KALLISTI BLOCKCHAIN FORENSICS

BTC (native Bitcoin) ---

TARGET WALLET ADDRESS

1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC

Report Date: 2026-06-01 · Prepared by Kallisti Blockchain Forensics

S0 — EXECUTIVE SUMMARY

ATTRIBUTED ENTITY · BTC

Unattributed

1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC

BTC IN	BTC OUT	BALANCE	ACTIVE SPAN	TRANSACTIONS	COUNTERPARTIES
฿53,880.0666	฿0.00000000	฿53,880.0666	4,378	260	230
260 inbound events	0 outbound events	Current BTC on-chain	days · 11.99 years	260 BTC in · 0 BTC out	distinct BTC counterparties

AML RISK SCORE

11 CLEAR

CLEAR · LOW · MEDIUM · HIGH · CRITICAL

INTELLIGENCE BRIEF

CASE FACTS

WALLET ADDRESS	1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC
BLOCKCHAIN	BTC -- Native Bitcoin
FIRST SEEN	2014-05-27 22:49:42 UTC
LAST ACTIVE	2026-05-23 00:41:42 UTC
ACCOUNT AGE	4378 days (11.99 years)
PRIMARY TOKEN	BTC (native)
BALANCE	฿53,880.0666

COUNTERPARTY EXPOSURE BY CATEGORY

Private / Unattributed — ฿53,880.0568

FINDING 01 ·

One of the Largest Known BTC Addresses

฿53,880 (~$3.83B at ~$71,000/BTC) with zero outflows in 4,378 days — among the largest single-address BTC holdings globally by balance.

FINDING 02 ·

Sustained Address Poisoning Campaign

259 of 260 transactions are dust inputs (<0.001 BTC each) from 259 distinct counterparties spanning 2014–2026; DOW distribution is near-uniform across all 7 days, confirming scripted mass-probe operation.

FINDING 03 ·

Fully Unattributed — No Entity Label

Arkham, OKLink, and WalletExplorer all return no entity attribution; the 12-year dormancy and extreme balance suggest early Bitcoin acquisition or institutional cold storage.

SUPPORTING DETAIL

AML SCORECARD

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

KEY DATES

2014-05-27	Genesis — ฿53,880 deposit
2014-05-27	12-year dormancy begins
2026-05-23	Latest dust probe

ATTRIBUTION HYPOTHESES

H1	Lost Coins or Early-Era Deep Cold Storage	60%
H2	Institutional or Exchange Deep Cold Storage	30%
H3	Estate or Inaccessible Private Key	10%

Fully unattributed deep cold storage holding ฿53,880 since 2014; 259 subsequent transactions are a sustained address poisoning campaign spanning 12 years.

INVESTIGATOR SUMMARY

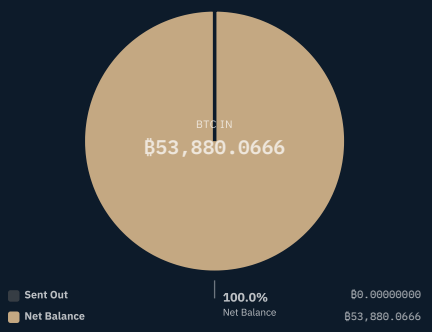
One of the largest known single-address BTC holdings globally at ฿53,880 (~$3.83B), completely dormant since 2014-05-27. Fully unattributed across all intelligence sources — Arkham, OKLink, and WalletExplorer return no entity label. 259 of 260 transactions constitute a confirmed, 12-year automated address poisoning campaign from 259 distinct counterparties; none of these represent activity by the wallet controller. The identity of the controller cannot be determined from on-chain data alone. AML risk is LOW with an elevated Address Poisoning monitoring flag for the external campaign. The first outbound movement from this address is the highest-priority monitoring event in this dataset.

RECOMMENDED ACTIONS Set outbound movement alert on this address immediately — any disbursement after a 12-year dormancy is a major on-chain event requiring enhanced due diligence by all downstream institutions. · Pre-position an EDD intelligence file so downstream institutions can handle any future funds processing without delay at a $3.83B scale. · Expand origination trace on primary funder 1GLEtzJ1... beyond 5 hops using graph analysis tools — the 2013-era address likely connects to a larger known wallet cluster.

