

幸运币 (Luckycoin, LKY) 双放攻击与修复报告

2025年6月13日

1. 新幸运币CTO团队的愿景与领导力 2
 2. 摘要 2
 3. 背景 3
 4. 重放攻击的性质 3
 - 攻击时间线概览: 3
 - 典型案例: 4
 5. 5A. 审计发现: Verichain的取证分析 4
 - 关键发现: 4
 - 观察到的攻击策略: 5
 - 5B. CTO团队的链上分析发现 5
 - 5C. 综合分析 6
 6. 补救与安全措施 6
 - ✓ 黑名单强制执行 6
 - ✓ 重放保护机制实施 7
 - ✓ 交易验证机制升级 7
 - ✓ 钱包监测与透明度提升 7
 - ✓ 社区参与与教育推广 7
 7. 结论 8
- 附录A:** 重放攻击涉及的钱包地址 9
- 附录B:** 活跃持币者与总持币者数据统计 10
- 附录C:** “Murad” 风格指标 11
- 附录D:** 持币者分布情况 12

1. 新幸运币CTO团队的愿景与领导力

幸运币的总体愿景，是成为顶尖且高度认可的比特币血统OG（元老）模因币（Meme Coin），自2013年以来，它拥有独特的历史和传奇故事。幸运币被广泛认可为最初的模因币，也是狗狗币（Dogecoin）的“始祖”。

我们的愿景不仅限于技术开发，我们更视自己为幸运币历史遗产的守护者，致力于保护幸运币在加密货币早期发展中的根基，并确保它作为OG模因币的持续影响力与生命力。

在2025年初，在2024年末重放攻击发生之后，社区成员迅速行动，保障了区块链的安全，维护了幸运币生态系统和社区的完整性。我们不辞辛劳，修补漏洞，自费聘请审计机构，并与审计团队合作，并成功从前任团队手中接管了所有关键的账户和权限，例如X账号、官网、tg等。

幸运的是，如今所有安全问题已妥善处理，重放保护机制已部署到位，Verichains审计也已顺利完成，我们终于可以向幸运币社区以及更广泛的加密货币社区，公开透明地汇报全部事实。

新CTO团队成员包括：

- 首席执行官（CEO）：Jet
- 首席开发（Head Developer）：Crypt0rc
- 营销主管（Head of Marketing）：Gogote
- 商务经理（Business Development Managers）：Dr. T 与 Phil J

我们的使命，是维持幸运币作为区块链历史中重要基石的地位，并引领其迈入一个更加安全、由社区驱动的未来。怀抱这一愿景，团队承诺始终坚持透明、信任，并坚定守护网络的安全与完整性。

2. 摘要

2024年12月26日，Luckycoin 遭遇了一起重大安全事件——重放攻击。攻击者利用复活链缺乏重放保护的漏洞，将历史链中的旧交易重新广播至当前链上，从而导致在活跃的幸福币网络中发生了未授权的转账。

本报告详细记录了此次攻击的全过程、Verichains (<https://verichains.io/>) 所执行的取证审计，以及幸运币团队随后采取的全面且有效的应对策略。

在此次攻击中，共有 2,679,390.79 LKY 被转移，涉及 1307 个不同的输入地址（大多为此前处于休眠状态的地址）和 580 个不同的输出地址。所有在此次重放攻击中、已被确认由攻击者控制的地址，均已被标记为“已被攻占”，并被列入黑名单。

幸运币团队已全面实施了重放保护机制，并对交易验证流程进行了升级，以确保此类攻击不再重演。

3. 背景

在2024年，Luckycoin通过使用区块高度为81,743的链状态快照进行复活，由此产生了两条链：

复活后的Luckycoin网络（当前主链）：

- 区块 0 - 81,743（历史链状态）
- 区块 81,744 及之后（新的挖矿与开发）

遗留链（非官方延续链）：

- 区块 0 - 1,607,181
- 活跃度极低，仅由少数独立矿工维持挖矿
- 区块奖励已降至约 0.00134 LKY

由于这两条链共享相同的交易历史和密钥结构，在缺乏重放保护的情况下，任何在分叉后于遗留链上执行的交易，都依然可以在复活链上被认定为有效交易。

4. 重放攻击的性质

重放攻击是指同一笔已签名交易可以在两条拥有相同历史、且缺乏重放隔离的区块链上被同时广播的攻击方式。在本案例中：

- 分叉前，一个钱包持有10 LKY，在两条链上都会拥有10 LKY。
- 如果资金尚未花费，攻击者可以将遗留链（链A）上的交易复制，并在复活链（链B）上重新广播，从而在复活链上完成转账。

