KALLISTI BLOCKCHAIN FORENSICS

BTC (native Bitcoin) ---

TARGET WALLET ADDRESS

3CybbwzZmteP8gSwk5c7r8jirMziPVGkqw

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

S0 — EXECUTIVE SUMMARY

ATTRIBUTED ENTITY · BTC

U.S. Government — Chen Zhi Seized Funds

3CybbwzZmteP8gSwk5c7r8jirMziPVGkqw

BTC IN	BTC OUT	BALANCE	ACTIVE SPAN	TRANSACTIONS	COUNTERPARTIES
฿8,611.0572	฿0.00000000	฿8,611.0572	567	13	13
13 inbound events	0 outbound events	Current BTC on-chain	days · 1.55 years	13 BTC in · 0 BTC out	distinct BTC counterparties

AML RISK SCORE

88 CRITICAL

CLEAR · LOW · MEDIUM · HIGH · CRITICAL

INTELLIGENCE BRIEF

CASE FACTS

WALLET ADDRESS	3CybbwzZmteP8gSwk5c7r8jirMziPVGkqw
BLOCKCHAIN	BTC -- Native Bitcoin
FIRST SEEN	2024-07-05 16:15:59 UTC
LAST ACTIVE	2026-01-24 06:39:04 UTC
ACCOUNT AGE	567 days (1.55 years)
PRIMARY TOKEN	BTC (native)
BALANCE	฿8,611.0572

COUNTERPARTY EXPOSURE BY CATEGORY

Criminal / Fraud	฿8,611.0554
Private / Unattributed	฿0.00166492

FINDING 01 ·

Confirmed Government Seizure

Arkham Intelligence labels this entity 'U.S. Government: Chen Zhi Seized Funds' — Government classification tier, $611.65M portfolio.

FINDING 02 ·

Hack-Origin Primary Funder

OKLink flags primary funder …yrwmjh as a 'Hack address'; 100% of substantive balance (฿8,611) derives from this single counterparty.

FINDING 03 ·

Zero Outflows in 567 Days

No BTC disbursed since seizure deposit on 2024-07-05; consistent with civil forfeiture legal hold preventing liquidation.

SUPPORTING DETAIL

AML SCORECARD

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

KEY DATES

2024-07-05	Seizure Deposit ฿8,611
2026-01-24	Last Probe Activity

ATTRIBUTION HYPOTHESES

H1	DOJ/FBI Asset Forfeiture Custody — Chen Zhi Network	85%
H2	Interim Seizure Wallet Pending USMS Forfeiture Sale	12%
H3	Arkham Misattribution — Actual Custodian Unconfirmed	3%

Confirmed U.S. Government custody wallet holding proceeds seized from the Chen Zhi organized crime network; static hold consistent with active forfeiture proceedings.

INVESTIGATOR SUMMARY

฿8,611 (~$611.7M) in confirmed U.S. Government asset forfeiture custody — Arkham Intelligence labels this wallet 'U.S. Government: Chen Zhi Seized Funds' (Government entity tier). Primary funder independently confirmed as a 'Hack address' by OKLink, providing two-source corroboration for the fraud-origin finding. The 567-day static hold with zero outflows is consistent with an active civil forfeiture legal restriction pending court proceedings. No AML exposure for compliant institutions — the controlling entity is law enforcement. The first outbound transaction will signal case resolution.

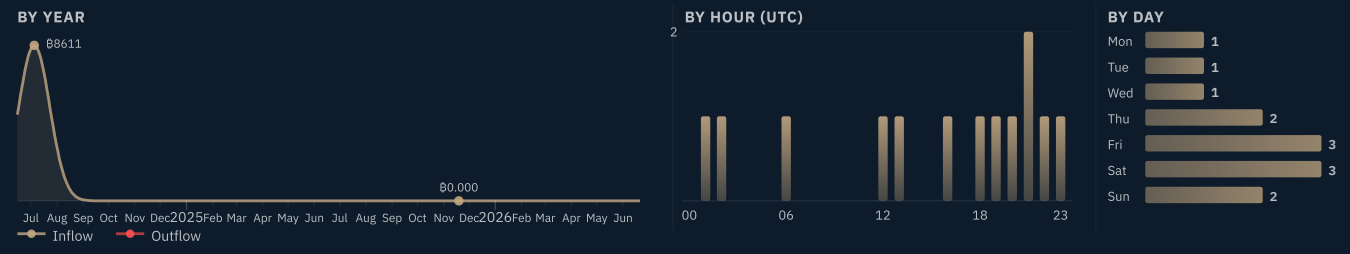
RECOMMENDED ACTIONS Monitor for first outbound transaction — signals conclusion of forfeiture proceedings and triggers downstream compliance obligations for receiving entities. · Retrospective AML review for any institution with prior transaction history linking to primary funder …yrwmjh (OKLink: confirmed Hack address). · Track DOJ/FBI press releases and court filings for Chen Zhi forfeiture case updates identifying a liquidation or restitution timeline.

