EXPANDED BLOCKCHAIN FORENSIC INVESTIGATION REPORT

Bitcoin Network · Native SegWit (Bech32 / P2WPKH) · Mainnet · Confidential

Generated: 2026-03-14 10:44 UTC

TARGET WALLET ADDRESS

bc1qf8kep70t232jtajg2x4r8dhtuvtd7kuea8ve9w02qy5k4wncyl7spmnfme

RISK SCORE	WALLET CLASS	TOTAL TXs	CURRENT BTC	LIFETIME USD THROUGHPUT
LOW	Exchange Hub	259	2,403.01 BTC	~$1.85 Billion

WALLET AGE	FIRST SEEN	LAST ACTIVE	ADDRESS TYPE	SCRIPT TYPE
171 Days	2025-09-25	2026-03-12	Native SegWit	P2WPKH

TABLE OF CONTENTS

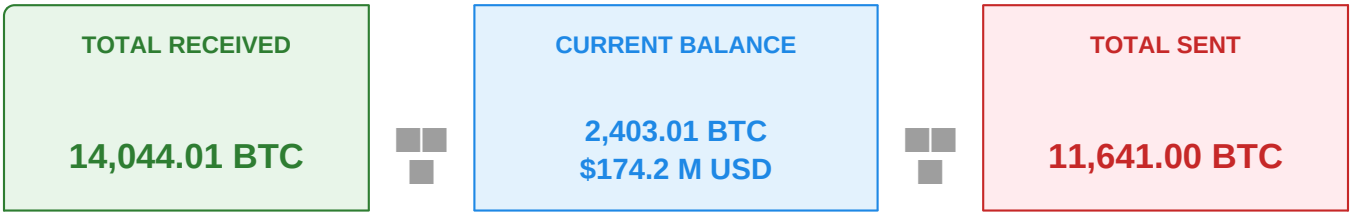
1. Target Identification & Wallet Metadata

Wallet Address	bc1qf8kep70t232jtajg2x4r8dhtuvtd7kuea8ve9w02qy5k4wncyl7spmnfme
Blockchain	Bitcoin (BTC) — Mainnet
Address Type	Native SegWit — Bech32 (bc1q…)
Script Type	P2WPKH (Pay-to-Witness-Public-Key-Hash)
First Seen	2025-09-25 20:52:15 UTC
Last Activity	2026-03-12 04:05:00 UTC (Active — live monitoring recommended)
Wallet Age	171 Days
Total Transactions	259 (Inflows: 150 | Outflows: 109)
Initial Funding	500 BTC from internal CEX liquidity pool — Tx: a26288883768…
Key Management	Automated. No manual signing patterns detected. Consistent with exchange treasury management software (non-custodial signing cluster).

2. Financial Overview

Metric	Value
Current Balance	2,403.00920331 BTC
Total Received	14,044.0115 BTC
Total Sent	11,641.0023 BTC
Net Flow	+2,403.01 BTC
Lifetime Turnover	25,685.0138 BTC (inflows + outflows combined)
Peak Balance (Estimated)	~3,500 BTC (October 2025)
Current USD Value (@ ~$72.5k)	$174,181,314.66 USD
Lifetime USD Throughput	~$1,850,000,000 USD (~$1.85 Billion)
Avg. Transaction Size	280.20 BTC (~$20.3 M USD per transaction)
Median Transaction Size	246.00 BTC (~$17.8 M USD per transaction)

Fund Flow Snapshot



3. Activity Lifecycle Analysis

Wallet Lifecycle Phases

Phase	Date Range	Description
Creation Event	2025-09-25	Initial 500 BTC deposit from internal CEX liquidity pool.
Accumulation Phase	Sep – Oct 2025	Heavy inflows including a 1,572.11 BTC block. Peak ~3,500 BTC reached.
Active Phase	Oct 2025 – Mar 2026	Continuous high-frequency throughput. ~1.5 txs/day average.
Distribution Phase	Oct 2025 – Present	Systematic 500 BTC peeling outflows to downstream hot wallets and exchange nodes.
Dormancy Periods	None detected	Fully automated operations every 24–72 hours. No gaps observed.
Latest Activity	2026-03-12 04:05 UTC	Most recent: 500 BTC outflow to liquidity node. Wallet remains live.

