Report on the Replay Attack and Remediation on the Luckycoin (LKY) Network

13th June, 2025

1. Vision and Leadership of the New Luckycoin CTO Team

The overall vision of Luckycoin is to be a premiere and highly valued Bitcoin-lineage OG memecoin that has an inherent and unique history with great lore (since 2013). It is widely recognized as the **original meme coin** and the **father of Dogecoin.**

Our vision extends beyond technical development; we see ourselves as **custodians of Luckycoin's legacy**, preserving its roots in the early days of cryptocurrency and ensuring its continued relevance as the OG Meme coin.

In early 2025, subsequent to the late 2024 replay attack, a small group of highly motivated, and quick-thinking community members moved to secure the chain and preserve the integrity of the Luckycoin ecosystem and community. We worked tirelessly to patch the vulnerability, pay for and work with the auditors, then secure all of the critical credentials such as the X account, websites, etc. from the previous CTO Team who were very helpful.

Thankfully now that everything is secure, with the requisite replay protection in place, and the verichains audit complete we are able to share a fully transparent report to the LKY, and wider crypto community stating all of the facts.

The new CTO Team includes:

- **CEO**: *Jet*
- **Head Developer**: *Crypt0rc*
- **Head of Marketing**: *Gogote*
- **Business Development Managers**: *Dr. T* and *Phil J*

Our mission is to maintain Luckycoin's status as a **historical pillar** of the blockchain world while steering it into a secure and community-driven future. With this vision, the team is committed to transparency, trust, and safeguarding against threats to the network's integrity.

---

2. Executive Summary

On December 26, 2024, Luckycoin experienced a significant security incident, a replay attack that exploited the lack of replay protection in the revived chain. This vulnerability allowed an attacker to re-broadcast historical transactions from the legacy chain, resulting in unauthorized transfers on the live Luckycoin network.

This report documents the attack, the forensic audit performed by Verichains (https://verichains.io/), and the robust mitigation strategies deployed by the LKY team. In total, **2,679,390.79 LKY** were moved during the attack, involving 1307 distinct input-addresses (previously dormant) and 580 distinct output-addresses. The addresses involved in the replay attack that were under the control of the attacker have been labeled as compromised and have since been **blacklisted**. The team has implemented comprehensive **replay protection and validation upgrades to ensure that such attacks cannot re-occur.**

---

3. Background

Following Luckycoin's revival in 2024 using a chainstate snapshot up to block 81,743, two chains came into existence:

- **Revived Luckycoin Network** (current chain):
    - Block 0–81,743 (historical chainstate)
    - Blocks 81,744–present (new mining and development)
- **Legacy Chain** (unofficial continuation):
    - Block 0–1,607,181
    - Low activity, mined by a few independent miners
    - Block reward reduced to ~0.00134 LKY

Due to the shared transaction history and key structure, any transaction executed on the legacy chain post-fork remained valid on the revived chain—if no replay protection was implemented.

---

4. Nature of the Replay Attack

Replay attacks occur when the same signed transaction can be broadcast across two chains with identical history and no replay isolation. In this case:

- A wallet holding 10 LKY before the fork has 10 LKY on both chains.

- A transaction on Chain A (legacy) can be copied and rebroadcast on Chain B (revived) if funds are unspent.

Observed Timeline:

- **November 18, 2024**: First replayed transaction occurred:
  Current chain:
  https://luckyscan.org/tx/4a5f7edc540cf01427d19aebfe98bdb7fcb99db331178d6fd457527df1cb9c1c
  Legacy chain:
  https://chainz.cryptoid.info/lky/tx.dws?4a5f7edc540cf01427d19aebfe98bdb7fcb99db331178d6fd457527df1cb9c1c.htm
  This single unnoticed replayed transaction indicates that the attacker prepared the operation more than a month in advance.

- **December 26, 2024**: Coordinated replay transactions were initiated on the revived chain, paired with reactivation of dormant supply.

- **December 30, 2024**: Last found replayed transaction conducted.