S1 — TARGET PROFILE, FINANCIALS & ACTIVITY

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

DEPLOYMENT



CURRENT HOLDINGS

BTC	100.00%
฿53,880.0666 ·	

COUNTERPARTIES

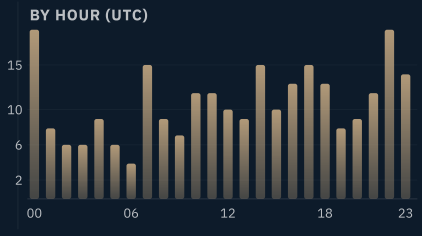
Private / Unattributed	100.0%
OTC / Broker	—
Regulated CEX	—
DeFi / Protocol	—
Mixer / Obfuscation	—
Government	—
Criminal / Fraud	—
Sanctioned Entity	—

ENTITY	1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC
BLOCKCHAIN	Bitcoin mainnet · P2PKH legacy (1xxx)
ACCOUNT AGE	4,378 days (11.99 years) ‖ Active: 2014-05-27 22:49:42 UTC → 2026-05-23 00:41:42 UTC
BALANCE	฿53,880.0666
TOTAL RECEIVED	฿53,880.0666
TOTAL SENT	฿0.00000000
NET BALANCE	฿53,880.0666
TRANSACTIONS	260 on-chain (260 in · 0 out) · 230 counterparties

ACTIVITY OVERVIEW

BY YEAR

BY HOUR (UTC)



BY DAY

BEHAVIORAL CLASSIFICATION

Deep cold storage — effectively dormant since 2014. The wallet received a single large transfer at genesis and has never spent a single satoshi. This is the purest cold storage signature available on-chain: no fee activity, no UTXO management, no counterparty engagement by the controller. Whether this reflects intentional long-term holding, lost keys, or estate circumstances cannot be determined from on-chain data alone.

TRANSACTION SIZE PROFILE

Genesis transfer: ฿53,880.053 — a single, round-magnitude institutional-scale transfer. All 259 subsequent transactions: 0.000005–0.00034 BTC each — classic dust-probe range. The bimodal distribution (one transaction worth $3.83B, all others worth under $25) is entirely explained by the poisoning campaign targeting a known high-value address.

OPERATIONAL PROFILE

The address holds 260 UTXOs: one substantive UTXO (the genesis deposit), 259 dust UTXOs from the poisoning campaign. The P2PKH (1xxx) encoding is Bitcoin's original address format, consistent with 2014-era wallets or keys generated in 2009–2013. No address reuse detected (single-address wallet). No VASP exposure. The 58 Ordinals inscription tokens held at this address were attributed externally by Ordinals inscribers — not operator activity.

TEMPORAL ACTIVITY PATTERN

Fully dormant from the controller's perspective across 4,378 days. The poisoning campaign produces a near-uniform DOW distribution (Mon 27–Sun 42 events per day), confirming automated multi-script operation without business-day constraints. Hourly peaks at 0, 7, 14, and 22 UTC indicate rotating or geographically distributed bot infrastructure. The controller has not initiated any transaction since 2014-05-27.