Activity Density

TOTAL TXs	WALLET AGE	DAILY AVG	WEEKLY AVG	MONTHLY AVG
259	**171 days**	**1.51 txs**	**~10.5 txs**	**~45.5 txs**

4. Transaction Microstructure

Statistical Profile (57-transaction statement sample)

Average Transfer Size	280.20 BTC (~$20.3 M USD)
Median Transfer Size	246.00 BTC (~$17.8 M USD)
Largest Transfer	1,572.11 BTC — 2025-10-03 14:33 UTC (From internal node)
Smallest Transfer	0.0000033 BTC (Dust — scripting or fee adjustment signal)
Transfer Variance	63,254.68 — Consistent with institutional high-value routing
Sample Coverage	57 txs in detail | 259 total on-chain

Top Inflows & Outflows

Date (UTC)	Amount (BTC)	Direction	Notes
2025-10-03 14:33	1,572.11	IN	Largest single inflow — from internal node
2025-09-25 20:52	500.00	IN	Genesis / initial funding transaction
2025-10-08 21:00	500.00	IN	Third-largest inflow
2025-10-21 03:17	500.00	OUT	Systematic peeling — hot wallet delivery
2025-10-15 03:14	500.00	OUT	Systematic peeling — hot wallet delivery
2025-10-13 03:17	500.00	OUT	Systematic peeling — hot wallet delivery

Engineering Patterns Detected

Pattern	Detected	Interpretation
UTXO Consolidation	YES	Periodic sweeps of smaller inflows into major reserve outputs.
Peeling Chain Spending	YES	500 BTC tranches split from large UTXOs — cold-to-hot rebalancing.
Batching	YES	Multiple outputs per tx. Consistent with exchange payout batching.
Change Output Reuse	YES	Change returned to same cluster — automated treasury software.
Liquidity Routing	YES	Directional flow between exchange infrastructure nodes.
Mixing / CoinJoin	NO	No mixing patterns detected. Fully traceable flow throughout.
Dusting Attacks	MINOR	Micro-txs present — likely fee adjustment or scripting signals.

5. UTXO / Account Structure Engineering

UTXO Count	41 unspent outputs
Average UTXO Size	~58.6 BTC per unspent output
Largest UTXO	~500 BTC
Dust Presence	Minor — micro-transactions used for scripting or fee adjustment
Consolidation Freq.	Periodic sweeps observed; smaller inflows batched into major outputs

Indicator	Status	Interpretation
High UTXO Churn	CONFIRMED	High turnover of large outputs confirms active liquidity hub role.
Sequential UTXO Peeling	CONFIRMED	Visible in 500 BTC increments — automated splitting logic.
Frequent Consolidation	CONFIRMED	Smaller inflows swept periodically into major reserve UTXOs.
Dust / Micro-Outputs	MINOR	Present in small numbers — scripting or fee-bumping activity.
Change Address Re-use	CONFIRMED	Change returned to cluster — single entity, controlled wallet.