Notable Example:

- **TXID**:
  `79405d979b65dc06cf59c459fa02d490093bdfbb04ee164ee2cb3f7154507eb8`
  - **Legacy Chain Block**: #158359
  - **Revived Chain Block**: #243598
  - **Wallets involved**: ~390K LKY from legacy addresses replayed onto the active chain.
  - **Details**: Legacy Explorer | Current Chain

5A. Audit Findings: Verichain's Forensic Analysis

In early January 2025, **Verichains** was engaged and paid to perform a comprehensive audit. Their mandate:

- Identify replayed transactions using cryptographic and chain analysis
- Isolate affected wallet addresses
- Quantify exposure and determine sell-off volumes
- Recommendations on handling the aftermath of the replay attack

Key Findings:

- A total of **404** transactions involving **2,679,390.79 LKY** were replayed (find full report here: https://luckycoinstats.com/static/json/replayAttackTxs.json)
- The earliest replayed transaction conducted predates public awareness, suggesting premeditation and deliberate obfuscation by the attacker.

Attack Strategy Observed:

1. Replay transactions to valid addresses in the attacker's possession.
2. Consolidate funds into new wallets not found on the original chain. e.g. to this consolidation address: https://luckyscan.org/address/Kx3GDSzj71Jy6TdmShAwyGsgyX9tvrdizE
3. Begin off-chain liquidation.

A signature case involved the wallet `L11X5fCkHLBs3kFCxQet1ebvn7bcsWyn15`, which received **1.67M LKY** from replayed inputs and was used for onward transactions to centralized exchanges.

5B. Findings: CTO team's on-chain analysis

In parallel, members of the CTO Team conducted on-chain analysis in order to gain a better understanding about the scale and size of the attack. In doing so, they stumbled upon addresses that were not part of the replay attack but could be proven to be in possession of the

attacker. We'll highlight one such case below:
Address: `LGP4NC8eqDEcLHpqhzACMTrHr8SB4dKVr4`

This wallet received an input of just **0.01 LKY** on december 27th in this transaction: view tx; (https://luckyscan.org/tx/1dd4f01ad0b7bf9780e05c46cad43e9d26d7a34f57e04eab145c0bf9ecf211be) likely by a community member that wanted to make the wallet appear "undormant" on the luckyscan holders page.

This input of 0.01 LKY however, proved the attackers ownership over this address, because it was sent in batch with other inputs that were already known to be in the attackers possession, as can be seen in this transaction: view tx; (https://luckyscan.org/tx/c48e8a5af3c37cd4293be660956d05729732cb717fe8ced3e09c609e7c3e2d6a).

The large amount of coins in the address (300,000 LKY resp.) suggests that the attacker deliberately held some back in case the CTO team blacklisted the replayed coins, further highlighting the attacker's high level of sophistication.

5C. Overview

Combining all of the above research together, and in close coordination with exchanges – as to not blacklist exchange deposit addresses – the CTO team put together a list of 674 addresses, of which 355 contained non-zero balances, to be blacklisted. It's important to note that not all of the replayed transactions ended up on this list, only the addresses of which ownership by the attacker could be proven.

Key Numbers and Findings:

- A total of 404 transactions were replayed (find full report here: https://luckycoinstats.com/static/json/replayAttackTxs.json)
- An estimated 700k LKY got sent to exchange addresses (e.g. non-kyc deposit;https://luckyscan.org/tx/2b08eaabd79b7b0c7a61ab0d505afcbe0db306bd02738334ce33ed247108dff0 or mexc deposit; https://luckyscan.org/tx/7763a9a22baa634e7396282257994e5764155a918c22c61bab1d27b8bdd038f0) and subsequently sold.
- Not all replayed transactions ended up in the attackers possession, some merely acted as decoys, adding to the overall chaos.
- Sum of total inputs equals 3,163,389.46 LKY, and sum of total outputs equals 3,163,280.19 LKY (~109.30 LKY paid in miner fees).
- A total of **2,679,390.79 LKY** moved from dormant addresses to new addresses.

- The attacker tried to obfuscate other large amounts that were not part of the replayed transactions, but those got detected by on-chain analysis.

---

6. Remediation and Security Measures

Following the audit, the Luckycoin CTO team swiftly implemented a robust set of countermeasures to restore network integrity and prevent recurrence:

Blacklist Enforcement

- **2,262,408.88 LKY** from 671 compromised addresses permanently **blacklisted**.
- Blacklisting was enforced at the **protocol level**, **rendering funds unspendable.**

Replay Protection Implementation

- Chain-specific **SIGHASH marker** introduced to break transaction compatibility.
  https://github.com/LuckyCoinProj/luckycoinV4/commit/ff25c2a23bece74d59051be0f489a761e144f247
  SigHash scheme before the fix: SHA256(SHA256(preimage))
  SigHash scheme after fix: SHA256(SHA256(CHAIN_ID || preimage))
- Legacy chain transactions are now invalid on the current network.
- Ensures any broadcast attempt from the legacy chain fails at consensus level.

