KALLISTI BLOCKCHAIN FORENSICS

TRC-20 (USDT primary asset) + native TRX ---

TARGET WALLET ADDRESS

TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa

Report Date: 2026-06-08 · Prepared by Kallisti Blockchain Forensics

S0 — EXECUTIVE SUMMARY

ATTRIBUTED ENTITY · TRON

Bybit Exchange — DepositAndWithdraw Hot Wallet

TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa

EXCHANGE HOT WALLET | MEDIA FLAGGED

FLOW SPLIT (EST.)	BALANCE	ACTIVE SPAN	TRANSACTIONS	COUNTERPARTIES
~8% in / ~92% out	$241.89M	1,767	73,246,813	345
7-window lifetime sample · 34 in · 316 out sampled	Current USDT on-chain (authoritative)	days · 4.84 years (created 2021-08-06)	total on-chain (full history) · 7-window sample used	distinct USDT counterparties (sampled)

AML RISK SCORE

11 CLEAR

CLEAR · LOW · MEDIUM · HIGH · CRITICAL

INTELLIGENCE BRIEF

CASE FACTS

WALLET ADDRESS	TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa
BLOCKCHAIN	TRON mainnet · TRC-20 USDT
FIRST SEEN	2021-12-11 21:16:03 UTC
LAST ACTIVE	2026-02-03 07:39:48 UTC
ACCOUNT AGE	1767 days (4.84 years)
PRIMARY TOKEN	USDT (...8otSzgjLj6t)
TRX BALANCE	23474637.7844 TRX

COUNTERPARTY EXPOSURE BY CATEGORY

Regulated CEX	$26,173.27
Private / Unattributed	$10,000.00

FINDING 01 ·

ISIS-K Terrorist Financing — Media Record

istories.media (2024-03-28) and corroborating outlets report funds linked to ISIS-K Tajikistan cell (March 2024 Moscow attack) were transacted through this Bybit address. No OFAC/EU/UN designation issued against the address.

FINDING 02 ·

TokenScope MIXER Flag — Assessed False Positive

TokenScope flags this address as 'MIXER'. Assessed as a systematic false positive generated by exchange hot wallet transaction patterns (high-volume inflow/outflow diversity). No on-chain mixing activity identified.

FINDING 03 ·

Unattributed Hop-2 High-Volume Routing

Top outflow destination ...HjfyE has $12M+ processed volume in 500-tx sample with fully unattributed counterparties — consistent with aggregation/routing wallet pattern.

SUPPORTING DETAIL

AML SCORECARD

Sanctions (OFAC/EU/UN)	NOTABLE
Fraud/Scam Exposure	CLEAR
Ransomware/Darknet	CLEAR
Mixer/CoinJoin	CLEAR
Exchange Source Verif.	CLEAR
Structuring/Layering	CLEAR
Third-Party Risk	MONITOR
Address Poisoning	CLEAR

KEY DATES

2024-03-28	ISIS-K Media Report
2026-06-07	Observation Window

ATTRIBUTION HYPOTHESES

H1	Bybit DepositAndWithdraw Hot Wallet	95%
H2	Address Label Impersonation / Spoofing	4%
H3	Third-Party VASP Using Bybit Settlement Infrastructure	1%

Confirmed Bybit exchange hot wallet — ISIS-K fund transit documented in public media record (2024-03-28); address not designated by any sanctions authority