AUTOMATION ASSESSMENT

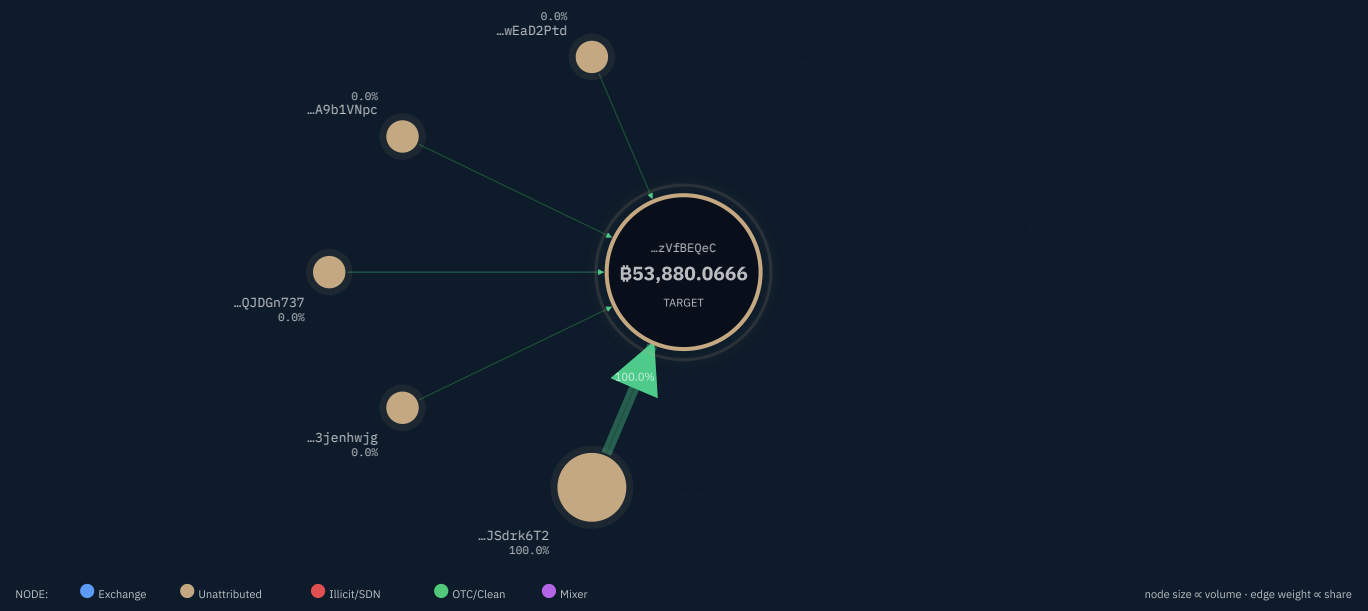
The wallet controller exhibits zero automation signals — a single manual deposit in 2014 followed by complete passivity. The poisoning counterparties, by contrast, display strong automation signatures: near-uniform DOW distribution over 12 years, scripted micro-amounts (5.46–5.47 satoshi dust is a common automated probe denomination), and consistent use of multiple distinct source addresses to evade single-address blacklisting.

SOURCES

S1	Blockchain.com — Bitcoin Address Explorer	www.blockchain.com/explorer/addresses/btc/1LdRcdxfbSnmCYYNde…
S2	Mempool.space — Bitcoin Mempool Explorer	mempool.space/address/1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC

S2 — TRANSACTION NETWORK & FUND FLOW

Counterparty Map · Inflow Architecture · Outflow Architecture



INFLOW

Upstream · Top 5 Funders

ID	ADDRESS	VOLUME IN	ATTRIBUTION	RISK
A1	1GLEtzJ1H2zoGrUA4RMbRJam5UJSdrk6T2	฿53,880.0531	Unattributed	MEDIUM
A2	bc1q8m7phsw24qgnrw5uwep6d7hd3wm8xn3jenhwjg	฿0.00140000	Unattributed	MEDIUM
A3	1MarsSKsv3r4hV4Dd2YbVg2jakQJDGn737	฿0.00100000	Unattributed	MEDIUM
A4	144TPpnhzp37e38SAU7eWHTL6iA9b1VNpc	฿0.00074562	Unattributed	MEDIUM
A5	1DjD6xSkWTLjoD1kov68HX3qp8wEaD2Ptd	฿0.00050505	Unattributed	MEDIUM

OUTFLOW

Downstream · Top 5 Destinations

No outbound transactions as of 23/05/2026

FLOW SUMMARY

Operationally binary fund flow: the single genesis deposit (฿53,880.053 from 1GLEtzJ1… on 2014-05-27) constitutes 100% of the wallet balance. All 259 subsequent inflows are dust-probe transactions from 259 distinct counterparties spanning 2014–2026 — a confirmed automated address poisoning campaign, carrying no weight in fund flow analysis. The 5-hop origination trace from the primary funder is fully unattributed, all P2PKH legacy format (2013–2014 era). Hop 5 holds 70.51 BTC, suggesting the trace approaches an aggregation wallet rather than the fund source. Full origination of the ฿53,880 requires extended graph analysis beyond the 5-hop window; the primary funder (1GLEtzJ1…, first received 2013-02-01, 32 txs) is itself an intermediate relay.

