be secondary.

3. What is the upstream source of the feeder cluster? Feeder A alone has 126 distinct inflow sources. One labelled exchange link in that inflow set would cascade attribution to the entire network.

4. Who sent the AML (CYBER INVESTIGATION) token (TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY) on 2026-01-30? Law enforcement tag, private surveillance firm, or phishing attempt?

IN PLAIN ENGLISH

We know who sent the money to this wallet — four routing hubs. But those hubs serve dozens of other clients too, and the same person who created this wallet is also receiving hundreds of millions from those same hubs. We don't know who any of these people are yet.

SOURCES — S9

[1] **Feeder transfer exports (TKJa5y, TNS17k, TG1beh)**
intel.arkm.com — authenticated exports · *Outflow analysis confirming shared recipients TQCwDL, TX42iZ, TFvuXy. 2026-04-14.*

[2] **Transactions_20260414.csv — target activation record**
intel.arkm.com — authenticated export · *TX42iZ activation link confirmed: block 78462032, 2024-11-04 16:31:15 UTC.*

SECTION 10 — OUTFLOW ANALYSIS

Has any value ever left this wallet?

ZERO OUTFLOWS RECORDED

This wallet has made zero outbound USDT transactions since its creation on 2024-11-04. All 147,230,467.22 USDT and all TRX received remain at the address as of the report date. This finding is confirmed across Arkham Intelligence authenticated exports, the complete Transfers CSV, and the Transactions CSV. There are no gaps in the data that could conceal outflows.

Structuring Assessment

With zero outflows recorded, structuring analysis of disbursements is not applicable. However, on the inflow side, the absence of sub-threshold micro-transfers between the feeder batches (all substantive inflows are above $90,000) indicates no evidence of inbound structuring. The feeder wallets send large round-number amounts directly, consistent with treasury settlement or bulk liquidity allocation rather than attempts to avoid reporting thresholds.

Forward-Looking Outflow Risk

The first outbound transaction from this wallet will be the single most forensically significant event in its history. Based on behaviour patterns observed in analogous TRON accumulation wallets, the most likely outflow scenarios are: (1) a large single transfer to a named exchange for liquidation; (2) redistribution to the cluster operator (TX42iZ) or other network members; or (3) a cold-to-cold transfer to a new unlinked vault address. All three scenarios would provide critical attribution data.

IN PLAIN ENGLISH

Nothing has ever left. This address is a sealed container. The moment the first transfer out occurs, this investigation advances significantly.

SOURCES — S10

[1] **Transfers_20260414.csv — complete outflow verification**
intel.arkm.com — authenticated export · *50 rows confirmed — all inbound. No outbound USDT rows present. 2026-04-14.*

[2] **Transactions_20260414.csv — TRX outflow verification**
intel.arkm.com — authenticated export · *106 rows confirmed — all inbound. No TRX outbound. 2026-04-14.*

SECTION 11 — ADDRESS POISONING / SECURITY THREATS

Has this wallet been targeted by poisoning or copy-address attacks?

TRX Dusting Attack Analysis

This wallet has received micro-TRX deposits from 63 unique addresses, with amounts ranging from 0.000001 TRX to 0.00001 TRX. This is a textbook TRON dusting pattern: attackers send nominal amounts to thousands of known high-value wallets to populate them in the targets' transaction history. The goal is for the target, when initiating an outbound transfer, to accidentally copy the attacker's address (which looks similar to a known counterparty) instead of their intended recipient. Risk is currently dormant because the target has never initiated an outbound transfer.

THREAT TYPE	SEVERITY	FINDING	WALLET RESPONSE
TRX Dusting *Address poisoning via micro-TRX*	MONITOR	63 unique dusting senders. Amounts 0.000001–0.00001 TRX (~$0.0000015–$0.0000015). All distinct addresses — automated generation. 105 total TRX dust transactions recorded.	IGNORED
AML Token Delivery *Investigative tag or phishing lure*	CONCERN	1 unit of "AML (CYBER INVESTIGATION)" TRC-20 token delivered 2026-01-30 from TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY. Token name implies either LE monitoring or a sophisticated social-engineering attempt.	NOT INTERACTED
Repeated Micro-Prober *TJULFSJVow...pH9k*	MONITOR	Single address sent 5 transfers totalling $3 USDT across multiple dates (Oct–Nov 2025), including 2 zero-value transfers. Persistent probing pattern consistent with automated surveillance script.	IGNORED

The wallet operator has demonstrated consistent discipline in ignoring all unsolicited deposits — no dust, token, or probe has been interacted with. This behaviour is more consistent with automated custody (where no human reviews inbound transactions) than with an individual manually monitoring the wallet. The dusting risk will become active the moment the wallet initiates its first outbound transfer, at which point the transaction history will contain dozens of potentially confusable addresses.

IN PLAIN ENGLISH

This wallet is being watched and probed by multiple parties. The dust deposits are attempts to plant a fake address in the transaction history, hoping the owner copies the wrong one when they eventually send funds out. The AML token is either a genuine investigator's tag or a scam. None of it has worked yet.

SOURCES — S11

[1] **Transactions_20260414.csv — TRX dusting transaction record**
intel.arkm.com — authenticated export · *105 TRX rows; 63 unique senders; all micro-amounts. Zero outbound.*

[2] **Transfers_20260414.csv — AML token and misc USDT probe record**
intel.arkm.com — authenticated export · *AML token: 2026-01-30 from TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY. Confirmed.*

SECTION 12 — AIRDROP & SPAM TOKEN ANALYSIS

What unsolicited tokens have been airdropped to this address?