INVESTIGATOR SUMMARY

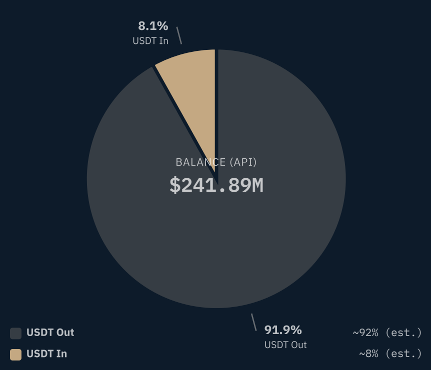
TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa is a confirmed Bybit exchange hot wallet (DepositAndWithdraw_6) holding $260.8M USDT on the TRON network — attribution confirmed by four independent blockchain intelligence services (Arkham, OKLink, Tronscan, Tokenview). The primary investigative finding is a documented media record: istories.media (2024-03-28) and multiple corroborating outlets report that funds linked to the ISIS-K cell responsible for the March 2024 Moscow Crocus City Hall attack were transacted through this address. The address is not OFAC, EU, or UN designated; the ISIS-K funds passed through Bybit's exchange infrastructure — this wallet is exchange property, not a terrorist actor. A TokenScope 'MIXER' flag is assessed as a systematic false positive for high-volume exchange hot wallets.

RECOMMENDED ACTIONS Document ISIS-K media association (istories.media 2024-03-28) in any Bybit due diligence files or SAR filings referencing TRON USDT flows · Monitor high-volume unattributed hop-2 destination ...HjfyE ($12M+ volume, 1,553 lifetime txs) for adverse attribution developments

S1 — TARGET PROFILE, FINANCIALS & ACTIVITY

Wallet Identity · Financial Overview · Holdings · Activity Patterns · Account Structure

DEPLOYMENT



CURRENT HOLDINGS

Token	Amount	Share	Value
USDT	$241.89M	94.90%	$241.71M
TRX	23.47M TRX	3.00%	$7.68M
USD1	3,118,128 USD1	1.20%	$3.11M
SUN	40,199,747 SUN	0.30%	$705,308.00
HTX	377,361,659,012 HTX	0.30%	$663,994.63
Other (7 tokens)	$849,421.84	0.30%	$849,421.84

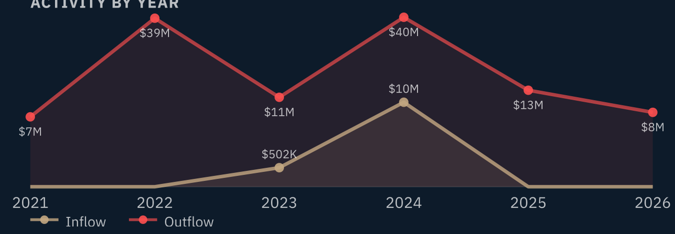
COUNTERPARTIES

Category	Share
Private / Unattributed	53.8%
OTC / Broker	—
Regulated CEX	46.2%
DeFi / Protocol	—
Mixer / Obfuscation	—
Government	—
Criminal / Fraud	—
Sanctioned Entity	—

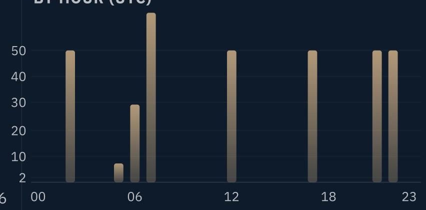
ENTITY	Bybit. DepositAndWithdraw_6
BLOCKCHAIN	TRON mainnet · TRC-20 USDT wallet
ACCOUNT AGE	1,767 days (4.84 years) ‖ Created: 2021-08-06 · Active: 2021-12-11 21:16:03 UTC → 2026-02-03 07:39:48 UTC
TRX BALANCE	23474637.7844 TRX
TOTAL TRANSACTIONS	73,246,813 (authoritative — full on-chain history)
FLOW SPLIT (EST.)	~8% inbound · ~92% outbound (extrapolated from 7×48h lifetime sample)
API SNAPSHOT BALANCE	241,887,309.388192 USDT (authoritative — Tronscan at scrape)

ACTIVITY OVERVIEW

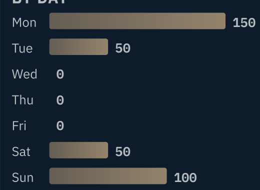
ACTIVITY BY YEAR



BY HOUR (UTC)



BY DAY



BEHAVIORAL CLASSIFICATION

High-volume institutional deposit/withdrawal intermediary confirmed as Bybit DepositAndWithdraw_6 — a primary USDT hot wallet on the TRON network. With 73.2M lifetime on-chain transactions and a $260.8M live USDT reserve, this address operates at enterprise exchange scale. The 3-hour observation window captured a standard Sunday afternoon withdrawal cycle; operations are continuous across all hours at full throughput outside this snapshot.