Transaction Validation Upgrades

- Improved detection logic for **legacy-originating inputs**.
- Enhanced rules for distinguishing legitimate post-revival activity.

Wallet Monitoring & Transparency

- Released public tracking tools to monitor future dormant wallet movements (view here; https://luckycoinstats.com/tools).
- Ongoing flagging of suspicious or reactivated addresses.

- Public address blacklists maintained for reference.
- Full list of resources related to the replay attack can be found here; https://luckycoinstats.com/resources)

Community Engagement & Education

- Clear communications about dormant vs. reactivated supply.
- Community advisory notices to exchanges regarding tainted funds.

---

7. Conclusion

The Luckycoin replay attack revealed a critical gap in forked chain security—lack of replay protection. The CTO team's rapid and transparent response, backed by Verichain's audit, successfully:

- Isolated and nullified maliciously replayed transactions.
- Enhanced the protocol's cryptographic and structural defenses.
- Reaffirmed Luckycoin's commitment to security, history, and responsible decentralization.

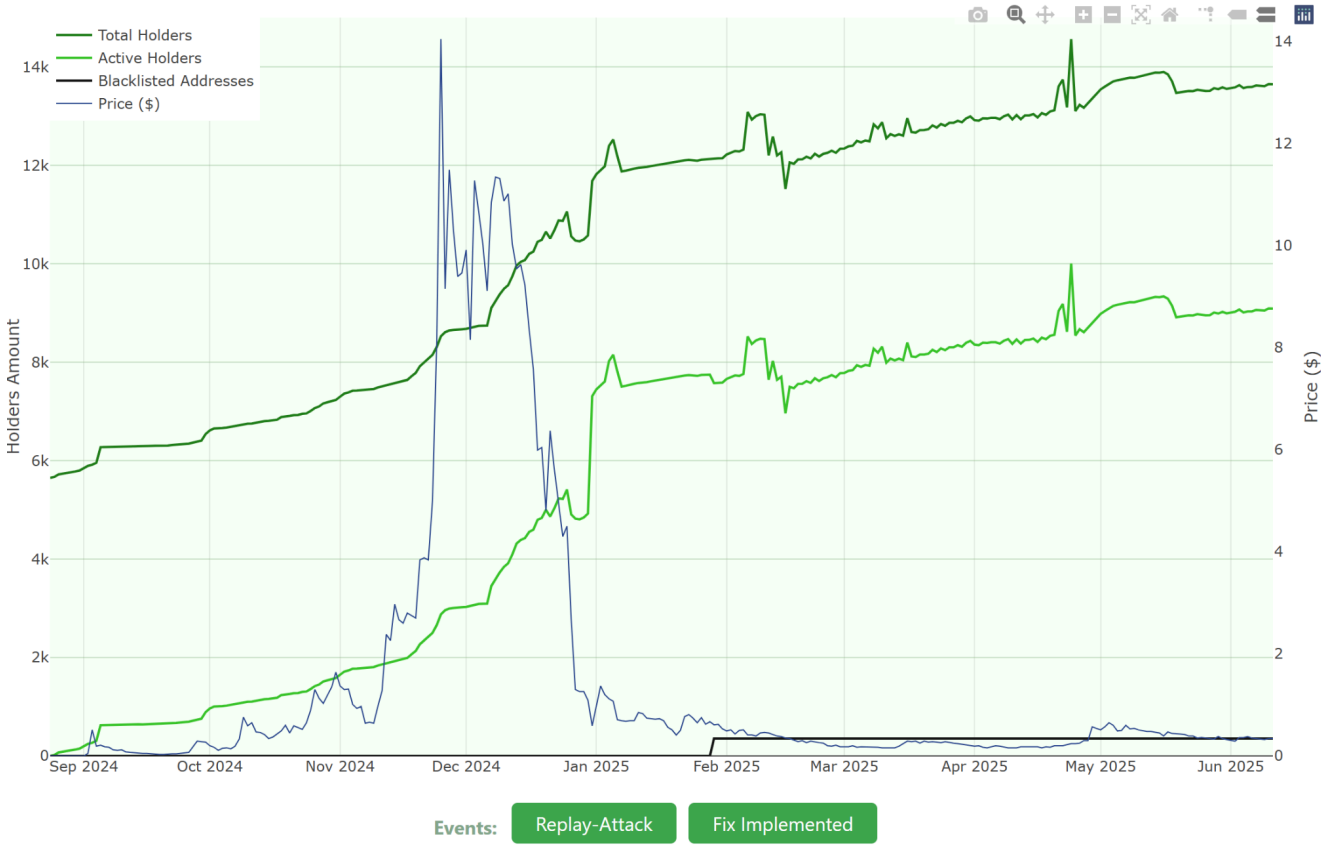
Today, the Luckycoin network is **more secure, transparent, and resilient**. With decisive action taken and safeguards in place, the team has turned a serious attack into an opportunity to build a stronger foundation for Luckycoin's next chapter.