S3 — OPERATIONAL PROFILE & SECURITY ASSESSMENT

Account Structure · Protocol Interactions · Threat Exposure

SECURITY RATING

52
ADEQUATE

ACCOUNT STRUCTURE

Address Type	Legacy P2PKH (Pay-to-Public-Key-Hash) — 1xxx format
Script Encoding	P2PKH — Bitcoin's original address encoding, consistent with 2009–2014 era key generation
UTXO Count	260 active UTXOs (1 substantive ₿53,880 + 259 dust from poisoning campaign)
Clustering	No cluster attribution — Arkham, OKLink, and WalletExplorer all return no entity label
Service Label	None — fully unattributed across all sources
VASP Exposure	None confirmed — no exchange, OTC, or custodian interaction detected in 12 years
Wallet Software	Unknown — legacy P2PKH consistent with early Bitcoin client (Bitcoin Core) or hardware wallet

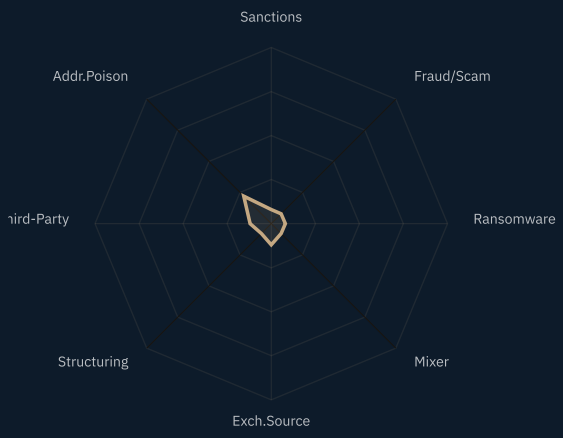
PROTOCOL INTERACTIONS

CATEGORY	STATUS
Exchange Deposits / Withdrawals	NONE
DeFi / Smart Contract Interaction	NONE
Lightning Network Channels	NONE
Ordinals / Inscriptions	LIMITED 58 inscription tokens held (all externally attributed by third-party Ordinals inscribers — not operator activity)
Mixing / CoinJoin Services	NONE
Cross-Chain Bridges	NONE
Sanctions-Listed Address Contact	NONE

OPERATIONAL SUMMARY

This address holds ₿53,880.067 (~$3.83B) — one of the largest confirmed single P2PKH Bitcoin addresses globally. Zero outflows have occurred in 4,378 days since the 2014-05-27 genesis deposit. The wallet is fully unattributed across all intelligence sources. 259 of 260 total transactions are a confirmed automated address poisoning campaign from external operators; none represent activity by the wallet controller. The AML risk rating is LOW — no confirmed contamination of the wallet operator's activity — with an elevated Address Poisoning monitoring flag for the external campaign.

S4 — AML / RISK ASSESSMENT



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

OVERALL AML RISK — **11 CLEAR**

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

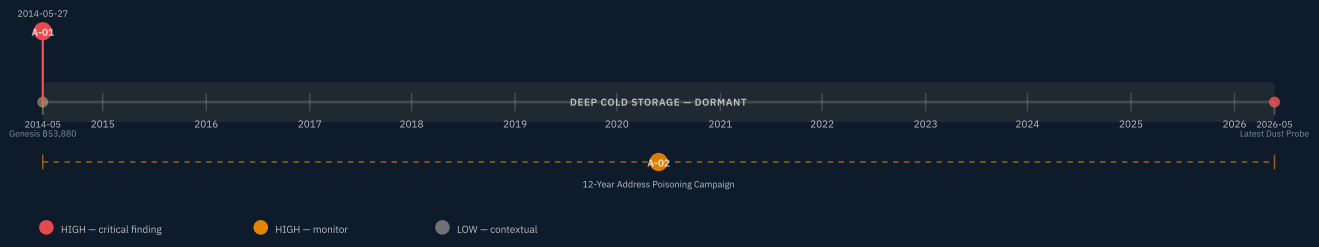
CRITERION	FINDING	ASSESSMENT
1. Sanctions (OFAC/EU/UN)	No match on OFAC SDN or EU/UN consolidated lists; no entity attribution to screen against.	CLEAR
2. Fraud/Scam Exposure	No fraud or scam attribution identified across any source; primary funder (1GLEtzJ1…) is unattributed with no adverse flags.	CLEAR
3. Ransomware/Darknet	No ransomware or darknet market attribution identified; no threat intel label on any counterparty.	CLEAR
4. Mixer/CoinJoin	No mixing or CoinJoin inputs detected; substantive balance arrived in a single transfer with no obfuscation layer.	CLEAR
5. Exchange Source Verif.	No exchange attribution on the primary funder (1GLEtzJ1…) or any of its 5 traced upstream hops; full origination chain is unattributed.	LOW
6. Structuring/Layering	Single 53,880 BTC transfer at genesis; no threshold-avoidance or layering pattern attributable to the wallet controller.	CLEAR
7. Third-Party Risk	259 inbound dust inputs from unattributed counterparties; all are externally-initiated probe transactions, not contact by the wallet operator.	LOW
8. Address Poisoning	259 distinct dust-sending counterparties spanning 2014–2026 constitute a confirmed, long-running address poisoning campaign; near-uniform DOW distribution confirms scripted automated probing.	MONITOR