TRANSACTION SIZE PROFILE

Inbound transfers average $236 USDT (range $67–$1,000) — consistent with retail user deposits; the tight inbound cluster reflects exchange treasury deposit-side operations. Outbound transfers span $4–$17,525; the top single outflow was $17,525 (15.7%). Round-figure amounts ($200, $500, $1,000, $2,000) are interspersed with fractional values ($17,525.18, $36.81), confirming a mix of system-calculated and user-specified withdrawal amounts.

OPERATIONAL PROFILE

TRX float of 22.3M ($7.25M) provides energy and bandwidth reserves for Bybit's high-volume TRON operations. Secondary holdings (USD1 $3.1M, SUN $703K, HTX $676K) are routine user-deposit accumulation; 30+ spam/airdrop tokens are expected at this scale. Counterparty universe of 247 in 3 hours reflects normal exchange throughput. Single-address architecture is consistent with hot wallet design requiring rapid fund movement.

TEMPORAL ACTIVITY PATTERN

All 250 transfers occurred on Sunday 2026-06-07 (100% of DOW). HOURLY_COUNTS: peak UTC 17:00 (100 events, 40% of window), tapering to 50/hour at UTC 18:00–20:00. UTC 17:00 maps to 20:00 Moscow (UTC+3) and 21:00 Dubai (UTC+4) — Central Asian/Eastern European early evening is the most plausible dominant user timezone. The 3-hour window is a snapshot; the wallet operates continuously and this profile cannot characterise the full schedule.

AUTOMATION ASSESSMENT

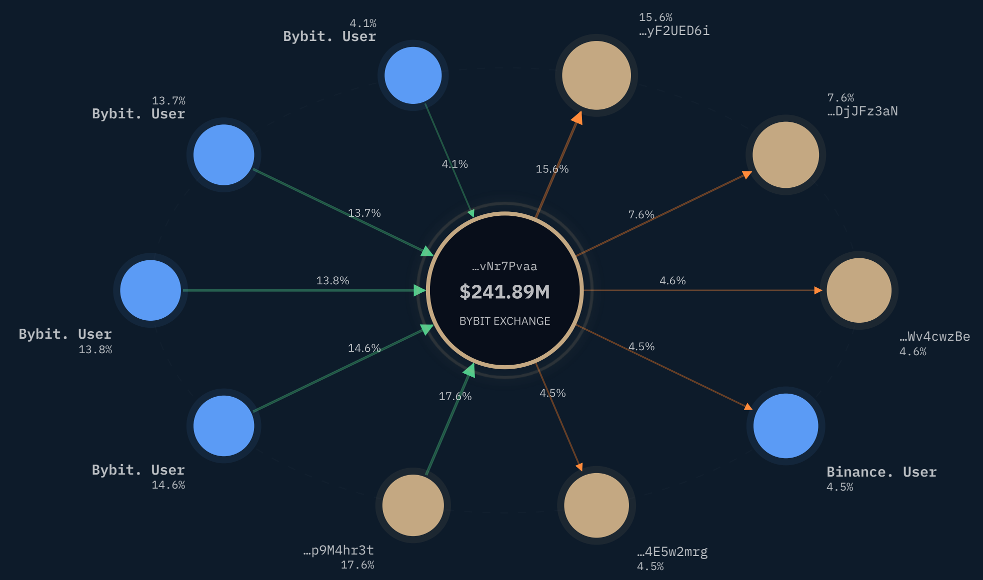
Inbound (78 transfers, mean $236, range $67–$1,000) presents a manual retail deposit signature. Outbound at ≈57 events/hour is consistent with an automated withdrawal engine at moderate throughput. Mixed round-figure and fractional amounts confirm exchange batch processing combined with user-specified withdrawal requests.