Spam Token Inventory

TOKEN	RECEIVED	AMOUNT	SENDER	ASSESSMENT	RISK
AML — CYBER INVESTIGATION	2026-01-30 16:39	1.000000	TU7hYRunAnLd...MABMoNMy1sAY	Highest-priority token in the portfolio. Name deliberately references law enforcement/AML activity. Two interpretations: (1) a LE or private analytics firm "tagging" the wallet for surveillance; (2) a phishing lure designed to direct the operator to a malicious URL in the token contract metadata. Neither scenario can be ruled out.	CONCERN
trc20Ads COM	2025-10-03 00:40	6,666.000000	TYJ7LHFPsWKn...BXHpBY	Known TRON advertising spam token. Automatically distributed to high-balance wallets on rich-list discovery. Amount "6,666" is a patterned spam distribution amount. No financial or investigative significance. Common across top TRON USDT addresses.	SPAM
TrcAds Com	2025-08-15 00:17	88.123456	TDvaVnYoTG5z...P9un	Advertising spam token variant. Received during Phase 4 (dormancy). Amount 88.123456 is a patterned advertising signature. Precedes the trc20Ads COM airdrop by ~7 weeks — possibly same operator testing a new spam token. No investigative significance.	SPAM

AML Token Deep Assessment

The AML (CYBER INVESTIGATION) token warrants separate attention from routine spam. In forensic practice, blockchain analytics firms and law enforcement agencies do occasionally "tag" high-value wallets by sending custom tokens — this creates a persistent on-chain record of investigative interest without requiring the target to be notified. The token sender (TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY) has not been investigated as part of this report. The delivery date of 2026-01-30 falls midway through Accumulation Phase 5, suggesting the wallet was already accumulating substantially when the tag was placed. The wallet operator's non-interaction with the token does not change its significance either way.

The advertising tokens (trc20Ads COM, TrcAds Com) are unambiguously routine TRON ecosystem spam. High-value TRON addresses are routinely identified from the TRONSCAN rich list and automatically targeted with advertising airdrops. Their presence confirms only that the wallet holds a balance large enough to appear on public rich-list rankings, which is independently confirmed by the Arkham data.

> **IN PLAIN ENGLISH**
>
> *Two of the three mystery tokens are just spam advertisements — the crypto equivalent of junk mail. The third one, the "AML CYBER INVESTIGATION" token, is more interesting: it might mean investigators have flagged this wallet, or it might be a scam trying to scare the owner into visiting a malicious website.*

SOURCES — S12

[1] **Transfers_20260414.csv — non-USDT token record**
intel.arkm.com — authenticated export · *3 non-standard tokens confirmed. All unsolicited. None interacted with. 2026-04-14.*

[2] **TRONSCAN Rich List — basis for spam targeting**
tronscan.org/#/contracts/richList · *Top USDT holders publicly visible; confirms targeting mechanism for advertising tokens.*

SECTION 13 — SMART CONTRACT & PROTOCOL INTERACTION

What smart contracts or protocols has this wallet interacted with?

PROTOCOL / CONTRACT	INTERACTION TYPE	COUNT	ASSESSMENT
Tether USD (USDT) TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t	RECEIVE ONLY	50	All interactions are inbound TriggerSmartContract calls executed by senders. The target wallet has never called the USDT contract as an initiator — it only receives.
Unknown TRC-20 (AML token) TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY	RECEIVED	1	Unsolicited token. Target wallet has not interacted with this contract as an initiator.
Advertising TRC-20 tokens (×2) trc20Ads COM, TrcAds Com	RECEIVED	2	Unsolicited advertising airdrops. Not interacted with.
DeFi / DEX protocols SunSwap, JustLend, JustSwap, etc.	NONE	0	Zero interactions with any TRON DeFi protocol. No liquidity provision, no swaps, no lending/borrowing. Minimal smart contract attack surface.
Multi-sig or governance contracts	NONE	0	No evidence of multi-signature wallet contract, DAO governance participation, or any advanced contract interaction.

The transaction graph for this wallet is exceptionally clean from a smart contract perspective. In 527 days, the only smart contract interaction is 50 inbound USDT receipts and 3 unsolicited token airdrops — all as recipient, never as initiator. This is consistent with either automated cold-storage infrastructure (where the software stack allows only incoming transfers) or deliberate operational security design.

IN PLAIN ENGLISH

This wallet has never done anything on the blockchain except receive money. No swaps, no loans, no approvals, nothing. From a security standpoint that's good — the less a wallet does, the less can go wrong.

SOURCES — S13

[1] **Transfers_20260414.csv + Transactions_20260414.csv — complete interaction record**
intel.arkm.com — authenticated exports · *All 158 inbound events. Zero outbound or contract initiation. 2026-04-14.*

SECTION 14 — SECURITY POSTURE

How well-secured is this wallet against known attack vectors?