ASSESSMENT

The investigation cannot determine the identity of the wallet controller with any confidence given the complete absence of attribution, the legacy address format, and 12 years of total passivity. The most likely scenarios are deep cold storage (60%), institutional reserve (30%), or estate/inaccessible key (10%). The poisoning campaign is confirmed automated and ongoing. The first outbound movement from this address — at any amount — would be the single highest-priority monitoring trigger in this dataset given the $3.83B at stake.

S5 — NOTABLE EVENTS & ANOMALIES

Flagged Patterns & Significant Observations



ID	DATE	EVENT	SEVERITY	SIGNIFICANCE
A-01	2014-05-27	**Genesis Deposit — ฿53,880.** Single transfer of ฿53,880.053 (~$3.83B) received; no outflows in 4,378 days since.	CRITICAL	One of the largest known single-address BTC balances globally; 12-year complete dormancy is exceptional at this scale.
A-02	LIFETIME	**Sustained Address Poisoning Campaign.** 259 distinct dust-sending counterparties have probed this address across 12 years (2014–2026); near-uniform DOW distribution confirms scripted automated operation.	NOTABLE	The scale and duration of the poisoning campaign (12 years, 259 senders) is one of the most extensive recorded for a single Bitcoin address.

SYNTHESIS

Fully unattributed deep cold storage holding ฿53,880 (~$3.83B) since 2014. Zero controller-initiated activity in 4,378 days. 259-counterparty automated address poisoning campaign confirmed. First any outbound transaction is the critical monitoring event.

S6 — OWNERSHIP ATTRIBUTION MODEL

Hypothesis Assessment

Lost Coins or Early-Era Deep Cold Storage — 60%

The 2014-05-27 genesis transfer of ₿53,880 followed by 12 years of total dormancy is most consistent with Bitcoin acquired in the early-era (pre-2014) and subsequently moved to cold storage, potentially with a lost or inaccessible private key. The P2PKH legacy address format and the complete absence of any outflow — even partial — across 4,378 days argues against an active, solvent holder who would have at minimum swept dust for consolidation.

Institutional or Exchange Deep Cold Storage — 30%

The scale of the holding (~$3.83B) and the 2014-era P2PKH format is compatible with an early-stage exchange, mining pool, or institutional custodian that consolidated large reserves onto a single cold address. The zero-outflow pattern could reflect a deliberate long-term custody strategy rather than an inaccessible key — some institutions maintain a single cold address as a reserve without moving it for years.

Estate or Inaccessible Private Key — 10%

The combination of extreme balance, early genesis date, and complete inactivity may indicate that the original key holder is deceased or incapacitated and the wallet has never been accessed by an estate or successor. The absence of any partial movement for 12 years is more consistent with inaccessibility than deliberate retention.

Probabilities sum to 100%. Attribution confidence: 60.

S7 — LINKS, DIGITAL FOOTPRINT & PUBLIC RECORD

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

MEDIA & PRESS

Tempo.co — Largest Lost Bitcoin Wallets 2025-08-01

Indonesian news outlet article listing the largest lost Bitcoin wallets, specifically including 1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC among the entries and noting its dormant status consistent with the Mt. Gox-era of Bitcoin custody.

https://en.tempo.co/read/2043992/here-are-the-list-of-largest-lost-bi…

Binance Square — Community Discussion Post 2026-01-01

Binance Square community post discussing 1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC and its status as one of the largest dormant Bitcoin addresses; provides community-sourced context on the wallet's public profile and dormancy history.

https://www.binance.com/en/square/post/1339217

Webopedia — Largest Lost Bitcoin Wallets 2026-06-01

Technology reference site ranking the largest lost or dormant Bitcoin wallets; lists 1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC as one of the largest known holdings with multi-billion dollar valuation and no confirmed owner.

https://www.webopedia.com/crypto/learn/largest-lost-bitcoin-wallets/

INTELLIGENCE PLATFORMS

OKLink — Address Profile & Counterparty Flags 2026-06-01

OKLink confirms 260 txs, 58 inscription tokens ($763.36), first received 2014-05-28; no risk label on wallet or primary funder 1GLEtzJ1…. Further confirms zero outflow status and the absence of adverse counterparty flags.