Appendix A: Replay Attack Wallets

			Replay-attack	Status	Note	Dormant balance
1	L3XnfLo5m3BrZxH5PVxxpg38G8F8X7oDfd	1.673.689,99 LKY	Replayed	Reactivated	Dec-26	1673689.99
2	KvQdB3YisGH8ekZZyAbbfrbe79HwHZXyuh	400.000,01 LKY	No	Linked to Wallet (KVr4)		400000
2	LGKiLwBMJWNXsPTgJ1dgnWAtNnDK73U7G3	390938,21569702 LKY	Replayed	Inactive	Dec-30	390938.22
3	LGP4NC8eqDEcLHpqhzACMTrHr8SB4dKVr4	300000 LKY	No	Reactivated	Dec-28	300000
4	LGRT3QAC7aWEdDLevaMmAmnCCTL4rGpBjC	261.505,44 LKY	Replayed	Inactive	Dec-26	261505.44
5	LHPYZCatvzmKPPuuXQfYpDR4s9xHGzVNd9	123.786,39 LKY	Replayed	Inactive	Dec-26	123786.39
6	LJnaiZ3XYhsJi38u7DYxgdgbF2yhxoU78E	105.174,41 LKY	Replayed	Inactive	Dec-26	105174.41
7	L5ENriQmbpTnLGAKVKZZQkenK3QNCdoWDp	98.089,80 LKY	Replayed	Inactive	Dec-26	98089.8
8	LBSykwdr3VpJgSRRMvsYw14V4L2Yew8cc8	67.231,43 LKY	Replayed	Reactivated	Dec-26	67231.43
9	L9kpbeED9p79jfckoUeyXZX5FkUaoaKeR3	50.382,00 LKY	Replayed	Inactive	Dec-26	50382
10	L4eAjozfHSLCPtGyLae6SHWwu5zUMoSK22	43.357,73 LKY	Replayed	Reactivated	Dec-26	43357.73
11	LDyobDvpETykUpPXTtqY5JHu39gmNJQe6f	40.229,00 LKY	Replayed	Inactive	Dec-26	40229
12	L2MCKQQeuLw9Bm2xjTNs2CztvCEXVT21Cz	35.020,00 LKY	Replayed	Inactive	Dec-26	35020
13	L7xum3N4KRXMyDgpgg7LPmWGJNyDCWvpx6	32.694,03 LKY	Replayed	Inactive	Dec-26	32694.03
14	L7csZfvQjkXNTPNUTnstd8voK7Q6ZBHq5m	30.985,35 LKY	Replayed	Inactive	Dec-26	30985.35
15	LDP5RY8iZYS3LN55tWtF2rikZjBJ6xnKiu	28.631,21 LKY	Replayed	Reactivated	Dec-26	28631.21
16	Kzi3wzTAXNbFxKfqvGXb3qNKMczk9Vvtjo	26.545,01 LKY	Replayed	Reactivated	Dec-26	26545.01
17	LBb3A1kapa7qPpU8Bn2BC7T272sb7dMSDt	25.969,39 LKY	Replayed	Reactivated	Dec-26	25969.39
18	L9R3ZBZrZ1vbbSgLmzd5v3VaLu5kFanKx7	24.826,03 LKY	Replayed	Inactive	Dec-26	24826.03
19	L5DEEHxRCy2c1uykMkLNoiYnMqT5n4XYyw	23.941,21 LKY	Replayed	Inactive	Dec-26	23941.21
20	L8RR7a3mnMreYBGUASP7RR3CMTstwY8CuR	23.692,43 LKY	Replayed	Inactive	Dec-26	23692.43
21	KvMWM1htzGME6qrV4id4gpZKa4rZV37t67	22.950,30 LKY	Replayed	Inactive	Dec-26	22950.3
22	Kz6Q3qpBbbVT7vGJ61CJ4AJwBdm543a8qi	19,626.41	Replayed	Inactive	Dec-26	19626.41
23	LJGiPi6KbzmohAvCtXLdpK8aqWMQ9YB6uo	18,314.6973822	Replayed	Inactive	Dec-26	18314.69
24	L88DrCv3e4rX1yuR7vdFKcwpVZZFXaxH6A	16,203.43475316	Replayed	Inactive	Dec-26	16203.43
25	Kvhy7cLo542fu7h2U7ye5apNvofwFiJFSz	15,688.01193202	Replayed	Inactive	Dec-26	15688.02
26	LAAf1KtzfKedEhX8rA85FESCKtWFnibZGe	15,640.4883466	Replayed	Reactivated	Dec-26	15640.48
27	L41QAzdncW4FgNM68wD8g4q9VvEtYGv5PX	13,669.9769725	Replayed	Inactive	Dec-26	13669.98
28	LGZY1ttSWuZenRTp9K6sKdif7yDirpEWQA	12,710.77092088	Replayed	Reactivated	Dec-26	12710.78
29	KyDy93T9vyHxHW3n1UAvpNcHLvmWAG4sAJ	12,625.48516811	Replayed	Reactivated	Dec-26	12625.48
