CRYPTO WALLET RISK REPORT

Date: 2026-03-08 16:18:30 UTC
Address: `0x098b716b8aaf21512996dc57eb0615e2383e2f96`
Type: ETH

RISK LEVEL: HIGH

SUMMARY

This address has been flagged as HIGH RISK due to OFAC SDN sanctions match; GoPlus: other sanctions lists, blacklist, theft / attacks; Behavioral: rapid inbound-outbound turnover, retention time anomaly, same-day full-drain behavior, counterparty fan-in, new-counterparty ratio, repeated fixed-amount pattern, micro-transfer probing / dust, burstiness score; Counterparty: other sanctions lists, blacklist, theft / attacks. Immediate attention required.

Risk Group Overview

Group	Status	Summary
SANCTIONS & WATCHLISTS	FLAGGED	3 of 4 checks flagged
FINANCIAL CRIME	CLEAN	All checks clean
CYBER THREATS	FLAGGED	1 of 5 checks flagged
SMART CONTRACT RISKS	CLEAN	All checks clean
COUNTERPARTY: SANCTIONS & WATCHLISTS	FLAGGED	2 of 2 checks flagged
COUNTERPARTY: FINANCIAL CRIME	CLEAN	All checks clean
COUNTERPARTY: CYBER THREATS	FLAGGED	1 of 5 checks flagged
COUNTERPARTY: SMART CONTRACT RISKS	CLEAN	All checks clean
VELOCITY / LAYERING	FLAGGED	3 of 3 checks flagged
COUNTERPARTY STRUCTURE	FLAGGED	2 of 4 checks flagged
AMOUNT PATTERNS	FLAGGED	2 of 5 checks flagged
TIME ANOMALIES	FLAGGED	1 of 3 checks flagged

SANCTIONS & WATCHLISTS

Status: **FLAGGED**

	Category	Description	Status
✗	OFAC SDN	FLAGGED — Lazarus Group (UID: 27307)	Flagged
✓	UK Sanctions	Not found on UK Sanctions list	Clean
✗	Other Sanctions Lists	Address found on other sanctions lists (GoPlus)	Flagged
✗	Blacklist	Appears on industry doubt blacklists	Flagged

FINANCIAL CRIME

Status: **CLEAN**

	Category	Description	Status
✓	Money Laundering	No money laundering indicators found	Clean
✓	Financial Crime	No financial crime associations found	Clean
✓	Darkweb Transactions	No darkweb transaction history found	Clean
✓	Blackmail	No blackmail associations found	Clean
✓	Mixing Services	No mixing service usage detected	Clean

CYBER THREATS

Status: **FLAGGED**

	Category	Description	Status
✓	Cybercrime	No cybercrime associations found	Clean
✗	Theft / Attacks	Associated with theft or attack activity	Flagged
✓	Phishing	No phishing associations found	Clean
✓	Malicious Mining	No malicious mining activity found	Clean
✓	Fake KYC	No fraudulent KYC associations found	Clean

SMART CONTRACT RISKS

Status: **CLEAN**

	Category	Description	Status
✓	Honeypot Contracts	No honeypot contract associations found	Clean
✓	Fake Token Interface	No fake token interface associations found	Clean
✓	Fake Tokens	No fraudulent token associations found	Clean
✓	Gas Fee Abuse	No gas fee manipulation found	Clean
✓	Reinitialization Attack	No reinitialization attack associations found	Clean

COUNTERPARTY: SANCTIONS & WATCHLISTS

Status: **FLAGGED**

	Category	Description	Status
✗	Counterparty: Other Sanctions Lists	5 of 20 counterparties flagged	Flagged
✗	Counterparty: Blacklist	5 of 20 counterparties flagged	Flagged

COUNTERPARTY: FINANCIAL CRIME

Status: **CLEAN**

	Category	Description	Status
✓	Counterparty: Money Laundering	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Financial Crime	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Darkweb Transactions	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Blackmail	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Mixing Services	No counterparties flagged (20 checked)	Clean

COUNTERPARTY: CYBER THREATS

Status: **FLAGGED**

	Category	Description	Status
✓	Counterparty: Cybercrime	No counterparties flagged (20 checked)	Clean
✗	Counterparty: Theft / Attacks	5 of 20 counterparties flagged	Flagged
✓	Counterparty: Phishing	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Malicious Mining	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Fake KYC	No counterparties flagged (20 checked)	Clean

COUNTERPARTY: SMART CONTRACT RISKS

Status: **CLEAN**

	Category	Description	Status
✓	Counterparty: Honeypot Contracts	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Fake Token Interface	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Fake Tokens	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Gas Fee Abuse	No counterparties flagged (20 checked)	Clean
✓	Counterparty: Reinitialization Attack	No counterparties flagged (20 checked)	Clean