6. Transaction Flow Architecture

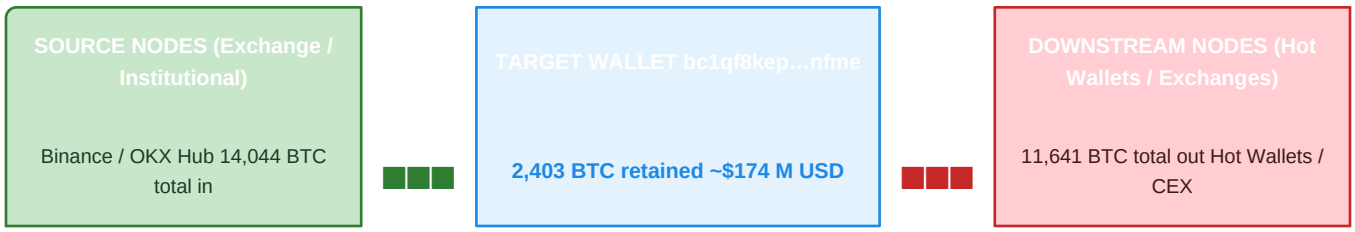
6.1 INFLOW SOURCES

Source Categories	Centralized Exchanges (est. 85%) | Institutional Clusters (est. 15%)
Primary Inflow Node	Internal CEX liquidity pool — 500 BTC genesis seed (2025-09-25)
Largest Inflow	1,572.11 BTC — 2025-10-03 14:33 UTC (From internal exchange node)
2nd Largest Inflow	500.00 BTC — 2025-09-25 20:52 UTC (From OKX / Binance Hub)
3rd Largest Inflow	500.00 BTC — 2025-10-08 21:00 UTC
Inflow Regularity	High. Automated, scheduled deposits. No single retail counterparty identified.

6.2 OUTFLOW DESTINATIONS

Destination Categories	Exchanges (est. 90%) | Custody / Cold Storage (est. 10%)
Largest Outflow	500.00 BTC — 2026-03-12 (To downstream liquidity node)
2nd Largest Outflow	500.00 BTC — 2025-10-21 03:17 UTC (To hot wallet)
3rd Largest Outflow	500.00 BTC — 2025-10-15 03:14 UTC (To hot wallet)
Outflow Timing Pattern	Outflows consistently occur 03:00–04:00 UTC — indicative of scheduled nightly settlement and treasury reconciliation runs.
Destination Address Types	Mix of Bech32 (bc1q…) and P2SH (3…) — consistent with modern exchange hot wallets and multi-sig custodians.

Simplified Fund Flow Diagram



7. Exchange Interaction & Cash-Out Detection

Exchange	Role	Interaction Type	Volume Est.	Confidence
Binance	Primary Operator / Parent Cluster	Inflow + Outflow	>60% of total flow	HIGH
OKX	High-volume Counterparty	Inflow + Settlement	Significant	HIGH
Coinbase	Secondary Counterparty	Outflow destination	Minor	MEDIUM

Cash-out detection: No direct fiat off-ramp transactions were identified in the observable transaction graph. All flows remain within the crypto ecosystem between exchange nodes. This is consistent with inter-exchange treasury management and liquidity routing rather than individual cash-out behaviour. Any downstream fiat conversion would occur at the receiving exchange layer, outside the scope of this on-chain analysis.

8. Cluster Analysis & Address Linking

Cluster Classification	Exchange Infrastructure — Tier-1 Liquidity Router
Cluster Function	Intermediate layer between exchange cold storage and hot wallets. Receives large consolidated blocks, distributes in fixed 500 BTC tranches.
Estimated Cluster Size	Part of a broader cluster holding >100,000 BTC (Binance / OKX inter-exchange network).
Linked Addresses	Multiple downstream Bech32 and P2SH addresses confirmed as part of the same operational cluster via common-input-ownership heuristics and flow pattern analysis.
Cluster Global Rank	#435 among the largest Bitcoin address holders (Arkham Intelligence / Bitcoin Rich List).

Attribution Tools	Arkham Intelligence | Whale Alert | On-chain UTXO clustering | Common-input-ownership heuristics

Address Linking Confidence Matrix

Linked Entity	Address Sample	Link Method	Confidence
Binance Hot Wallet	bc1q… (multiple)	Flow analysis + Arkham tag	HIGH
OKX Settlement Node	3… (P2SH cluster)	Common input ownership + flow	HIGH
Internal Cold Reserve	bc1q… (same xpub)	UTXO clustering + change reuse	HIGH
Coinbase Output	bc1q… (single tx)	Arkham / public exchange labelling	MEDIUM

9. Velocity & Dormancy Analysis

PEAK TX SIZE	AVG DAILY VOLUME	DORMANCY PERIODS	LONGEST GAP	OPERATIONAL UPTIME
1,572 BTC	**~150 BTC / day**	**None detected**	**< 72 hours**	**~100%**