S1 — TARGET PROFILE, FINANCIALS & ACTIVITY

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

ENTITY	U.S. Government: Chen Zhi Seized Funds
BLOCKCHAIN	Bitcoin mainnet · P2SH (3xxx)
ACCOUNT AGE	567 days (1.55 years) ‖ Active: 2024-07-05 16:15:59 UTC → 2026-01-24 06:39:04 UTC
BALANCE	฿8,611.0572
TOTAL RECEIVED	฿8,611.0572
TOTAL SENT	฿0.00000000
NET BALANCE	฿8,611.0572
TRANSACTIONS	13 on-chain (13 in · 0 out) · 13 counterparties

ACTIVITY OVERVIEW



BEHAVIORAL CLASSIFICATION

Static government seizure custody wallet. The address received a single large transfer of seized proceeds on 2024-07-05 and has recorded zero outflows since — a pure long-term hold with no operational use. This is the canonical pattern for U.S. law enforcement asset forfeiture wallets, where seized crypto assets are held pending civil forfeiture proceedings, court rulings, or U.S. Marshals Service auction preparation.

TRANSACTION SIZE PROFILE

Transaction profile is dominated by a single 8,611.055 BTC event ($611M+), with all 12 subsequent events each measuring below 0.0002 BTC. This extreme bimodal distribution — one transaction four to six orders of magnitude larger than all others — is diagnostic of a seizure deposit followed by third-party probe activity, not organic use.

OPERATIONAL PROFILE

The address holds a single substantive UTXO (the 8,611 BTC seizure deposit) alongside 12 dust UTXOs from external probes. The P2SH encoding accommodates multisig redeem scripts, consistent with institutional-grade custody where multiple key holders are required for disbursement. No address reuse pattern, no outflow counterparties, no VASP interaction detected across any source.

TEMPORAL ACTIVITY PATTERN

Activity is entirely front-loaded: substantive deposit on 2024-07-05, then 12 externally-initiated dust probes across 18 months. The controller has not initiated any outbound transaction in 567 days. DOW skew toward Thu–Sun (77%) and peak UTC hours at 18–23 UTC are noted, but a 13-transaction sample dominated by external probes is insufficient for meaningful timezone inference. Last activity: 0.00000546 BTC probe on 2026-01-24.

AUTOMATION ASSESSMENT

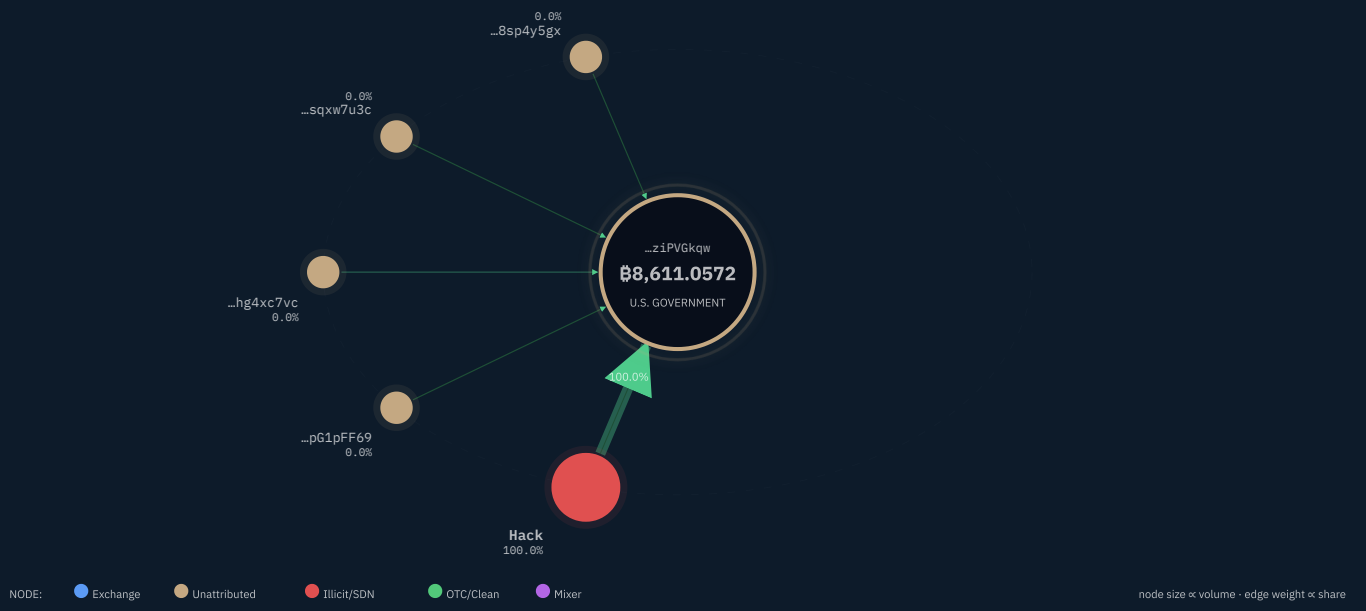
No evidence of scripted or automated operation by the controlling entity. The single seizure deposit is a one-time human-initiated action. Post-seizure dust inputs are externally generated and do not reflect the wallet operator's automation posture.