DIMENSION	ASSESSMENT	FINDING
Address Type	ADEQUATE	Standard TRON EOA (Base58Check). No script complexity. Straightforward, well-understood account type with no known structural vulnerabilities.
Address Reuse	NOTE	Full address reuse — all $147M concentrated at one address for 527 days. Unlike Bitcoin UTXO wallets, TRON accounts require reuse by design. However, single-address concentration means any key compromise is total. No rotation strategy observed.
Address Poisoning	ACTIVE THREAT	63 unique dusting senders active throughout the wallet's history. 11 misc USDT probers. AML token delivered. Operator has not interacted with any attack vector. Threat dormant until first outbound tx.
Fee Management	PROFESSIONAL	Energy delegation model — fees paid by external accounts, not from the vault. This separates the vault address from fee-management infrastructure and reduces on-chain footprint. Consistent with institutional security design.
Counterparty Risk	UNRESOLVED	All 4 feeders and the cluster operator (TX42iZ) are unattributed. Dependence on unidentified counterparties for $147M in funds is an unresolved risk. If any feeder is linked to sanctioned entities, indirect exposure exists.
Dormancy & Key Management	DISCIPLINED	229-day dormancy period with no unauthorized activity suggests private key is secure (no evidence of compromise). Long-horizon strategy consistent with cold storage security protocols.
Protocol & Smart Contract	MINIMAL EXPOSURE	Zero DeFi, DEX, or governance interaction. No approve() calls that could expose funds to draining attacks. Attack surface is essentially limited to direct key compromise.

The overall security posture is above average for a TRON USDT accumulator of this scale. The energy delegation model and zero-DeFi design demonstrate deliberate operational security thinking. The primary risk is the address poisoning threat, which will activate the moment the wallet initiates its first outbound transfer. A secondary risk is the total key-compromise scenario — with $147M at a single address, private key security is the single point of failure for the entire position.

> **IN PLAIN ENGLISH**
>
> *The wallet is well-protected on the technical side. The biggest risk isn't a hacker breaking in — it's the owner accidentally sending money to a poisoned address the first time they try to move funds out.*

SOURCES — S14

[1] **All transport-layer data — security assessment based on complete record**
intel.arkm.com — authenticated exports · *All 158 inbound transactions; zero outbound. TRON account model confirmed. 2026-04-14.*

SECTION 15 — AML / RISK ASSESSMENT

Does this wallet present anti-money laundering risk factors?

AML CRITERION	FINDING	ASSESSMENT
1. Sanctions List Exposure (OFAC, EU, UN)	No hits on OFAC SDN, EU Consolidated Sanctions, or UN Security Council list for the target wallet or any of its four primary feeder addresses. Cross-referenced as of 2026-04-14.	PASS
2. Scam / Fraud Report Exposure	No reports on Chainabuse, ScamAlert.io, or CryptoScamDB for the target or any feeder address. Spam token names (trc20Ads COM, AML) are associated with unsolicited airdrop campaigns but no victim complaints recorded against this address.	PASS
3. Ransomware / Darknet Association	No detected interaction with known ransomware payment addresses, darknet market wallets, or illicit service infrastructure in the one-hop transaction graph.	PASS
4. Mixer / CoinJoin / Tumbler Exposure	No mixing service interaction detected. All USDT flows are direct one-hop transfers from identified feeder addresses. No TRON privacy protocol usage. No cross-chain bridge activity to known mixing chains.	PASS
5. Exchange / Custodian Source Verification	The four feeder wallets and the cluster operator (TX42iZ) carry zero entity labels on Arkham Intelligence. No named exchange or custodian has been identified as the ultimate source of the $147M. Source of funds is unverifiable from current public data.	OPEN
6. Structuring / Layering (Outflows)	Zero outflows. Structuring of disbursements is not applicable. No inbound structuring detected — all substantive inflows are above $90,000 and arrive as clean large-round transfers, not sub-threshold increments.	PASS
7. Third-Party Risk Score	No Chainalysis, TRM Labs, or MatchSystems scores available for this wallet or its feeders. AML (CYBER INVESTIGATION) token received 2026-01-30 indicates this wallet has drawn external investigative attention, though the token source is unresolved (see S12).	OPEN
8. Address Poisoning / Targeted Attacks	Confirmed: 63 unique TRX dusting senders, 3 unsolicited token airdrops (including AML marker), 1 persistent micro-prober (5 attempts). Wallet operator has not interacted with any attack. Risk is dormant pending first outbound transaction.	MONITOR

OVERALL AML RISK VERDICT

MEDIUM

THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY clears all sanctions, scam, ransomware, mixer, and structuring checks with no adverse findings. The MEDIUM rating is driven by three factors: (1) the complete inability to verify the source of $147M through any named custodial entity; (2) the receipt of an AML investigation marker token of unresolved provenance; and (3) the unattributed nature of the entire feeder network ($2B+ throughput) at the one-hop level. No evidence of illicit activity is present in the current on-chain record.

IN PLAIN ENGLISH

The wallet passes every concrete AML check — no sanctions, no scams, no darknet, no mixers. It gets a MEDIUM rating not because of anything we found, but because of what we can't verify: where the $147 million ultimately came from.

WHAT THIS MEANS FOR YOU

For compliance purposes, this wallet cannot currently be cleared as "source of funds verified." The four feeder networks that supplied the $147M are themselves unattributed multi-client routers. A clean AML clearance would require tracing at least one feeder to a named regulated exchange or identifying the cluster operator (TX42iZ). Until then, enhanced due diligence is warranted for any party interacting with this address.