VELOCITY / LAYERING

Status: **FLAGGED**

	Category	Description	Status
✗	Rapid Inbound-Outbound Turnover	Turnover ratio: 0.47 (25 of 53 inbound ops forwarded within 24h)	Flagged
✗	Retention Time Anomaly	Median retention: 21.8h (37 in-out pairs analyzed)	Flagged
✗	Same-Day Full-Drain Behavior	Drain ratio: 0.42 (13 of 31 active days fully drained)	Flagged

COUNTERPARTY STRUCTURE

Status: **FLAGGED**

	Category	Description	Status
✓	Counterparty Fan-Out	Fan-out ratio: 0.30 (44 unique recipients in 147 outbound ops)	Clean
✗	Counterparty Fan-In	Fan-in ratio: 0.72 (38 unique senders in 53 inbound ops)	Flagged

✗	New-Counterparty Ratio	New-CP ratio: 0.79 (64 of 81 counterparties seen only once)	Flagged
✓	Counterparty Concentration Instability	Concentration instability: 0.0419 (HHI variance across 4 windows)	Clean

AMOUNT PATTERNS

Status: **FLAGGED**

	Category	Description	Status
✓	Amount Fragmentation (Structuring)	Structuring score: 0.00 (CV=8.18, 200 transactions)	Clean
✗	Repeated Fixed-Amount Pattern	Repeat ratio: 0.32 (most common amount appears 63 of 200 times)	Flagged
✓	Round-Number Intensity	Round-number ratio: 0.01 (3 of 200 transactions)	Clean
✓	Near-Equal In/Out Mirroring	Mirror ratio: 0.00 (0 of 53 inbound ops mirrored within 48h)	Clean
✗	Micro-Transfer Probing / Dust	Dust ratio: 0.20 (41 of 200 transactions below 0.01)	Flagged

TIME ANOMALIES

Status: **FLAGGED**

	Category	Description	Status
✗	Burstiness Score	Burstiness CV: 5.04 (199 inter-transaction intervals)	Flagged
✓	Off-Hours Concentration	Off-hours ratio: 0.20 (39 of 200 transactions between 00:00-06:00 UTC)	Clean
✓	Ping-Pong Periodicity	Longest periodic sequence: 0 ops (across 6 counterparties with 4+ ops)	Clean

WALLET ACTIVITY

Token Balances

Token	Amount	Price	USD Value
ETH	101.80	$1,940.1226	$197,509.19
AKITA	13,300,000.00	$0.0000	$0.10
JUSTICE	100.00	$0.0000	$0.00
JUP	1.00	$0.0002	$0.00
UBI	1.00	$0.0000	$0.00
0xe00a...4c92	599,956,070.11	—	—
0xeea2...442d	106,781.26	—	—
0x3327...5eba	3,999.99	—	—
0x933c...1be2	630.00	—	—
0x3fa4...4654	420.69	—	—
0x9854...7d03	2.70	—	—
		Total:	**$197,509.29**

WARRANTY RESTRICTIONS

APPENDIX 1: RISK CATEGORY DESCRIPTIONS

OTHER SANCTIONS LISTS
Third-party intelligence (GoPlus) indicates this address has been identified on one or more sanctions lists beyond OFAC SDN and UK Sanctions. A positive indicator suggests the address may be associated with designated persons, entities, or jurisdictions subject to financial restrictions.

BLACKLIST
An address appearing on industry blacklists has been flagged by one or more blockchain analytics firms, exchanges, or industry consortiums as potentially high-risk. Blacklisting may result from suspicious activity patterns or reported incidents.

MONEY LAUNDERING
An address flagged for money laundering has been linked to patterns or networks associated with the concealment of illegally obtained funds. This may include layering transactions, use of intermediary wallets, or connections to known laundering operations.

FINANCIAL CRIME
An address flagged for financial crime has been linked to broader financial criminal activity beyond money laundering, including fraud, embezzlement, market manipulation, or violation of financial regulations.

DARKWEB TRANSACTIONS
An address flagged for darkweb transactions has been associated with marketplaces or services operating on dark web networks. These transactions may involve the purchase or sale of illicit goods, services, or information.

BLACKMAIL
An address flagged for blackmail activity has been associated with extortion schemes, including ransomware demands, sextortion, or other forms of coercive demands for cryptocurrency payments.

MIXING SERVICES
An address flagged for mixing service usage has been linked to transaction mixing or tumbling services designed to obscure the origin and destination of funds. While not inherently illegal, mixing services are commonly associated with attempts to break transaction traceability.