攻击时间线：

- **2024年11月18日：**首次重放交易发生
当前链交易记录：
<https://luckyscan.org/tx/4a5f7edc540cf01427d19aebfe98bdb7fcb99db331178d6fd457527df1cb9c1c>
遗留链交易记录：
<https://chainz.cryptoid.info/lky/tx.dws?4a5f7edc540cf01427d19aebfe98bdb7fcb99db331178d6fd457527df1cb9c1c.htm>

这笔未被注意的重放交易表明，攻击者至少提前一个月就已策划此次攻击。

- **2024年12月26日：**攻击者开始在复活链上大规模协调重放交易，同时激活大量休眠资金。
- **2024年12月30日：**发现的最后一笔重放交易被执行。

典型案例：

交易哈希（TXID）：

79405d979b65dc06cf59c459fa02d490093bdfbb04ee164ee2cb3f7154507eb8

- 遗留链区块高度：#158359
- 复活链区块高度：#243598
- 涉及钱包：约39万枚 LKY 从遗留地址被重放至活跃链上。

交易详情：

遗留链浏览器 | 当前链浏览器

5A. 审计发现：Verichain 的取证分析

2025年1月初，幸运币团队聘请并支付了 Verichains 团队，对此次事件进行全面审计。其主要任务包括：

- 利用加密技术与链上分析，识别所有重放交易；
- 精确定位所有受影响的钱包地址；
- 评估整体风险敞口，统计被转移和可能出售的币量；
- 提出针对重放攻击事件后续处理的建议。

关键发现：

- 共计发现 404 笔重放交易，涉及总额为 2,679,390.79 LKY（完整报告链接：<https://luckycoinstats.com/static/json/replayAttackTxs.json>）。
- 最早的重放交易发生时间早于事件曝光，表明攻击者具备高度预谋性，并刻意隐藏操作轨迹。

观察到的攻击策略：

- 将重放交易发送至攻击者控制的有效地址。
- 将资金集中转移至全新的钱包地址，这些地址在原始链中并不存在，例如这个集中地址：
<https://luckyscan.org/address/Kx3GDSzj71Jy6TdmShAwyGsgyX9tvrdisE>
- 随后开始链下变现操作。

典型案例：

涉及钱包地址：L11X5fCkHLBs3kFCxQet1ebvn7bcsWyn15

该钱包共收到约 167 万枚 LKY 的重放输入，并进一步将资金转至中心化交易所账户。

5B. 发现：CT0团队的链上分析

与此同时，CT0团队成员也进行了链上分析，以更深入地了解此次攻击的规模和影响范围。在分析过程中，他们意外发现了一些并非参与重放攻击的地址，但能够通过链上证据确认这些地址归攻击者所有。以下是一个典型案例：

****地址：** **LGP4NC8eqDEcLHpqhZACMTrHr8SB4dKVr4

该钱包在2024年12月27日收到一笔仅 0.01 LKY 的转账，交易链接如下：

[查看交易](#)

这笔转账很可能是某位社区成员为了让该钱包在 Luckyscan 持币排行榜页面上显示为“非休眠”状态而故意发出的。

然而，这笔0.01 LKY的转账意外地暴露了攻击者对该地址的控制权。原因在于，该笔交易与多笔已知属于攻击者的钱包地址的输入一同打包发送，如以下交易所示：

[查看交易](#)

此外，该地址中的巨额资金（约30万枚 LKY）进一步暗示，攻击者可能有意保留部分资金，以防CT0团队对重放交易所得币进行黑名单处理，进一步凸显了攻击者的高超手段与缜密布局。

5C. 综合分析

结合上述所有调查研究结果，并与各大交易所紧密协调（以避免误将交易所充值地址列入黑名单），CTO团队最终整理出一份黑名单，共计674个地址，其中355个地址仍有非零余额。

需要特别说明的是，这份黑名单中并未包含所有参与重放的地址，仅包含已被确认证明由攻击者控制的地址。

关键数据与发现：

- 共计404笔重放交易（完整报告见此链接：<https://luckycoinstats.com/static/json/replayAttackTxs.json>）。
- 约70万枚 LKY 被发送至交易所地址（例如：
 - 非KYC充值地址：
<https://luckyscan.org/tx/2b08eaabd79b7b0c7a61ab0d505afcbe0db306bd02738334ce33ed247108dff0>
 - MEXC充值地址：
<https://luckyscan.org/tx/7763a9a22baa634e7396282257994e5764155a918c22c61bab1d27b8bdd038f0>），随后被出售。
- 并非所有重放交易的资金最终都落入攻击者之手，一些交易仅起到烟雾弹作用，增加了事件的混乱度。
- 总输入金额为3,163,389.46 LKY，总输出金额为3,163,280.19 LKY（约109.30 LKY用于支付矿工费）。
- 共计2,679,390.79 LKY 从休眠地址转移至新地址。
- 攻击者还试图掩盖一些未参与重放交易的大额资金，但这些资金已被链上分析成功识别