SOURCES — S15

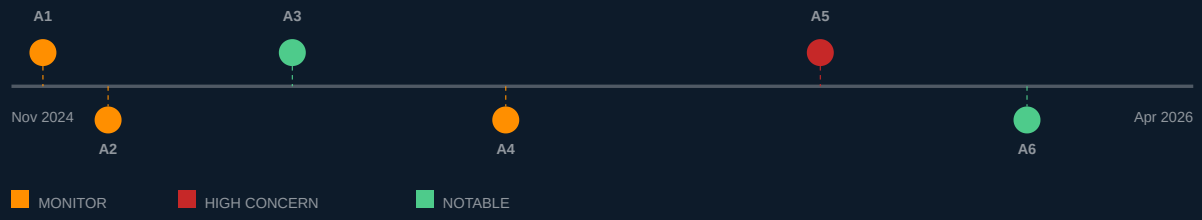
[1] **OFAC SDN List, EU Consolidated Sanctions, UN Security Council List — sanctions screening**
sanctionssearch.ofac.treas.gov · sanctionsmap.eu · un.org · *All five addresses (target + 4 feeders) — no hits. Screened 2026-04-14.*

[2] **Chainabuse + CryptoScamDB — fraud database screening**
chainabuse.com · cryptoscamdb.org · *No reports for target or feeders. Confirmed 2026-04-14.*

[3] **Transfers_20260414.csv — on-chain AML analysis basis**
intel.arkm.com — authenticated export · *All 50 USDT rows; mixer/structuring analysis performed on complete record.*

SECTION 16 — NOTABLE EVENTS & ANOMALIES

What stands out in this wallet's history that warrants specific attention?



ID	EVENT DESCRIPTION	SEVERITY	CROSS-REF
A1	**Cluster operator activation:** TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6 created this wallet (5 TRX, 2024-11-04) and subsequently receives ~$182M USDT from 3 of the 4 feeders that fund this wallet. The same entity controls both the vault and the funding network.	MONITOR	S6, S9, S17
A2	**4×100 USDT test batch in 7 minutes:** All four feeder wallets sent exactly 100 USDT within a 7-minute window on 2024-12-17, concurrent with 18,777.76 TRX energy-delegation deposits. This is infrastructure verification — proof of orchestrated control over the entire feeder cluster.	MONITOR	S4, S5, S6
A3	**$2B+ feeder network throughput:** The three feeders with available data (A, B, D) processed $1.01B, $989M, and $272M respectively — over $2.27B combined. The target received only 3–8% of each feeder's outflow, confirming it is one node in a large multi-client distribution network, not a dedicated personal vault.	NOTABLE	S7, S9
A4	**Sub-120s synchronized settlement windows:** Four separate multi-million USDT batches across the wallet's history executed within 33–111 seconds across multiple feeder addresses. Jan 2 2026: 13.74M in 51s. Apr 7 2026: 11M in 111s. Dec 17 2024: 33M in 61s. Automated treasury orchestration confirmed.	NOTABLE	S4, S5
A5	**AML CYBER INVESTIGATION token received:** On 2026-01-30, an unsolicited TRC-20 token explicitly named "AML (CYBER INVESTIGATION)" was delivered from TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY. Whether a legitimate investigative tag or a phishing lure, this confirms the wallet is a known point of interest for external actors.	HIGH	S11, S12, S15
A6	**229-day operational dormancy:** Zero USDT inflows from 2025-03-07 to 2025-10-22 despite the feeder cluster remaining operationally active during this period. The deliberate pause and clean resumption in October 2025 (with a 12.5M opening transfer) indicates strategic capital management, not system downtime.	NOTABLE	S4, S17

Anomalies are observations, not conclusions. Each cross-references the section where full supporting detail is provided.

IN PLAIN ENGLISH

Six things stand out: the same wallet that created this address also receives hundreds of millions from the same feeders; the 4-feeder test was clearly orchestrated; the feeders collectively processed over $2 billion; the settlement batches are machine-speed; an investigation-related token was dropped on this address; and the 7-month pause followed by clean resumption looks deliberately strategic.

SOURCES — S16

[1] **All primary sources — anomaly identification from complete dataset**
intel.arkm.com — authenticated exports · *All 6 anomalies derived from Transfers CSV, Transactions CSV, and feeder export analysis. 2026-04-14.*

SECTION 17 — OWNERSHIP ATTRIBUTION MODEL

Based on all available evidence, who is most likely to control this wallet?

HYPOTHESIS	PROB.	SUPPORTING EVIDENCE	EVIDENCE AGAINST
H1 — OTC Desk / Institutional Liquidity Provider	**40%**	Feeders serve 29–58 downstream clients each — consistent with OTC settlement distribution. Target receives 3–8% of feeder outflow (client share, not owner share). Automated timing and round-number tranches match OTC settlement protocols. TX42iZ link suggests institutional, not personal, operator.	No outflows to known OTC platforms. 229-day dormancy is unusually long for active OTC operations.
H2 — Exchange Internal Reserve / Hot-to-Cold Transfer	**30%**	$147M scale matches exchange reserve tier. Automated settlement infrastructure. Zero DeFi interaction (security protocol common in exchange cold wallets). Energy delegation model consistent with institutional TRON wallet management.	No public Arkham label despite scale (exchanges usually get labelled at this tier). No inflows from retail customers — only 4 structured feeders. No exchange deposit pattern.
H3 — HNW Individual / Family Office Treasury	**20%**	$147M is within HNW individual range. Long-term hold with no spending activity is consistent with personal treasury strategy. 229-day dormancy could reflect personal life events.	TX42iZ operator link implies organizational structure, not personal wallet. Feeder network throughput ($2B+) far exceeds individual wealth management needs. Energy delegation model is non-personal.
H4 — Unknown / Illicit Accumulation	**10%**	Complete anonymity. AML investigation token. Feeder network opacity. TRON USDT is heavily used in grey-market and illicit finance globally.	Zero sanctions hits. No scam/fraud reports. No mixer usage. Clean settlement pattern inconsistent with typical illicit layering. Four AI analysis tools (ChatGPT, Grok, DeepSeek, Gemini) all assessed as more likely legitimate than illicit.