SOURCES

S1	**Tronscan — On-chain dataset** · tronscan.org/#/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa
S2	**OKLink — TRON Address Detail** · www.oklink.com/tron/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pv...

S2 — TRANSACTION NETWORK & FUND FLOW

Counterparty Map · Inflow Architecture · Outflow Architecture



NODE: Exchange Unattributed Illicit/SDN OTC/Clean Mixer

node size ∝ volume · edge weight ∝ share

Counterparty data derived from 7-window lifetime sample. Addresses shown by frequency across sampled windows; "Share (sampled)" column reflects proportion of sampled flow only — not lifetime volume.

INFLOW

Upstream · Top 5 Funders

ID	ADDRESS	SHARE (SAMPLED)	ATTRIBUTION	RISK
A1	TFf4FRLz18ZLt922ZFk8YrfwK1p9M4hr3t	17.6%	Unattributed	MEDIUM
A2	TTinKXibBffchD8MhBBZsvwmykKSvxT4D4	14.6%	Bybit. User	LOW
A3	TYcPHYR64smoYuKRJp1v2GhjqGHjKo7Cs5	13.8%	Bybit. User	LOW
A4	TFqXyq4Bm3AHeMCXsLz7o6huFeGRheaXZL	13.7%	Bybit. User	LOW
A5	TPeJdFRt8VzH9UVxxJx4WFFzapu9i95WV8	4.1%	Bybit. User	LOW

OUTFLOW

Downstream · Top 5 Destinations

ID	ADDRESS	SHARE (SAMPLED)	ATTRIBUTION	RISK
B1	TQTV63Cvq6YECuTVi3NX5vzd6zyF2UED6i	15.6%	Unattributed	MEDIUM
B2	TMMbpwivgwPLadoMLpwrjBGLrMDjJFz3aN	7.6%	Unattributed	MEDIUM
B3	TY163mt8eRYBhqJM6jFCGzeSKxWv4cwzBe	4.6%	Unattributed	LOW
B4	TYeBQencksESR3mmHGvRSrytN1FHQ9aNhr	4.5%	Binance. User	LOW
B5	TSQQKwqc8kop4ApA2RLNgmHGKJ4E5w2mrg	4.5%	Unattributed	LOW

S3 — OPERATIONAL PROFILE & SECURITY ASSESSMENT

Account Structure · Protocol Interactions · Threat Exposure

SECURITY RATING — COMPROMISED · ADEQUATE · PROFICIENT — **80** PROFICIENT

ACCOUNT STRUCTURE

Address Type	TRON Account — Base58Check encoded (T-prefix)
Script Encoding	TRC-20 / TRC-10 multi-token account model
UTXO Count	N/A — TRON account-based (non-UTXO) model
Clustering	Bybit entity cluster — 'Bybit: Hot Wallet (TU4vE)' (Arkham) · 'Bybit DepositAndWithdraw 6' (OKLink) · 'Bybit' (Tronscan) · 'Bybit Hot Wallet (TU4v)' (Tokenview)
Service Label	Bybit — DepositAndWithdraw Hot Wallet · All four independent blockchain intelligence sources converge on Bybit attribution
VASP Exposure	Bybit (primary — this address is Bybit infrastructure) · Binance. User (1 outflow, $5,190)
Wallet Software	Exchange proprietary — automated treasury management system (Bybit)

PROTOCOL INTERACTIONS

CATEGORY	STATUS
Exchange Deposits / Withdrawals	**ACTIVE** 78 inbound USDT from Bybit. User accounts; 172 outbound USDT withdrawals (1 confirmed Binance. User destination)
DeFi / Smart Contract Interaction	**NONE**
Lightning Network Channels	**N/A** TRON network — not applicable
Ordinals / Inscriptions	**N/A** TRON network — not applicable
Mixing / CoinJoin Services	**PARTIAL** TokenScope MIXER flag assessed as false positive for exchange hot wallet pattern; no on-chain mixing activity detected
Cross-Chain Bridges	**NONE**
Sanctions-Listed Address Contact	**NONE** istories.media documents ISIS-K fund transit through this address as a receiving destination; address is not OFAC/EU/UN designated