CYBERCRIME
An address flagged for cybercrime has been associated with computer-related criminal activity, including but not limited to ransomware operations, unauthorized access to systems, or distribution of malicious software.

THEFT / ATTACKS
An address flagged for theft or attacks has been linked to the unauthorized taking of digital assets, exploitation of smart contract vulnerabilities, or participation in coordinated attacks against blockchain protocols or exchanges.

PHISHING
An address flagged for phishing has been associated with deceptive schemes designed to trick users into revealing private keys, seed phrases, or authorizing fraudulent transactions through fake websites, applications, or communications.

MALICIOUS MINING
An address flagged for malicious mining has been linked to cryptojacking operations or unauthorized use of computing resources to mine cryptocurrency without the owner's consent.

FAKE KYC
An address flagged for fake KYC has been associated with the use of fraudulent or stolen identity documents to pass know-your-customer verification processes, potentially enabling anonymous access to regulated services.

HONEYPOT CONTRACTS
An address flagged for honeypot contracts has been associated with deceptive smart contracts designed to appear profitable but contain hidden mechanisms that prevent users from withdrawing their funds after depositing.

FAKE TOKEN INTERFACE
An address flagged for fake token interfaces has been associated with smart contracts that impersonate legitimate token standards but contain modified or malicious functions designed to deceive users or automated systems.

FAKE TOKENS
An address flagged for fake tokens has been associated with the creation or distribution of fraudulent tokens that impersonate established cryptocurrencies, often used in scam schemes to defraud investors.

GAS FEE ABUSE
An address flagged for gas fee abuse has been associated with manipulation of transaction gas fees, including front-running attacks, sandwich attacks, or other forms of miner extractable value exploitation.

REINITIALIZATION ATTACK
An address flagged for reinitialization attacks has been associated with exploiting vulnerabilities in smart contract initialization functions, allowing attackers to re-initialize contracts and gain unauthorized control or extract funds.

COUNTERPARTY FLAG
Counterparty 0x35fb...d4b1 flagged for: Counterparty: Blacklist, Counterparty: Other Sanctions Lists, Counterparty: Theft / Attacks

COUNTERPARTY FLAG
Counterparty 0xf7b3...f1be flagged for: Counterparty: Blacklist, Counterparty: Other Sanctions Lists, Counterparty: Theft / Attacks

COUNTERPARTY FLAG
Counterparty 0x3e37...55e9 flagged for: Counterparty: Blacklist, Counterparty: Other Sanctions Lists, Counterparty: Theft / Attacks

COUNTERPARTY FLAG
Counterparty 0x53b6...bfc1 flagged for: Counterparty: Blacklist, Counterparty: Other Sanctions Lists, Counterparty: Theft / Attacks

COUNTERPARTY FLAG
Counterparty 0xa0e1...0e4b flagged for: Counterparty: Blacklist, Counterparty: Other Sanctions Lists, Counterparty: Theft / Attacks

RAPID INBOUND-OUTBOUND TURNOVER
Measures the ratio of funds that are received and then sent out within a short time window (< 24 hours). High turnover rates may indicate layering activity where funds are passed through the wallet to obscure their origin. Metric: percentage of inbound value forwarded within 24h.

RETENTION TIME ANOMALY
Analyzes the median time between receiving and sending funds. Wallets used for layering typically hold funds for very short periods (minutes to hours) compared to normal usage patterns. Metric: median retention time across all in-out pairs.

SAME-DAY FULL-DRAIN BEHAVIOR
Detects days where the wallet received significant inflows and then sent out a comparable or greater amount within the same calendar day, effectively draining the balance. Metric: number of same-day drain events as a fraction of active days.

COUNTERPARTY FAN-OUT
Counts the number of unique addresses that received funds from this wallet. A high fan-out ratio (many recipients relative to total transactions) may indicate fund distribution or structuring. Metric: unique outbound counterparties / total outbound transactions.

COUNTERPARTY FAN-IN
Counts the number of unique addresses that sent funds to this wallet. A high fan-in ratio may indicate fund consolidation or collection activity. Metric: unique inbound counterparties / total inbound transactions.

NEW-COUNTERPARTY RATIO
Measures the fraction of transactions involving counterparties that appear only once in the transaction history. A high new-counterparty ratio suggests the wallet avoids repeat relationships, which is common in layering. Metric: single-use counterparties / total unique counterparties.

COUNTERPARTY CONCENTRATION INSTABILITY
Tracks how the distribution of transaction volume across counterparties changes over time windows. High instability means the wallet frequently shifts its transaction partners, which may indicate evasion patterns. Metric: variance of Herfindahl index across time windows.