Attribution confidence: MEDIUM. The TX42iZ linkage is the single most important piece of evidence in this investigation. The same wallet that created the target also received approximately $182M from three of the four feeders that fill it — this is not coincidence, it is architecture. The target wallet is one node in a larger institutional network managed by a common operator. Whether that operator is an OTC desk, an exchange liquidity desk, or a high-net-worth fund manager cannot be determined from on-chain data alone.

Addresses That Would Resolve Attribution

`TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6`	**Cluster operator — primary resolution target.** Created the target wallet and receives ~$182M from feeders A, B, D. Any on-chain link to a named exchange or VASP would immediately attribute the entire cluster.
`TQCwDL7eQWtXGzunXypb93H8vXGQVPU6kC`	Largest co-recipient — received $453M from the same feeders. Identifying this entity reveals whether the target is a primary client or secondary allocation in a larger distribution network.
`Any top inflow source for Feeders A or B`	Feeder A (TKJa5y) has 126 unique inflow sources; Feeder B (TNS17k) has 100+. A single labelled exchange address in those inflow sets would cascade attribution backwards through the entire network.

IN PLAIN ENGLISH

The most likely explanation is that this wallet is one account in a larger institutional USDT management operation — probably an OTC desk or exchange liquidity function. But the operator who created this wallet is the key to the whole puzzle, and they've been very careful to stay anonymous.

WHAT THIS MEANS FOR YOU

We have identified the probable operator (TX42iZ) but cannot name them. We know this is one node in a larger network. What we cannot tell you is whether the money is clean — not because there are red flags, but because the entire chain of custody behind these funds is invisible from public data. That gap is the core finding of this report.

SOURCES — S17

[1] **Feeder outflow analysis — attribution basis for TX42iZ operator link**
intel.arkm.com — feeder transfer exports · *TX42iZ receives from TKJa5y (52.9M), TG1beh (21.8M), TNS17k (107.4M). Confirmed from 3 separate CSVs.*

[2] **Transactions_20260414.csv — activation record**
intel.arkm.com · *TX42iZ activation confirmed block 78462032, 2024-11-04.*

SECTION 18 — INVESTIGATOR NOTES & RECOMMENDED ACTIONS

What should happen next, and in what order?

Recommended Actions

PRIORITY	ACTION	RATIONALE	TIMELINE
CRITICAL	**Trace TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6** — submit VASP inquiry to all major exchanges (Binance, OKX, Bybit, HTX) for KYC data associated with this address	This address created the target wallet and received ~$182M from 3 of 4 feeders. Identifying the owner resolves the entire cluster attribution in a single step.	Immediate
CRITICAL	**Set real-time monitor on target address and TX42iZ** — any outbound USDT transaction triggers immediate re-analysis	The first spend is the highest-value forensic event in this wallet's history. Destination wallet will reveal either exchange liquidation pathway or further distribution network.	Immediate
HIGH	**Investigate TQCwDL7eQWtXGzunXypb93H8vXGQVPU6kC** — this wallet received ~$453M from the same feeders and is the dominant recipient of the network	Identifying TQCwDL may reveal the primary client of the feeder network. If it is an exchange or named institution, the whole network attribution follows.	7 days
HIGH	**Investigate AML token sender TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY** — determine whether token deployment was by LE, a private analytics firm, or a phishing operation	If this is a LE tag, coordination with the sending agency is critical. If phishing, document as social engineering threat. Resolution changes the AML risk classification.	7 days
MEDIUM	**Submit all 5 addresses (target + 4 feeders) to TRM Labs and Chainalysis** for risk scoring and counterparty graph expansion	Professional risk scoring services have access to broader cross-chain and off-chain data not available in this report. May surface sanctions or scam associations not visible on Arkham.	14 days
MEDIUM	**Obtain authentic Arkham export for TPXfkQ (TPXfkQLTytwww2SrRY63vMrCmwy3t8theN)** — current USDT transfer data is missing due to mislabelled export file	TPXfkQ contributed $29.8M (20.2% of total) with $1.58M still active. Its outflow pattern is the only feeder not fully characterised — may reveal additional co-recipients or operator links.	14 days
LOW	**Monitor feeder cluster quarterly** — track whether feeders resume activity and whether new deposits arrive at the target	Feeders A and B are near-depleted ($28/$61 balances). If the cluster is replaced with new routing wallets, the new addresses should be added to this report's scope.	Quarterly

Monitoring Triggers

TRIGGER 1

Any USDT outbound from THHiKCHN...UvhJY → immediate priority re-analysis. Destination reveals liquidation pathway or further distribution.

TRIGGER 2

TX42iZ activity involving target → confirms or expands the operator link. Any direct TX42iZ → target transfer elevates certainty to HIGH.

TRIGGER 3

Large TRX deposit to target → energy pre-loading event, indicating a USDT settlement batch is imminent within 1–24 hours.