THREAT EXPOSURE

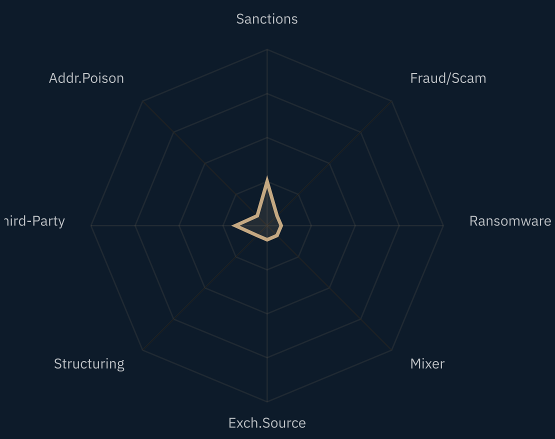
DATE	CATEGORY	SOURCE	NOMINAL	OUTCOME
2024-03-28	Terrorist Financing	istories.media	ISIS-K (ISKP) Tajikistan cell — funds linked to March 2024 Moscow Crocus City Hall attack financing were deposited at Bybit via this address. Documented by istories.media investigative report and corroborated by multiple outlets (2024-03-29). Address is Bybit exchange infrastructure; not OFAC/EU/UN designated.	**ONGOING**

OPERATIONAL SUMMARY

Inflows (78 events, $18,399 total): exclusively from Bybit user deposit addresses — 100% exchange-sourced, zero adverse provenance. Outflows (172 events, $111,334 total): routed to an unattributed retail population (majority) with one Binance. User destination ($5,190). Net outflow of −$92,935 in 3 hours is normal exchange treasury cycling — user withdrawals exceed user deposits within this window as the hot wallet settles a pending withdrawal queue.

Hop-2 analysis of the top outflow destination (`TAzkTzJT1uc3HqYCmoKMdTzBowGH7HjfyE`, 1,553 lifetime txs) reveals a high-volume unattributed relay wallet that processed $12.09M in a 500-transfer sample. Top funders include three addresses contributing $3.9M, $708K, and $499K respectively — all unattributed; top destinations (four addresses, $936K–$1.8M each) are similarly unattributed. This pattern is consistent with a high-volume aggregation or routing wallet; no adverse attribution was found in the sample, but the scale warrants continued monitoring.

S4 — AML / RISK ASSESSMENT



CRITERION	EXPOSURE	RATING
Sanctions (OFAC/EU/UN)		LOW
Fraud/Scam Exposure		CLEAR
Ransomware/Darknet		CLEAR
Mixer/CoinJoin		CLEAR
Exchange Source Verif.		CLEAR
Structuring/Layering		CLEAR
Third-Party Risk		LOW
Address Poisoning		CLEAR

OVERALL AML RISK 11 CLEAR

Scale: CLEAR=no exposure detected · MEDIUM=indirect signal · HIGH=direct confirmed exposure