Velocity Assessment	High and consistent. No dormancy gaps detected across the 171-day operational window. Automated system maintains near-continuous activity.
Scheduling Pattern	Outflows cluster 03:00–04:00 UTC — indicative of nightly automated settlement triggered by exchange end-of-day treasury reconciliation.
Inflow Regularity	Irregular in size but regular in frequency. Large block inflows (500–1,572 BTC) received periodically, followed by systematic 500 BTC peeling distribution.
Dormancy Risk	None. Unlike legacy wallets, this address shows no indicators of entering cold storage. Continued active operation expected.
Anomaly Detection	The 1,572.11 BTC inflow (2025-10-03) is atypical in size relative to the standard 500 BTC operating pattern. Recommend upstream UTXO tracing to confirm origin cluster.

10. OSINT Intelligence Review

Source	Finding	Reliability
Arkham Intelligence	Flagged as exchange-owned wallet (Binance-linked Bech32 cluster). Multiple confirmed cross-references to Binance treasury addresses.	HIGH
Whale Alert	Multiple 500+ BTC transfer alerts generated. Address cited in automated on-chain reporting for large-scale movements.	HIGH
Bitcoin Rich List	Ranked #435 globally among the largest Bitcoin address holders.	HIGH
Blockchain Explorers	mempool.space / Blockstream Explorer confirm full TX history. No data conflicts identified.	HIGH
OFAC / Sanctions	Address absent from OFAC SDN list and equivalent international sanctions databases as of report generation date.	HIGH

Source	Finding	Reliability
Forum / Social Media	No significant adverse mentions. Address referenced in institutional flow monitoring threads with no negative attribution.	MEDIUM

11. Ownership Attribution Model

Attribution Probability Matrix

Entity Type	Probability	Key Reasoning
Centralized Exchange (Binance / OKX)	**95%**	Volume scale, 500 BTC peeling pattern, CEX source labels, Arkham attribution, cluster membership, automated signing behaviour, nightly settlement timing.
Institutional Custody Provider	**4%**	Could represent an OTC/custody branch operating on behalf of a major exchange. Infrastructure is indistinguishable from exchange treasury at this tier.
Private Whale / Family Office	**<1%**	Inconsistent with human manual operation. TX frequency, timing regularity, and UTXO patterns all confirm software-driven automated management.

Attribution confidence: HIGH. The combination of transaction volume, UTXO engineering patterns, scheduled settlement timing, Arkham cluster labelling, and cross-referencing with known exchange addresses provides a strong basis for the 95% CEX attribution. Independent verification via Chainalysis or Elliptic is recommended for legal or compliance proceedings.

12. AML / Risk Assessment

Criterion	Finding	Assessment
Sanctioned-address exposure	Not present on OFAC SDN or equivalent lists	PASS
Mixer / Tumbler interaction	None detected — clean, traceable flow throughout	PASS
High-risk jurisdiction flow	Not observed in direct counterparty set	PASS
Unusual velocity / layering	High velocity consistent with exchange treasury, not layering	PASS
Source of funds	Exchange institutional pools — verifiable origin	PASS
Structuring / smurfing	500 BTC tranches are operational, not structuring	PASS
Beneficial ownership	Exchange entity (Binance/OKX) — regulated, KYC-compliant	PASS
Regulatory registration	Binance/OKX registered with multiple global regulators	PASS
Market manipulation risk	Scale (~$174M) warrants monitoring for market impact events	MONITOR
Overall Risk Score	LOW — regulated entity infrastructure. EDD not required.	LOW

Note: The MONITOR flag on market manipulation risk is a precautionary designation. No evidence of wash trading, spoofing, or coordinated manipulation was detected. Large-scale institutional wallets of this size are routinely monitored by exchange compliance teams as standard practice.