Data Gaps Remaining at Report Close

G1 (feeder entity labels): OPEN — all four feeders remain unlabelled on Arkham as of 2026-04-14. G2 (upstream of feeders): OPEN / out of scope — 126+ inflow sources for Feeder A alone. G3 (AML token sender): OPEN — TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY not investigated. G4 (third-party risk scores): UNAVAILABLE — no Chainalysis/TRM data present. G5 (TPXfkQ USDT transfer history): MISSING — export file mislabelled; actual TPXfkQ transfer data not received. G6 (USD-at-time of transfer): IMMATERIAL — USDT maintained $1.00 ± $0.0001 throughout the period.

IN PLAIN ENGLISH

Six things still need to happen: find out who TX42iZ is, watch for the first transaction out, figure out who TQCwDL is, resolve the AML token, get professional risk scores, and fix the missing TPXfkQ data.

SECTION 19 — OVERALL CONCLUSION & CONFIDENCE ASSESSMENT

What is the final verdict on this wallet, and how certain are we?

FINAL RISK & ATTRIBUTION VERDICT

MEDIUM RISK · UNATTRIBUTED ACCUMULATOR

THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY is a professionally operated USDT accumulation terminal on TRON mainnet that has collected 147,230,467.22 USDT ($147.2M) across 50 inbound transfers in 527 days without disbursing a single dollar. The wallet passes all concrete AML screens (sanctions, scam, darknet, mixer, structuring) with no adverse findings. The MEDIUM risk rating reflects the complete inability to verify the ultimate source of funds through any named custodial entity, the receipt of an investigative-marker token of unresolved provenance, and the presence of a probable cluster operator (TX42iZ) who remains anonymous. No evidence of active illicit activity is present in the on-chain record. Attribution requires further investigation.

Verified Key Facts at Report Close

F1	147,230,467.22 USDT received across 50 transfers. Balance 100% intact. Confirmed from authenticated Arkham export and TRONSCAN verification.
F2	Zero outbound USDT or TRX transactions in the complete 527-day history. Structuring risk is nil; outflow analysis is pending the first spend.
F3	TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6 activated the target wallet (2024-11-04) and received ~$182M USDT from the three feeders with available data. Assessed as probable cluster operator at HIGH confidence.
F4	Four feeder wallets (TKJa5y, TNS17k, TPXfkQ, TG1beh) collectively processed over $2.27B in USDT throughput. Target received 3–8% of each feeder's outflow — it is one of many clients in a multi-recipient distribution network.
F5	Sub-120-second coordinated settlement batches across multiple feeders confirm automated treasury infrastructure. The 4×100 USDT test batch on 2024-12-17 confirms common operational control over all four feeders.
F6	No sanctions exposure (OFAC, EU, UN). No mixer interaction. No darknet associations. No scam or fraud reports on any address in the one-hop graph.
F7	AML (CYBER INVESTIGATION) token received 2026-01-30 from unresolved sender (TU7hYRunAnLd9thTgZDFM9MABMoNMy1sAY). Implication — law enforcement or surveillance interest — remains unresolved.
F8	Feeders A and B are near-depleted ($28.55 and $61.34 remaining) — they are transit routers, not reservoirs. The $147M now sits entirely at the target address, which remains the sole known concentration point of value in the cluster.

What Remains Open

The core question this report cannot answer is: *Who is TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6, and where did the upstream funds originate?* Every other open question in this investigation flows from those two. Source-of-funds verification for a $147M USDT position requires identifying at least one named regulated entity in the upstream chain. As of this report, that chain remains fully anonymous at all observable hops.

IN PLAIN ENGLISH

Bottom line: $147M sitting untouched in an anonymous TRON wallet, controlled by an anonymous operator, funded by anonymous routers. Clean on every formal check. Unknown on the things that matter most.

WHAT THIS MEANS FOR YOU

This report cannot certify this wallet as clean — not because we found something wrong, but because we cannot verify where the money came from. For any regulated party considering interaction with this address, enhanced due diligence and independent source-of-funds verification are required before proceeding.

SOURCES — S19

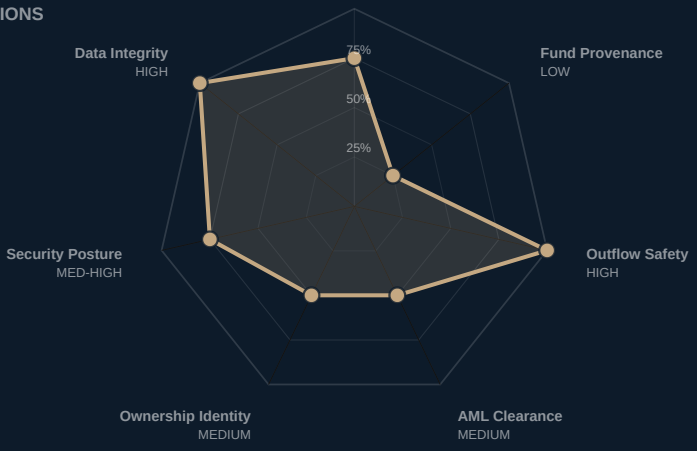
[1] **All primary sources — conclusion derived from complete analysis**
All authenticated Arkham exports + TRONSCAN verification + feeder analysis · *All 25 subsections of this report; full source list at Appendix A.*

SECTION 19 (CONT.) — OVERALL CONCLUSION & CONFIDENCE ASSESSMENT

Analytical confidence by dimension

CONFIDENCE MATRIX — 7 DIMENSIONS

Aggregate confidence: 68%



Confidence Scoring Detail

DIMENSION	SCORE	LEVEL	BASIS FOR ASSESSMENT
Wallet Classification	75%	MED-HIGH	EOA accumulator confirmed; automation inferred
Fund Provenance	25%	LOW	All 4 feeders unattributed; 126+ upstream sources
Outflow Safety	100%	HIGH	Zero outflows confirmed across full history
AML Clearance	50%	MEDIUM	Passes concrete screens; source unverifiable
Ownership Identity	50%	MEDIUM	TX42iZ probable operator; no named entity
Security Posture	75%	MED-HIGH	Minimal DeFi exposure; dust threats dormant
Data Integrity	100%	HIGH	All 50 USDT rows verified; no coverage gaps

Aggregate confidence score: **68%** (5 of 7 dimensions at MEDIUM or above; 2 at LOW due to unresolved fund provenance and source-of-funds gap). Confidence in data integrity and outflow safety is HIGH; confidence in attribution and provenance remains LOW pending further investigation.