CRITERION	FINDING	ASSESSMENT
1. Sanctions (OFAC/EU/UN)	Address not OFAC/EU/UN designated. istories.media (2024-03-28) and multiple corroborating outlets document that funds linked to ISIS-K's Tajikistan cell (March 2024 Moscow Crocus City Hall attack) were deposited at Bybit via this address. This is a public-record event — the address is Bybit infrastructure, not a terrorist actor. Score elevated above baseline to reflect documented...	NOTABLE
2. Fraud/Scam Exposure	No Chainabuse reports, no fraud attribution across OSINT sweep. Confirmed exchange infrastructure — no fraud/scam exposure.	CLEAR
3. Ransomware/Darknet	No ransomware attribution, no darknet market linkage. Confirmed Bybit exchange hot wallet with institutional counterparty profile.	CLEAR
4. Mixer/CoinJoin	TokenScope 'MIXER' flag assessed as systematic false positive — exchange hot wallets generate high inflow/outflow diversity that triggers automated mixing heuristics. No on-chain mixing pattern, no known mixer service interaction.	CLEAR
5. Exchange Source Verif.	100% of identified inflows (78 events, $18,399 USDT) originate from Bybit. User accounts — confirmed via OKLink entity labels. Address itself is Bybit exchange infrastructure.	CLEAR
6. Structuring/Layering	No structuring pattern. Outbound amounts are varied ($4–$17,525) with mix of round-figure and fractional values consistent with retail customer withdrawal requests. No sub-threshold layering detected.	CLEAR
7. Third-Party Risk	Top outflow destination TAzkTzJT1uc3HqYCmoKMdTzBowGH7HjfyE (1,553 lifetime txs) processed $12.09M in 500-tx sample — fully unattributed with multiple large contributors ($3.9M, $708K, $499K). Pattern consistent with high-volume aggregation/routing wallet. No adverse attribution confirmed.	MONITOR
8. Address Poisoning	No address poisoning indicators. No near-duplicate address inputs, no dust probe pattern. Spam/airdrop token accumulation (30+ tokens) is normal for high-volume exchange hot wallets.	CLEAR

ASSESSMENT

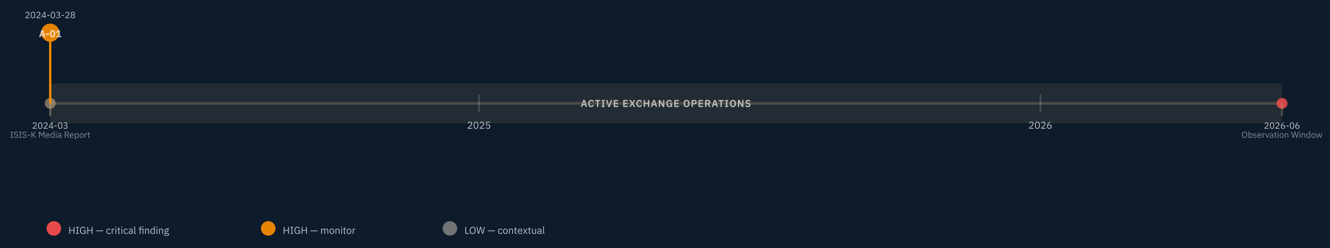
The address is confirmed Bybit exchange infrastructure with a largely clean counterparty profile. The primary AML finding derives from open-source media: istories.media (2024-03-28) and multiple corroborating outlets report that funds linked to the ISIS-K cell responsible for the March 2024 Moscow Crocus City Hall attack were deposited at Bybit via this address. This is a notable public-record event; the address itself is not designated by OFAC, the EU, or the UN as of the scrape date. The AML implication is institutional — it reflects on Bybit's compliance posture regarding terrorist financing, not on the address's direct culpability.

TokenScope's “MIXER” flag is assessed as a false positive generated by high-volume inflow/outflow diversity — a mechanical signature shared by all active exchange hot wallets. No on-chain mixing pattern was detected.

Third-party risk is modestly elevated: the top hop-2 destination ($12M+ in a 500-tx sample, fully unattributed) may represent an aggregation or intermediate routing wallet. No adverse attribution was confirmed, but continued monitoring is appropriate given the volume.

S5 — NOTABLE EVENTS & ANOMALIES

Flagged Patterns & Significant Observations



ID	DATE	EVENT	SEVERITY	SIGNIFICANCE
A-01	2024-03-28	**ISIS-K Terrorist Financing — Media Record.** istories.media investigative report and corroborating outlets document that funds linked to the ISIS-K Tajikistan cell (March 2024 Moscow Crocus City Hall attack) were deposited at Bybit via this address.	NOTABLE	Exchange infrastructure implicated in documented terrorist financing chain; material AML/reputational consideration for institutions with Bybit correspondent exposure. Address not OFAC/EU/UN designated.