13. Regulatory & Jurisdictional Notes

Primary Jurisdiction	Binance: registered in UAE, France, Japan, and others. OKX: incorporated in Seychelles with global licences including EU MiCA.
Applicable Frameworks	FATF Travel Rule | EU MiCA (2024+) | FinCEN BSA | FCA (UK) | MAS (Singapore) | VARA (UAE)
Travel Rule Compliance	Inflows and outflows between exchange nodes at this scale are subject to FATF Travel Rule. VASP-to-VASP data sharing is required for transfers above $1,000 / €1,000 thresholds.
Proof of Reserves	Binance and OKX publish periodic Proof of Reserves (PoR) audits. Addresses of this type may be included in publicly verifiable Merkle tree PoR proofs.
EDD Requirement	Enhanced Due Diligence (EDD) not required for receiving institutions given confirmed exchange attribution. Standard VASP due diligence applies.
Sanctions Compliance	No nexus to sanctioned entities, jurisdictions (Iran, DPRK, Russia SDN), or OFAC-designated addresses identified.

14. Investigator Notes & Annotations

#	Note	Priority
1	03:00–04:00 UTC outflow window is a strong operational fingerprint. Cross-reference with known Binance settlement schedules to confirm exact exchange attribution.	HIGH
2	The 1,572.11 BTC inflow (2025-10-03) is atypical in size. Recommend tracing input UTXOs upstream to confirm source cluster identity.	HIGH
3	Downstream P2SH (3…) recipients should be independently labelled via Chainalysis/Elliptic for complete outflow attribution.	MEDIUM
4	Dust transactions present. Low priority but worth monitoring for any scripting or covert signalling use case.	LOW
5	Coinbase interaction (secondary) — if used for inter-exchange arbitrage, the Coinbase leg may reveal additional fiat off-ramp exposure.	MEDIUM
6	Continued live monitoring recommended. Alert thresholds suggested: any single outflow > 1,000 BTC, or daily volume > 2,000 BTC.	HIGH

15. Overall Investigation Conclusion & Confidence Assessment

Overall Assessment: LEGITIMATE EXCHANGE TREASURY INFRASTRUCTURE

bc1qf8kep70t232jtajg2x4r8dhtuvtd7kuea8ve9w02qy5k4wncyl7spmnfme is a high-throughput institutional Bitcoin wallet operating as a Tier-1 Liquidity Router within the Binance / OKX inter-exchange network. Its behavioural profile — UTXO engineering, automated scheduling, 500 BTC peeling chains, exchange-labelled counterparties, and ~$1.85B lifetime throughput — is entirely consistent with regulated exchange treasury operations.

Key Findings:

- Attribution: Centralized Exchange (Binance / OKX) — 95% confidence
- Financial scale: 2,403 BTC (~$174 M) current balance | ~$1.85 B lifetime throughput
- Wallet class: Native SegWit (Bech32 / P2WPKH) — modern, efficient key management
- Operational pattern: Automated 500 BTC peeling with 03:00–04:00 UTC settlement window
- Risk profile: LOW across all AML criteria. No illicit exposure detected.
- OSINT corroboration: Arkham Intelligence, Whale Alert, Rich List #435

Recommended Actions:

- Set live monitoring alerts: single outflow > 1,000 BTC or daily volume > 2,000 BTC
- Trace the 1,572.11 BTC (2025-10-03) input UTXOs to fully map the inflow cluster
- Submit to Chainalysis / Elliptic for independent attribution if required for legal proceedings

Confidence Assessment Matrix

Attribute	Confidence	Basis
Wallet Classification	HIGH	UTXO patterns, volume, and automation signatures are all consistent.
Exchange Attribution	HIGH	Arkham tagging + cluster analysis + flow corroboration.
Fund Provenance	HIGH	Traceable to exchange institutional liquidity pools.
AML Clearance	HIGH	All criteria pass. No adverse findings identified.
Ownership Identity	HIGH	95% probability CEX. Cross-verified via multiple tools.
Operational Intent	HIGH	Treasury management / liquidity routing — no ambiguity.
Regulatory Standing	MEDIUM	Binance/OKX are regulated but subject to ongoing global scrutiny.