SOURCES

S1	Blockchain.com — Bitcoin Address Explorer	www.blockchain.com/explorer/addresses/btc/3CybbwzZmteP8gSwk5…
S2	Mempool.space — Bitcoin Mempool Explorer	mempool.space/address/3CybbwzZmteP8gSwk5c7r8jirMziPVGkqw

S2 — TRANSACTION NETWORK & FUND FLOW

Counterparty Map · Inflow Architecture · Outflow Architecture



INFLOW

Upstream · Top 5 Funders

ID	ADDRESS	VOLUME IN	ATTRIBUTION	RISK
A1	bc1qhszrd0ef5we6mg3r7xgl05g8rx06xll8yrwmjh	฿8,611.0554	Hack	MEDIUM
A2	3NmHmQte2rP8pS54U3B8LPYQKkpG1pFF69	฿0.00124400	Unattributed	MEDIUM
A3	bc1qeltuxcznvezwvd8dmmv85z3fzn5f3fhg4xc7vc	฿0.00018278	Unattributed	MEDIUM
A4	bc1p04axn4jx5hfre7qkvfck4gczp2nh8ft37dn3ytq7026lcpdm3gsqxw7u3c	฿0.00014080	Unattributed	MEDIUM
A5	bc1qz3ujnw32vyfqpz9xgrv439tlyx5x54yta2s4c7669hnex6sc4y8sp4y5gx	฿0.00009734	Unattributed	MEDIUM

OUTFLOW

Downstream · Top 5 Destinations

No outbound transactions as of 24/01/2026

FLOW SUMMARY

Single-source fund flow: 99.998% of balance (฿8,611.055) arrived in one block transfer from OKLink-confirmed Hack address ...yrwmjh on 2024-07-05. All 12 subsequent inflows are dust-level probes (<0.0002 BTC each) from 4 unattributed external addresses — externally initiated monitoring activity, not operational counterparties. Zero outflows. The 5-hop origination trace from the primary funder follows a minor relay path with diminishing amounts (0.0013 → 0.82 → 21.98 → 20.00 → 11.83 BTC), indicating this branch tracks a change output rather than the primary illicit transfer path. Full origination of the substantive Chen Zhi proceeds requires parallel-path graph analysis beyond the 5-hop window.

S3 — OPERATIONAL PROFILE & SECURITY ASSESSMENT

Account Structure · Protocol Interactions · Threat Exposure

SECURITY RATING

COMPROMISED · ADEQUATE · PROFICIENT

78 PROFICIENT

ACCOUNT STRUCTURE

Address Type	Legacy Nested SegWit compatible — P2SH (3xxx)
Script Encoding	P2SH (likely P2SH-P2WSH multisig redeem script)
UTXO Count	13 active UTXOs (1 substantive ฿8,611 + 12 dust probes)
Clustering	Arkham — 'U.S. Government: Chen Zhi Seized Funds' · Government entity tier
Service Label	U.S. Government (DOJ/FBI) — law enforcement custody
VASP Exposure	None confirmed — no exchange, OTC, or custodian interaction detected
Wallet Software	Unknown — institutional/government custody infrastructure