30	LK7Y8e6wDDNpLPCC92db5wXPfHQ5HqwBig	12,354.70283241	Replayed	Inactive	Dec-26	12354.7
31	LDHbAZpyWYkAL16CGaC7x3oxSdVLWLd8B8	10,881.09788604	No	Reactivated	**Nov-25**	10881.09
32	LJojoTaLG1b9WVJrnAEWqNy3ECkFhTUTfg	10,765.14334805	Replayed	Reactivated	Dec-26	10765.14
33	LFGbiQTi9zwD6ZHzuRdzPxb9bHdhsUh1Dw	9,977.95594473	Replayed	Inactive	Dec-26	9977.95
34	L3ypmcKxxypG7DHhbByWeMHva9pgMaKN96	8,989.66784804	Replayed	Reactivated	Dec-26	8989.66
35	KwAuTZmpQVE1Hi7YcV7Hbov7mXdA5cKX6e	8,264.02964766	Replayed	Inactive	Dec-26	8264.03
36	L1FgudPG54AcJBfERFki1yDah4RaGdReFz	8,052.97375076	Replayed	Reactivated	Dec-26	8052.97
37	LAjVFU5UxMyK6xrkH1nfdboDdBp3WSDC3m	8,009.98287288	Replayed	Inactive	Dec-26	8009.98
38	L3DqLExk9Vy8AtckeN6wpJZjF2ZMPgHa4K	7,699.590858	Replayed	Inactive	Dec-26	7699.59
39	LBe3Vm9r5sNNNvMH8v49Df5qMHAk3DhXdv	7,550.36176524	Replayed	Reactivated	Dec-26	7550.36
40	KwirGW1xht9GYgbA2PsHyweSF7Ks1N79tA	7,458.4409786	Replayed	Inactive	Dec-26	7458.44
41	LCK6mNR5H6vyqmuUoP6DKjGPdujQWPsJrV	7,220.968044	Replayed	Inactive	Dec-26	7220.96
42	LDuiS4Zjsc2CxDrB4Qs9L9gEqNVYy3iuK2	6,865.70	Replayed	Inactive	Dec-26	6865.7
43	L3CXXMVXusE3gdFRtWnoL8whxZnP4fYcNq	6,628.89663879	Replayed	Reactivated	Dec-26	6628.89
44	LD3ytEQuN2hg4VwZfRVACh8SDAWNNKkSGV	6,583.1723475	Replayed	Reactivated	Dec-26	6583.17
45	L6iD41By13cKFkRammN1F1SDrk45og7vFe	6,357.80155379	Replayed	Inactive	Dec-26	6357.8
46	LF9mdjkZE15wX36JKCGG1WBh31u4uKdn8k	6,326.9721399	Replayed	Reactivated	Dec-26	6326.9
47	KwXhjGP6MJ8Z9ME9ryUzsGt8agZHyPssVH	6,295.41170754	Replayed	Reactivated	Dec-26	6295.41
48	Kxpz6GFRabRxfRMmQ3X23Z85PhdFFuUtfA	5,992.21123701	Replayed	Reactivated	Dec-26	5992.21
49	LCt5GfbtJbRyf2GVLSxpCiTGq72URsCrTP	5,983.94328229	Replayed	Reactivated	Dec-26	5983.94
50	LFYm4KJfbwfa4sSmEPQ1nDLsfLny8FTat8	5,870.8182482	Replayed	Inactive	Dec-26	5870.81
51	Kyi9AC3fMG1XoSgEWy6jcGRg51xC2vxk1L	5,829.93173262	Replayed	Inactive	Dec-26	5829.93
52	L3XQ7dhQrXLWAS2vZn2FwuNZtT6iwyw5fA	5,798.94133274	Replayed	Inactive	Dec-26	5798.94
53	L3QpG8HPowoe9T8eH5685Zrrm8ftcUPA8q	5,743.82893133	Replayed	Inactive	Dec-26	5743.82
54	LEn59yqQjdD1mTbZq9nPr7DSz29bEfNf55	5,729.29593286	Replayed	Inactive	Dec-26	5729.29
55	LGGvfmTYcSdMyPZtuaoiTzgUnHa2pgtHNc	5,687.60858495	Replayed	Reactivated	Dec-26	5687.6
56	L7tJNbXHSWJhJhQcDyG5bpQgocAWYL6uyT	5,655.70745282	Replayed	Reactivated	Dec-26	5655.7
57	L3FQzh4Jo2qGFkkqxJZutugvaezgJpi5FF	5,569.13929976	Replayed	Inactive	Dec-26	5569.14
58	L9uTwFt6kAKDp6ajTXBLu6Hr32ibCre4HQ	5,393.73168321	Replayed	Inactive	Dec-26	5393.73
59	KvNvqXLxxuwCL8g59BX2tVNGMWPrPnuLEh	5,362.55112771	Replayed	Inactive	Dec-26	5362.55
60	L4Z9rYrZt6GCZALXgQxadMYshREAgJdbaf	5,349.26785591	Replayed	Reactivated	Dec-26	5349.27
				total		4174368.31