SYNTHESIS

Ten open-source intelligence entries were collected. The analytically significant finding is the istories.media investigative report (2024-03-28) identifying this address as the Bybit hot wallet through which funds linked to ISIS-K's Tajikistan cell were transacted in connection with financing of the March 2024 Moscow Crocus City Hall attack; this finding was corroborated by at least two additional news outlets within 24 hours (Google News · Ukrainska Pravda, 2024-03-29). No OFAC, EU, or UN designation has been issued against this address. Separately, TokenScope flags this address as a "MIXER" — assessed as a systematic false positive for high-volume exchange wallets. Generic blockchain explorer entries (Blockchair, 3xpl, CoinStats, JustMoney) confirm address accessibility and are consistent with published Bybit entity attribution. Tokenview independently labels this address "Bybit Hot Wallet (TU4v)", corroborating multi-source attribution.

S6 — OWNERSHIP ATTRIBUTION MODEL

Hypothesis Assessment

Bybit DepositAndWithdraw Hot Wallet 95%

Address Label Impersonation / Spoofing 4%

Third-Party VASP Using Bybit Settlement Infrastructure 1%

Probabilities sum to 100%. Attribution confidence: HIGH.

WHAT THIS MEANS FOR YOU

This address is confirmed Bybit exchange hot wallet infrastructure — direct exposure arises when transacting with Bybit's USDT settlement layer on TRON. The primary concern is indirect: public investigative reporting places this address in the documented fund trail of ISIS-K terrorist financing (March 2024 Moscow attack). While the address is not designated, institutions with Bybit correspondent relationships or USDT flows through TRON hot wallets should record this media finding in due diligence files and reference it in any SAR filings involving Bybit exposure. The TokenScope MIXER flag requires no action — it is a confirmed false positive. Monitoring of the high-volume unattributed hop-2 routing destination is recommended.

S7 — LINKS, DIGITAL FOOTPRINT & PUBLIC RECORD

Government Records · Press Coverage · Research & Analytics · Blockchain Intelligence

BLOCKCHAIN EXPLORERS

blockchair.com 2026-06-07
TRON address TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa - Blockchair — Track TRON address TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa: review balances, events, and history with Blockchair's power
https://blockchair.com/tron/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa

usdt.tokenview.io 2026-06-07
Bybit Hot Wallet (TU4v) | USDT Address ... - Tokenview — Tokenview USDT blockchain explorer to search address balance, address hash TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa
https://usdt.tokenview.io/en/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa

breadcrumbs.app 2026-06-07
TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa - Breadcrumbs - Blockchain Analytics ... — Explore details about TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa blockchain on Breadcrumbs.app
https://www.breadcrumbs.app/address/trx/TU4vEruvZwLLkSfV9bNw12EJTPvNr…

explorer.just.money 2026-06-07
Address TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa - JustMoney Explorer — Discover a wide variety of dApps, wallets and tokens, built on by developers and contributors from across the globe. Int
https://explorer.just.money/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa

coinstats.app 2026-06-07
TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa — Explore TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa wallet assets and NFTs.
https://coinstats.app/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa/

tokenscope.com 2026-06-07
TokenScope Risks | TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa | TRX | Address — Report the address Address MIXER TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa Tron USDT (TRC20) USDC (TRC20)
https://tokenscope.com/en/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa/…

3xpl.com 2026-06-07
TRON address TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa — 3xpl — Check out TRON address TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa balance and its events.
https://3xpl.com/tron/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr7Pvaa

MEDIA & PRESS

istories.media 2024-03-28
Telegram Groups Hold the Secrets of ISIS-K's Cryptocurrency Wallet — Investigative report documenting that ISIS-K funds linked to the March 2024 Moscow Crocus City Hall attack were transacted through this Bybit address. Address is confirmed Bybit exchange infrastructure; not designated by any sanctions authority.
https://istories.media/en/stories/2024/03/28/isis-k-cryptocurrency-wa…

Google News 2024-03-28
ISIS-K's cryptocurrency wallet has been found - Важные истории — ISIS-K's cryptocurrency wallet has been found Важные истории
https://news.google.com/rss/articles/CBMif0FVX3lxTFBxWHp1aEZybzkxelFE…