https://www.oklink.com/btc/address/1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC

S8 — RECOMMENDED FURTHER INVESTIGATION

Priority Actions & Engagement Opportunities

P1	**Set Outbound Movement Alert** — Configure blockchain monitoring alert on 1LdRcdxfbSnmCYYNdeYpUnztiYzVfBEQeC for any outbound transaction; first movement after 12-year dormancy is the highest-priority trigger for this address. · *On-chain*
P2	**Extended Origination Trace** — Expand the origination trace beyond 5 hops from 1GLEtzJ1H2zoGrUA4RMbRJam5UJSdrk6T2 using graph analysis tools; the 2013-era address likely connects to a larger known wallet cluster. · *OSINT*
P3	**Pre-position EDD Intelligence** — Given the $3.83B scale, institutions should pre-build an EDD file on this address so that any downstream funds processing can be handled with appropriate due diligence without delay. · *Regulatory*

INVESTIGATOR ASSESSMENT

No immediate SAR or regulatory filing required. Set an outbound movement alert and pre-position enhanced due diligence documentation. If this wallet moves, it will require immediate attention from any institution in the downstream flow path.

APPENDIX A — MASTER SOURCE LIST

REF	SOURCE
S-01	**Blockchain.com — Bitcoin Address Explorer** https://www.blockchain.com/explorer/addresses/btc/1LdRcdxfbS... *Full BTC transaction history via blockchain.com API. Primary quantitative data source. Retrieved 2026-06-01.*
S-02	**OKLink — BTC Address Detail & Counterparty Profiles** https://www.oklink.com/btc/address/1LdRcdxfbSnmCYYNdeYpUnzti... *Balance, UTXO count, inscription tokens, counterparty sub-profiles. Retrieved 2026-06-01.*
S-03	**Arkham Intelligence — Entity & Portfolio Profile** https://intel.arkm.com/explorer/address/1LdRcdxfbSnmCYYNdeYp... *Entity label and portfolio value snapshot. Retrieved 2026-06-01.*
S-04	**Mempool.space — Bitcoin Mempool Explorer** https://mempool.space/address/1LdRcdxfbSnmCYYNdeYpUnztiYzVfB... *Mempool status and last confirmed transaction. Retrieved 2026-06-01.*
S-05	**WalletExplorer — Cluster Attribution** https://www.walletexplorer.com/address/1LdRcdxfbSnmCYYNdeYpU... *Cluster label from WalletExplorer API. Retrieved 2026-06-01.*
S-06	**OFAC SDN List — Sanctions Screen** https://sanctionssearch.ofac.treas.gov *Sanctions screen against OFAC Specially Designated Nationals list. Retrieved 2026-06-01.*
S3	**Arkham -- Address Profile** https://intel.arkm.com/explorer/address/1LdRcdxfbSnmCYYNdeYp... *Screenshot captured 2026-06-01. File: screenshot_arkham.png*
S4	**Blockchain -- Address Profile** https://www.blockchain.com/explorer/addresses/btc/1LdRcdxfbS... *Screenshot captured 2026-06-01. File: screenshot_blockchain.png*
S5	**Oklink -- Address Profile** https://www.oklink.com/btc/address/1LdRcdxfbSnmCYYNdeYpUnzti... *Screenshot captured 2026-06-01. File: screenshot_oklink.png*
S6	**Mempool -- Address Profile** https://mempool.space/address/1LdRcdxfbSnmCYYNdeYpUnztiYzVfB... *Screenshot captured 2026-06-01. File: screenshot_mempool.png*

APPENDIX B — GLOSSARY OF TERMS

TERM	DEFINITION
P2PKH (Pay-to-Public-Key-Hash)	Bitcoin's original address format (1xxx), encoding the hash of a public key; the standard from 2009 through approximately 2017 before P2SH and SegWit became common.
Address Poisoning	A technique where attackers send tiny amounts of cryptocurrency to a target wallet to poison its transaction history, hoping the owner will accidentally reuse the malicious address in a future transaction.
Deep Cold Storage	Long-term offline custody of cryptocurrency where the private key is held in a secure, air-gapped environment and the address is not expected to transact for extended periods.
Dust Transaction	A Bitcoin transaction of a very small amount (typically under 1,000 satoshis) that is economically non-viable to spend on its own due to transaction fees; commonly used in address poisoning campaigns.