** Status "Inactive" in the above tables means that ownership by the attacker could not be proven, suggesting the transactions were used to attribute to the overall public chaos and confusion*

Appendix B: Current Active vs Total Holder Statistics



** The difference between "Total" and "Active" addresses in this graph represents "Dormant" wallets (5651 address at the start of the revival vs. 4561 after the replay attack)*

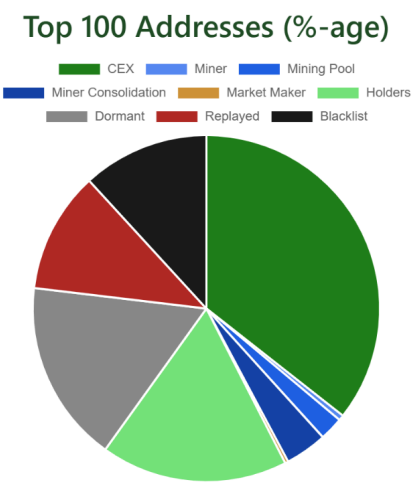
Appendix C: “Murad” Style Metrics

💎🙌-EDNESS METRICS	
ALL WALLETS	
Holders	13659
All-Time Wallets Holding > $100K	178
Wallets still Holding > 50% of peak coins	80
Wallets still holding > 50% of peak coins (%-age)	45%
ACTIVE WALLETS	
Active Holders ⓘ	9098
Active All-Time Wallets Holding > $100K	108
Active Wallets still Holding > 50% of peak coins	71
Active Wallets still holding > 50% of peak coins (%-age)	66%
OTHER MURAD METRICS	
Median Wallet Balance	2.87 **USD**
Median Wallet Balance (LKY)	8.21 **LKY**
Average Wallet Balance	476.86 **USD**
Average Wallet Balance (LKY)	1362.47 **LKY**

**as of 12/06/2025*

Appendix D: Current Holder Distribution

TOP 100 HOLDERS STATISTICS		
	Amount of coins in top 100 addresses	14,623,068.43
	Percentage of total ciculating supply	78.6 %
CATEGORIES		
Holders	Individual holders	2,537,107.70
CEX	Centralized Exchanges	5,207,090.61
Miner	Individual Miners	74,705.84
Mining Pool	Mining Pool	317,998.86
Miner Cons.	Miner Consolidation Wallet	567,046.46
Market Maker	Market Maker	50,000.00
Dormant	Dormant	2,488,682.48
Replayed	Inputs originating from this address found in the replay-attack	1,649,039.91
Blacklist	Blacklist	1,731,396.57



as of 12/06/2025