6. 补救与安全措施

在审计完成后，Luckycoin CTO团队迅速实施了一系列强有力的应对措施，以恢复网络完整性并防止类似事件再次发生：

✅ 黑名单强制执行

- 共计 2,262,408.88 LKY，来自 671 个已被攻陷的钱包地址，已被永久列入黑名单。

- 黑名单在协议层面强制执行，使得这些资金永久无法使用。

✅ 重放保护机制实施

- 引入链特有的 SIGHASH 标记，以打破与其他链的交易兼容性。

相关提交链接：

<https://github.com/LuckyCoinProj/luckycoinV4/commit/ff25c2a23bece74d59051be0f489a761e144f247>

修复前的 SigHash 签名哈希方案：

SHA256(SHA256(交易预映像 preimage))

修复后的 SigHash 签名哈希方案：

SHA256(SHA256(CHAIN_ID || 交易预映像 preimage))

- 遗留链上的交易现已在当前网络中无效。
- 确保所有来自遗留链的交易广播请求，在共识层面自动被拒绝。

✅ 交易验证机制升级

- 改进了识别遗留链来源输入的检测逻辑。
- 优化了区分复活链后合法活动与攻击行为的规则。

✅ 钱包监测与透明度提升

- 发布了公开的追踪工具，以监测未来休眠钱包的动态（工具链接：<https://luckycoinstats.com/tools>）。
- 持续标记可疑地址与被重新激活的地址。
- 维护公开的钱包地址黑名单，供社区参考。

完整的重放攻击相关资源列表请见：

<https://luckycoinstats.com/resources>

✅ 社区参与与教育推广

- 清晰传达休眠供应与已激活供应之间的区别。
- 向交易所发布社区公告，提醒注意涉及受污染资金的风险。

7. 结论

此次Luckycoin重放攻击，揭示了分叉链安全中的一个关键漏洞——缺乏重放保护机制。幸运币CT0团队在Verichain审计支持下，迅速而透明地采取了应对措施，成功：