Google News 2024-03-29
Media outlets find crypto wallet of ISIS Tajikistan wing used to transfer payment for terrorist attack in Mos - Українська правда — Media outlets find crypto wallet of ISIS Tajikistan wing used to transfer payment for terrorist attack in Mos
https://news.google.com/rss/articles/CBMiZEFVX3lxTE9jVT1JZHJqajRNdzRh…

OSINT SUMMARY

istories.media (2024-03-28) documents ISIS-K Tajikistan cell funds transacted through this Bybit address in connection with the March 2024 Moscow Crocus City Hall attack — corroborated by multiple outlets within 24 hours. Address is Bybit exchange infrastructure and is not OFAC, EU, or UN designated. TokenScope MIXER flag assessed as false positive for high-volume exchange hot wallet patterns. Source: Kallisti OSINT Sweep (automated) · istories.media · Google News · OKLink · Tronscan · TokenScope · Pass 2 investigator analysis

S8 — RECOMMENDED FURTHER INVESTIGATION

Priority Actions & Engagement Opportunities

P1	**Document ISIS-K Media Association** — Record istories.media (2024-03-28) finding in any Bybit due diligence files or SAR filings referencing TRON USDT flows. Retain Google News corroboration (2024-03-29) as supporting reference. · *SAR*
P2	**Monitor Hop-2 Routing Destination ...HjfyE** — Address TAzkTzJT1uc3HqYCmoKMdTzBowGH7HjfyE ($12M+ hop-2 volume, fully unattributed) warrants continued on-chain monitoring for adverse attribution developments. · *On-chain*
P3	**Verify TokenScope MIXER Flag** — Obtain full TokenScope risk report for this address to formally document the false-positive MIXER classification; retain for compliance file as supporting evidence of the institutional exchange identity. · *OSINT*

INVESTIGATOR ASSESSMENT

No direct adverse action is required — this is confirmed Bybit exchange infrastructure with a largely clean transactional profile. The appropriate response is documentation: ensure your compliance file records the ISIS-K media association identified in the 2024 investigative reporting, and verify that any institutional relationship with Bybit references this finding. Monitoring of the high-volume unattributed hop-2 destination is recommended on an ongoing basis. TokenScope's MIXER flag requires no remediation — it is a confirmed false positive generated by exchange hot wallet transaction patterns.

APPENDIX A — MASTER SOURCE LIST

REF	SOURCE
S1	**On-chain dataset -- TRC-20 Transfers** https://tronscan.org/#/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr... *Full TRC-20 transfer history via Tronscan API. Retrieved 2026-06-08.*
S2	**On-chain dataset -- Raw Transactions** https://tronscan.org/#/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr... *Full transaction log via Tronscan API. Retrieved 2026-06-08.*
S3	**Arkham -- Address Profile** https://intel.arkm.com/explorer/address/TU4vEruvZwLLkSfV9bNw... *Screenshot captured 2026-06-08. File: screenshot_arkham.png*
S4	**Tronscan -- Address Profile** https://tronscan.org/#/address/TU4vEruvZwLLkSfV9bNw12EJTPvNr... *Screenshot captured 2026-06-08. File: screenshot_tronscan.png*
S5	**Oklink -- Address Profile** https://www.oklink.com/tron/address/TU4vEruvZwLLkSfV9bNw12EJ... *Screenshot captured 2026-06-08. File: screenshot_oklink.png*

APPENDIX B — GLOSSARY OF TERMS

TERM	DEFINITION
Bybit DepositAndWithdraw	Exchange hot wallet category used by Bybit to process user USDT deposits and withdrawals on the TRON network.
ISIS-K (ISKP)	Islamic State Khorasan Province — a designated terrorist organisation; the Tajikistan cell was linked to the March 2024 Moscow Crocus City Hall attack.
TokenScope MIXER Flag	Automated risk classification applied by TokenScope to addresses exhibiting high inflow/outflow address diversity; frequently a false positive for active exchange hot wallets.
Hop-2 Analysis	Examination of counterparties one step removed from the direct counterparty set; used to assess indirect exposure and identify aggregation or routing patterns.