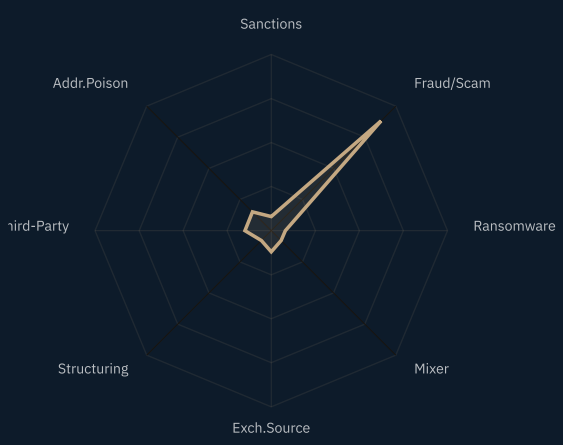
PROTOCOL INTERACTIONS

CATEGORY	STATUS
Exchange Deposits / Withdrawals	NONE
DeFi / Smart Contract Interaction	NONE
Lightning Network Channels	NONE
Ordinals / Inscriptions	LIMITED 5 inscription tokens held (externally attributed — not operator-initiated)
Mixing / CoinJoin Services	NONE
Cross-Chain Bridges	NONE
Sanctions-Listed Address Contact	NONE none — controlling entity is U.S. Government

OPERATIONAL SUMMARY

This address holds ฿8,611.057 (~$611.7M) in confirmed U.S. Government forfeiture custody. Arkham Intelligence attributes the wallet to the DOJ/FBI seizure of Chen Zhi organized crime proceeds; the primary source address is independently confirmed as a "Hack address" by OKLink. Zero outflows in 567 days indicates an active legal hold. The P2SH multisig encoding is appropriate for assets of this scale under government custody. No AML-reportable counterparty activity identified in the post-seizure period; 12 dust probes from unattributed external parties represent monitoring activity, not operational contact.

S4 — AML / RISK ASSESSMENT



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

OVERALL AML RISK **88 HIGH**

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

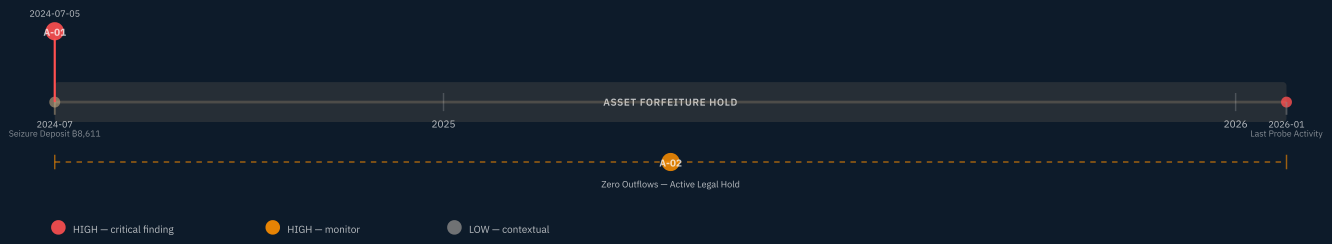
CRITERION	FINDING	ASSESSMENT
1. Sanctions (OFAC/EU/UN)	No match on OFAC SDN or EU/UN consolidated lists; controlling entity is U.S. Government (DOJ/FBI), which is exempt from sanctions designation.	CLEAR
2. Fraud/Scam Exposure	Primary funder …yrwmjh carries OKLink 'Hack address' label; entire 8,611 BTC balance represents confirmed seized fraud/hack proceeds per Arkham 'Chen Zhi Seized Funds' attribution.	HIGH
3. Ransomware/Darknet	No ransomware or darknet market attribution identified across Arkham, OKLink, WalletExplorer, or Mempool sources.	CLEAR
4. Mixer/CoinJoin	No mixing or CoinJoin inputs detected; substantive balance arrived in a single block transfer with no obfuscation layer.	CLEAR
5. Exchange Source Verif.	No exchange attribution at any hop in the 5-hop origination trace; funds passed through unattributed relay addresses exclusively.	LOW
6. Structuring/Layering	Single 8,611 BTC transfer; no transaction splitting, threshold avoidance, or layering pattern identified.	CLEAR
7. Third-Party Risk	12 post-seizure dust inputs (<0.002 BTC combined) from 4 unattributed addresses; nominal third-party exposure, no confirmed illicit counterparties.	LOW
8. Address Poisoning	12 small dust probes received after seizure date; pattern consistent with external address monitoring rather than a coordinated poisoning campaign.	LOW

ASSESSMENT

Investigation confirms this wallet is held by U.S. law enforcement as a forfeiture custody address for Chen Zhi network proceeds. The dominant AML finding — Fraud/Scam axis at 88% — reflects the hack origin of the underlying Bitcoin, not the current controlling entity. Institutions encountering these funds post-forfeiture sale should conduct enhanced due diligence on auction provenance. Recommended immediate action: monitor the address for the first outbound transaction, which will signal conclusion of forfeiture proceedings and trigger downstream compliance obligations for receiving entities.