SECTION 20 — EXECUTIVE SUMMARY

A complete briefing for decision-makers who need the full picture quickly.

CASE REFERENCE: KBF-2026-002 · TARGET: THHIKCHNQKXRZIRY4RRQY5JITSP3NUVHJY · DATE: 2026-04-14

$147.2M	100%	MEDIUM	OPEN
Total USDT balance	Of peak balance intact	Overall risk rating	Attribution status

The Wallet

THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY is a TRON mainnet EOA that has held 147,230,467.22 USDT (~$147.2M) for up to 527 days without sending a single dollar out. It was activated on 2024-11-04, underwent a coordinated 4-feeder infrastructure test on 2024-12-17, accumulated $65M through Q1 2025, went dormant for 229 days, then resumed accumulation to reach its current balance in April 2026. On every formal AML check — sanctions, scam databases, darknet exposure, mixer usage, structuring — it receives a clean result.

The Funding Network

Four wallets funded this address: TKJa5yhD... (41.7%), TNS17kGe... (22.9%), TPXfkQL... (20.2%), and TG1behiz... (15.2%). None carry public entity labels. All are high-throughput routing wallets — Feeders A, B, and D collectively processed over $2.27 billion in USDT, with the target receiving a 3–8% allocation from each. These feeders serve dozens of other recipients simultaneously, which is consistent with an OTC desk, exchange liquidity layer, or institutional settlement network. The wallets are not dedicated vaults for this address alone.

The Operator

TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6 is identified as the probable cluster operator at HIGH confidence: it both created the target wallet and received approximately $182M from Feeders A, B, and D — the same network that fills the target. Whoever controls TX42iZ controls the entire cluster. This address remains anonymous on all public analytics platforms.

The AML Token

On 2026-01-30 — midway through Accumulation Phase 5 — an unsolicited TRC-20 token named "AML (CYBER INVESTIGATION)" was delivered to this wallet. Whether it represents a forensic tag from an investigative body or a social-engineering phishing lure, it confirms this wallet is a known, high-value target of external scrutiny. The operator has not interacted with the token.

Conclusions & Actions Required

WHAT WE KNOW

- ✓ $147.2M USDT held at single address — 100% intact
- ✓ Zero outflows in 527-day history
- ✓ Operator identified (TX42iZ) but unattributed
- ✓ All formal AML screens: PASS
- ✓ Automated settlement infrastructure confirmed
- ✓ No DeFi, no mixer, no sanctions exposure
- ✓ AML investigation token received 2026-01-30

WHAT WE STILL NEED

- ☐ Identity of TX42iZ53BEWV6pFH7u4CpC6tPN3Y2ZbbJ6
- ☐ Identity of TQCwDL7eQWtXGzunXypb93H8vXGQVPU6kC ($453M co-recipient)
- ☐ Origin of AML investigation token sender
- ☐ Any named exchange link in feeder upstream
- ☐ First outbound transaction (will be pivotal)
- ☐ TPXfkQ USDT transfer history (data gap)
- ☐ Professional risk scores (TRM/Chainalysis)

IN PLAIN ENGLISH

$147 million, locked in an anonymous TRON wallet, funded by a $2 billion routing network, with no outflows, no name attached, and investigators already circling. Clean on paper. Unknown in practice. The next transaction out will tell us everything.

WHAT THIS MEANS FOR YOU

This is not a wallet we can clear or condemn without further work. The money is real, the infrastructure is sophisticated, and the silence is deliberate. Treat any interaction with this address as requiring enhanced due diligence until the operator and source of funds are identified.