AMOUNT FRAGMENTATION (STRUCTURING)
Detects whether transaction amounts cluster just below common reporting thresholds or are broken into many similar-sized fragments. This is a classic structuring indicator. Metric: coefficient of variation of transaction amounts and clustering near round thresholds.

REPEATED FIXED-AMOUNT PATTERN
Identifies transactions where the same exact amount appears multiple times. Repeated fixed amounts may indicate automated transfers or structured payments. Metric: maximum frequency of any single amount / total transactions.

ROUND-NUMBER INTENSITY
Measures the fraction of transactions with round amounts (e.g., 100, 500, 1000). While some round amounts are normal, an unusually high proportion may indicate manual or structured transfers. Metric: round-amount transactions / total transactions.

NEAR-EQUAL IN/OUT MIRRORING
Detects cases where inbound transaction amounts are closely matched by subsequent outbound amounts (within a small tolerance). This pass-through pattern is a layering indicator. Metric: fraction of inbound amounts matched by a subsequent outbound within 5% tolerance.

MICRO-TRANSFER PROBING / DUST
Identifies an unusual volume of very small transactions (dust) which may be used to probe wallet activity, link addresses, or test transaction paths before moving larger amounts. Metric: fraction of transactions below dust threshold.

BURSTINESS SCORE
Measures how clustered transactions are in time versus being evenly distributed. High burstiness (many transactions in short bursts followed by long quiet periods) may indicate automated or coordinated activity. Metric: Fano factor of inter-transaction intervals.

OFF-HOURS CONCENTRATION
Analyzes whether transactions are disproportionately concentrated during unusual hours (e.g., 00:00-06:00 UTC). Off-hours concentration may indicate automated activity or operations in jurisdictions attempting to avoid oversight. Metric: fraction of transactions during off-hours.

PING-PONG PERIODICITY
Detects alternating in-out transaction patterns with regular timing intervals between the same counterparty pairs. This pattern may indicate wash trading or artificial volume generation. Metric: longest detected periodic sequence length.

APPENDIX 2: RECENT OPERATIONS

Date	Direction	Token	Amount	Counterparty
2025-12-13 11:03	IN	MALLY	2,093,071.86	0x0934d7c6fa5eed7af6603ab3cb58f8d656abe5fe
2025-09-06 23:52	IN	WETH	0.00	0x985409c0e4b1853a42800765bafcd9efc1c57d03
2025-09-06 23:52	IN	Visit website getether.net to claim rewards	2.70	0x2c3c4b7213ad8aaabefd8e4472719338a47f1610
2024-08-06 18:16	IN	ETH	0.00	0xfc3ff9d9abd3abadda68821e443779beb1082f43
2024-05-13 23:33	IN	ETH	0.00	0x09564ac9288ed66bd32e793e76ce4336c1a9ed00
2024-04-04 03:01	IN	ETH	0.00	0xbc25d517cc9d7ea453622ded3213302de34d29eb
2024-04-04 02:48	IN	ETH	0.00	0xdf225c04450504e9198569982c98de2e15b9df2a
2024-02-24 03:50	IN	ETH	2.00	0xe129927cfc61ce2f0b2a0ca6d8f9482d4ee60c64
2023-12-23 04:36	IN	Visit LiquidETH.org to claim rewards	1.70	0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae
2023-10-25 02:46	IN	ETH	0.01	0x4e5b2e1dc63f6b91cb6cd759936495434c7e972f
2023-09-22 11:35	IN	Visit https://apyeth.net to claim rewards	1.40	0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae
2023-09-10 05:50	IN	Visit https://usdreward.org to claim rewards	3,999.99	0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48
2023-08-07 14:08	IN	ETH	0.00	0xe2601b3896198443a41506a8c2ca6f116f1e9b72
2023-07-29 05:40	IN	MOMO	58,006,827.60	0x00859b3baac525143bb8a3ee3e19ddf9daf2408c
2023-07-07 02:26	IN	MILADY 2.0	78,211,261.85	0x7ef4c5f5e4e9cf35661f40638d49e8fe9ccb7c49
2023-05-21 03:16	IN	SCAT	92,192,877.86	0x7ef4c5f5e4e9cf35661f40638d49e8fe9ccb7c49
2023-03-21 17:02	OUT	ETH	2.00	0xb66cd966670d962c227b3eaba30a872dbfb995db
2023-03-19 12:18	IN	ETH	0.00	0xe3ae7649b160b2a38d1d286413bf1956620d9841
2023-03-19 12:05	IN	ETH	0.00	0xe3ae7649b160b2a38d1d286413bf1956620d9841
2023-03-17 03:48	IN	ETH	100.00	0xb66cd966670d962c227b3eaba30a872dbfb995db