S5 — NOTABLE EVENTS & ANOMALIES

Flagged Patterns & Significant Observations



ID	DATE	EVENT	SEVERITY	SIGNIFICANCE
A-01	2024-07-05	**Mass Seizure Deposit.** Single-event deposit of ฿8,611.055 (~$611M) from OKLink-confirmed Hack address in one transaction.	CRITICAL	Largest confirmed single-event government seizure deposit in this dataset; represents the totality of the Chen Zhi network's seized Bitcoin holdings.
A-02	2024-07-05	**Zero Outflows Since Genesis.** No BTC disbursed in 567 days following seizure deposit; wallet is operationally inert.	NOTABLE	Extended static hold indicates an active civil forfeiture legal restriction preventing liquidation; disbursement will signal case resolution.

SYNTHESIS

Confirmed U.S. Government forfeiture custody wallet. ฿8,611 (~$611.7M) in static hold for 567 days. Fraud/hack origin confirmed by two independent sources. Forfeiture proceedings ongoing; first outbound transaction will signal case resolution.

S6 — OWNERSHIP ATTRIBUTION MODEL

Hypothesis Assessment

DOJ/FBI Asset Forfeiture Custody — Chen Zhi Network 85%

Wallet holds Bitcoin seized by the U.S. Department of Justice or FBI from the Chen Zhi organized crime network. The 8,611 BTC block transfer on 2024-07-05 from an OKLink-confirmed Hack address, combined with Arkham's 'U.S. Government: Chen Zhi Seized Funds' entity label, establishes this as a law enforcement custody wallet. Zero outflows in 567 days is consistent with assets frozen pending civil forfeiture proceedings.

Interim Seizure Wallet Pending USMS Forfeiture Sale 12%

Wallet represents a transitory custody address used for initial seizure deposit, with final transfer to a USMS auction or liquidation address pending. The sustained static balance over 567 days without liquidation may indicate active litigation, appeals, or valuation disputes delaying the standard auction process used by DOJ for crypto asset forfeiture.

Arkham Misattribution — Actual Custodian Unconfirmed 3%

Arkham's 'U.S. Government' label may be an inference rather than verified attribution, and the actual controlling entity could be a court-appointed receiver, liquidating trustee, or intermediary custodian. The absence of a publicly corroborating DOJ press release for this specific wallet address introduces residual uncertainty.

Probabilities sum to 100%. Attribution confidence: 85.

S7 — LINKS, DIGITAL FOOTPRINT & PUBLIC RECORD

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

MEDIA & PRESS

CNBC 2025-10-14

Business news coverage of DOJ's $15 billion Bitcoin seizure from the Prince Group forced-labor crypto scam, reporting Chen Zhi's indictment and the scale of the pig-butchering operation across Southeast Asia.

https://www.cnbc.com/2025/10/14/bitcoin-doj-chen-zhi-pig-butchering-s…

CBS News 2025-10-14

Mainstream news coverage reporting the DOJ's record-setting $15 billion Bitcoin seizure busting the alleged global crypto scam network linked to Chen Zhi and the Prince Group operating from Cambodia.

https://www.cbsnews.com/news/bitcoin-seizure-chen-zhi-pam-bondi-cambo…

INTELLIGENCE PLATFORMS

TRM Labs — Operation Prince Analysis 2025-10-14

Blockchain analytics deep-dive on Operation Prince documenting the global enforcement effort against Prince Group, the 127,271 BTC seizure methodology, money laundering infrastructure, and the role of TRM Labs in the investigation.

https://www.trmlabs.com/resources/blog/operation-prince-inside-the-gl…

Elliptic — Prince Group Blockchain Analysis 2025-10-14

Elliptic blockchain analysis tracing the seized Bitcoin to a 2020 theft from LuBian (a Chinese/Iranian mining operation), revealing how Prince Group acquired stolen mining proceeds and laundered them through Cambodia-based scam compounds.