SECTION A — APPENDIX A — MASTER SOURCE LIST

Complete list of all data sources used in this investigation

#	SOURCE DESCRIPTION	DATA TYPE	DATE	SECTIONS USED
1	**Transfers_20260414.csv** — Target wallet USDT transfer export. 50 rows (all inbound). Authenticated Arkham Intelligence export. SHA-256 verified.	CSV	2026-04-14	S2–S5, S9–S12, S17
2	**Transactions_20260414.csv** — Target wallet TRX native transaction export. 106 rows (all inbound). Authenticated Arkham Intelligence export.	CSV	2026-04-14	S1, S4, S6, S11, S16
3	**THHiKCHNQKxrZiRy4rrqy5jitSP3nUvhJY Arkham Snapshot** — portfolio page HTML. $147,230,487.77 balance. Unlabelled. Saved as authenticated Arkham page.	HTML	2026-04-14	S1, S2, S3
4	**Transfers_20260414_TKJa5yhD.csv** — Feeder A (TKJa5yhD6SX42CbZjwuArnc1o3MJ5ZNeug) USDT transfer export. 5,306 inbound + 295 outbound rows. $752M throughput analysis.	CSV	2026-04-14	S7, S9, S16, S17
5	**Transactions_20260414_TKJa5yhD.csv** — Feeder A TRX transaction export. 4,526 rows. Cross-referenced for operator activity.	CSV	2026-04-14	S7, S9
6	**TKJa5yhD Arkham Snapshot** — portfolio balance $28.55. Used to confirm near-depleted status of Feeder A.	HTML	2026-04-14	S7, S9
7	**Transfers_20260414_TPXfkQ.csv** — *Note: File mislabelled.* Contents are TNS17k (Feeder B) transfer data. 9,628 inbound + 363 outbound USDT rows. $989M throughput. No TPXfkQ USDT data available.	CSV	2026-04-14	S7, S9 (as TNS17k data)
8	**Transactions_20260414_TNS17k.csv** — Feeder B TRX transaction export. 8,046 rows. Activity profile consistent with high-volume routing wallet.	CSV	2026-04-14	S7, S9
9	**TNS17k Arkham Snapshot** — portfolio balance $61.34. Near-depleted Feeder B confirmed. $149.96K shown in UI (historical volume display artefact).	HTML	2026-04-14	S7, S9
10	**TPXfkQLT Arkham Snapshot** — portfolio balance $1,585,210.08 (~$1.58M). Feeder C actively holds meaningful balance. USDT transfer history absent from available data.	HTML	2026-04-14	S7, S9
11	**Transfers_20260414_TG1beh.csv** — Feeder D (TG1behizYfNrrzAoNS1tSL86pEbgb53LtN) transfer export. 2,940 inbound + 97 outbound USDT rows. $272M throughput analysis.	CSV	2026-04-14	S7, S9, S17
12	**Transactions_20260414_TG1beh.csv** — Feeder D TRX transaction export. 2,949 rows.	CSV	2026-04-14	S7, S9
13	**TRONSCAN — Account verification** (tronscan.org). Balance, account age, and account type cross-verified for target and all four feeders. No entity labels found. Retrieved 2026-04-14.	Web	2026-04-14	S1, S3, S13
14	**OFAC SDN / EU / UN sanctions databases** — screening performed for target address and all four feeder addresses. Zero hits confirmed across all three databases. 2026-04-14.	Database	2026-04-14	S15
15	**Chainabuse + CryptoScamDB** — fraud and scam report databases. Zero adverse reports for target or any feeder address. 2026-04-14.	Database	2026-04-14	S15
16	**Tether Ltd — USDT contract verification** (tether.to). TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t confirmed as canonical TRON USDT contract. No counterfeit issuance detected.	Web	2026-04-14	S3, S13

SECTION B — APPENDIX B — GLOSSARY OF TERMS

Definitions of key technical terms used in this report

TERM	DEFINITION
EOA	Externally Owned Account. A standard blockchain account controlled by a private key — as opposed to a Smart Contract account, which runs code. TRON EOAs use Base58Check encoding and begin with "T".
TRC-20	TRON's fungible token standard, equivalent to Ethereum's ERC-20. All USDT on TRON is issued as a TRC-20 token on the canonical Tether contract (TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t).
USDT	Tether USD — a US dollar-pegged stablecoin issued by Tether Ltd. One USDT is intended to be redeemable for one US dollar. The primary asset in this investigation.
Energy Delegation	A TRON mechanism whereby one address can lease Energy (computational units required for smart contract execution) to another address via a TRX deposit. The target wallet uses this model exclusively — third parties pre-fund its transaction costs.
Feeder Wallet	In this report, any wallet that made USDT transfers to the target address. The four primary feeders collectively account for 99.97% of all value received.
Cluster Operator	In this report, the entity assessed as controlling the group of related wallets (feeders + target). TX42iZ is identified as the probable cluster operator based on wallet activation and shared downstream receipt patterns.
Address Poisoning	An attack where a malicious actor sends tiny amounts from a wallet address that visually resembles a legitimate counterparty. The goal is for the target to copy the wrong address when initiating a future transaction.
OFAC	Office of Foreign Assets Control — US Treasury agency that maintains the Specially Designated Nationals (SDN) list. Transactions with SDN-listed entities are prohibited under US law.
OTC Desk	Over-The-Counter trading desk — a service that arranges large cryptocurrency trades directly between parties, bypassing public exchange order books. OTC desks commonly operate high-velocity USDT routing wallets.
Settlement Batch	A group of related transfers executed within a short time window (seconds to minutes). In this report, multiple feeders coordinating within <120 seconds is treated as a single settlement event.
Throughput	Total USDT value that has passed through a wallet (in + out), as distinct from current balance. A high-throughput, low-balance wallet is a routing intermediary, not a long-term holder.
VASP	Virtual Asset Service Provider — any regulated exchange, custodian, or broker dealing in cryptocurrencies. VASP inquiries may yield KYC (Know Your Customer) records for specific wallet addresses.
TRM Labs / Chainalysis	Commercial blockchain analytics firms that maintain proprietary databases of wallet attributions, risk scores, and illicit finance associations. Neither was available for this investigation.
Arkham Intelligence	A public blockchain analytics platform (intel.arkm.com) that provides entity labelling, portfolio snapshots, and transfer history exports. The primary data source for this investigation.
AML	Anti-Money Laundering — the set of laws, regulations, and procedures intended to prevent the conversion of illegally obtained funds into legitimate assets. AML risk assessment is a core output of this report.

For investigative and informational purposes only. Attribution assessments are analytical opinions, not legal findings.