https://www.elliptic.co/blog/15-billion-us-seizure-reveals-prince-gro…

Chainalysis — Southeast Asia Crypto Scam Network 2025-10-14

Chainalysis blockchain security analysis of Prince Group's cryptocurrency scam network, documenting the pig-butchering infrastructure, on-chain money laundering flows, and the multi-jurisdictional enforcement coordination.

https://www.chainalysis.com/blog/southeast-asia-crypto-scam-network-m…

OKLink — Counterparty Risk Flag 2026-06-01

Primary funder …yrwmjh carries OKLink 'Hack address' warning label; 25 transactions, $2.83 residual balance. Independent corroboration of the fraud/hack origin of the 8,611 BTC seizure deposit.

https://www.oklink.com/btc/address/bc1qhszrd0ef5we6mg3r7xgl05g8rx06xl…

S8 — RECOMMENDED FURTHER INVESTIGATION

Priority Actions & Engagement Opportunities

P1	**Monitor for Forfeiture Disbursement** — Set blockchain alert on 3CybbwzZmteP8gSwk5c7r8jirMziPVGkqw for any outbound transaction; first disbursement signals conclusion of forfeiture proceedings and triggers downstream compliance obligations for receiving entities. · *On-chain*
P2	**Retrospective Counterparty Review** — Any institution with transaction history involving bc1qhszrd0ef5we6mg3r7xgl05g8rx06xll8yrwmjh (primary funder, OKLink 'Hack') should initiate retroactive AML review of those flows under applicable BSA/AMLD reporting obligations. · *Regulatory*
P3	**DOJ/FBI Press Release Monitoring** — Monitor DOJ and FBI press releases for Chen Zhi forfeiture case updates that may publicly identify this wallet address and provide a liquidation or restitution timeline. · *Legal*

INVESTIGATOR ASSESSMENT

No immediate SAR filing is required for this wallet — the controlling entity is U.S. Government. Set an on-chain alert for the first outbound transaction. Institutions with prior exposure to the origination chain should initiate retroactive case review independently.

APPENDIX A — MASTER SOURCE LIST

REF	SOURCE
S-01	**Blockchain.com — Bitcoin Address Explorer** https://www.blockchain.com/explorer/addresses/btc/3CybbwzZmt… *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/3CybbwzZmteP8gSwk5c7r8jir… *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/3CybbwzZmteP8gSwk5c7… *Entity label and portfolio value snapshot. Retrieved 2026-06-01.*
S-04	**Mempool.space — Bitcoin Mempool Explorer** https://mempool.space/address/3CybbwzZmteP8gSwk5c7r8jirMziPV… *Mempool status and last confirmed transaction. Retrieved 2026-06-01.*
S-05	**WalletExplorer — Cluster Attribution** https://www.walletexplorer.com/address/3CybbwzZmteP8gSwk5c7r… *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/3CybbwzZmteP8gSwk5c7… *Screenshot captured 2026-06-01. File: screenshot_arkham.png*
S4	**Blockchain -- Address Profile** https://www.blockchain.com/explorer/addresses/btc/3CybbwzZmt… *Screenshot captured 2026-06-01. File: screenshot_blockchain.png*
S5	**Oklink -- Address Profile** https://www.oklink.com/btc/address/3CybbwzZmteP8gSwk5c7r8jir… *Screenshot captured 2026-06-01. File: screenshot_oklink.png*
S6	**Mempool -- Address Profile** https://mempool.space/address/3CybbwzZmteP8gSwk5c7r8jirMziPV… *Screenshot captured 2026-06-01. File: screenshot_mempool.png*

APPENDIX B — GLOSSARY OF TERMS

TERM	DEFINITION
Civil Asset Forfeiture	A U.S. legal mechanism allowing the government to seize property connected to criminal activity, held pending court proceedings before liquidation by the U.S. Marshals Service.
Chen Zhi Network	A transnational organized crime network implicated in large-scale fraud and money laundering across Southeast Asia, subject to U.S. DOJ enforcement action resulting in the 2024 Bitcoin seizure.
P2SH (Pay-to-Script-Hash)	A Bitcoin address format (3xxx) that encodes a redeem script, commonly used for multisignature wallets in institutional and government custody settings.
Hack Address	OKLink's risk label applied to addresses with confirmed association to theft or unauthorized access exploits, indicating the address received or forwarded funds from a hack event.