- 隔离并彻底清除所有恶意重放交易；
- 加强了协议的加密机制与结构性安全防御；
- 重申了Luckycoin在安全、历史传承与负责任的去中心化方面的坚定承诺。

如今，Luckycoin网络已更加安全、透明且具备韧性。通过果断行动与周密防护，团队已将这场严重攻击转化为一次夯实Luckycoin未来发展基础的契机。

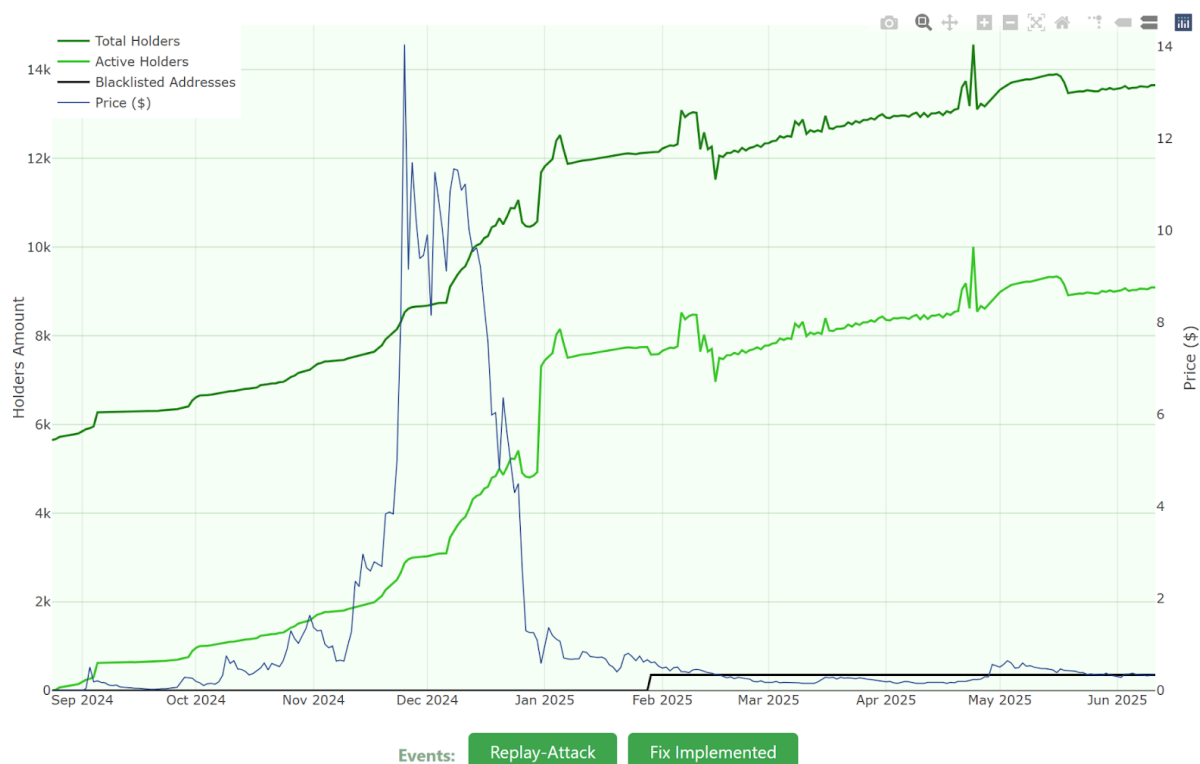


附录 A：重放攻击涉及的钱包地址

			Replay-attack	Status	Note	Dormant balance
1	L3Xnfl05m3BrZxH5PVxpg38G8F8X7oDfd	1,673.689,99 LKY	Replayed	Reactivated	Dec-26	1673689.99
2	KvQdB3YisGH8ekZZYAbbf7b9HwHZxyuh	400.000,01 LKY	No	Linked to Wallet (KvR4)		400000
2	LGKILwBMJWNXsPtJg1dgnWatNnDK73U7G3	390938,21569702 LKY	Replayed	Inactive	Dec-30	390938.22
3	LGP4NC8eqDEcLHpqhZACMTrHr8SB4dKvR4	300000 LKY	No	Reactivated	Dec-28	300000
4	LGRT3QAC7aWEdLLevaMmAmnCCTL4rGpBJC	261.505,44 LKY	Replayed	Inactive	Dec-26	261505.44
5	LHPYZCatvzmKPPuuXQfYpDR4s9xHGzVNd9	123.786,39 LKY	Replayed	Inactive	Dec-26	123786.39
6	UnaiZ3XYHsJI38u7DYxgdgbF2yhxoU78E	105.174,41 LKY	Replayed	Inactive	Dec-26	105174.41
7	L5ENriQmbpTnLGAkvKZZQkenK3QNCdoWDp	98.089,80 LKY	Replayed	Inactive	Dec-26	98089.8
8	LBSykwdr3VpJg5RRMvsYw14V4L2Yew8cc8	67.231,43 LKY	Replayed	Reactivated	Dec-26	67231.43
9	L9kpbeED9p79JfckoUeyXZ5FkUaoaKeR3	50.382,00 LKY	Replayed	Inactive	Dec-26	50382
10	L4eAjozfHSLCPTGyLae6SHWwu5zUmO5K22	43.357,73 LKY	Replayed	Reactivated	Dec-26	43357.73
11	LDyobDvpETy2c1uYkMkLNoiYnMqT5n4XYyw	40.229,00 LKY	Replayed	Inactive	Dec-26	40229
12	L2MCKQQueuLw9Bm2xjTNS2CztvCEXVT21Cz	35.020,00 LKY	Replayed	Inactive	Dec-26	35020
13	L7xum3N4KRXMpDpgg7LPmWGJNyDCWvpx6	32.694,03 LKY	Replayed	Inactive	Dec-26	32694.03
14	L7csZfvQjkXNTPNUtndst8voK7Q6ZB8q5m	30.985,35 LKY	Replayed	Inactive	Dec-26	30985.35
15	LDP5RY8iZY3LNS5tVKfLdpK8aqWMQ9YB6uo	28.631,21 LKY	Replayed	Reactivated	Dec-26	28631.21
16	Kzi3wzTAXNbFxKfQvGXb3qNKMczk9Vvtjo	26.545,01 LKY	Replayed	Reactivated	Dec-26	26545.01
17	LBb3A1kapa7qPjU8Bn2BC7T272sb7dM5Dt	25.969,39 LKY	Replayed	Reactivated	Dec-26	25969.39
18	L9R3ZBZr21vbbSgLMed5v3Valu5kFanKx7	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	Kz6Q3qp8BbV77VgJ61C4AJwBdm543a8qi	19,626.41	Replayed	Inactive	Dec-26	19626.41
23	UGiPi6KbzmohAvCtXldpK8aqWMQ9YB6uo	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
29	KyDy93T9vyHxHW3n1UAvpNcHLvmWAG4sAJ	12,625.48516811	Replayed	Reactivated	Dec-26	12625.48
30	LK7Y8e6wDDnPLCC92db5wXPFHQ5HqwBig	12,354.70283241	Replayed	Inactive	Dec-26	12354.7
31	LDHbAZpyWykAL16CGaC7x3oxSdVLWld8B8	10,881.09788604	No	Reactivated	Nov-25	10881.09
32	LJoToTaLG1b9WVJrnAEWqNy3EckFhTUTfg	10,765.14334805	Replayed	Reactivated	Dec-26	10765.14
33	LFGbiQTI9zwD6ZHzuRdzPxb9bHdhsUh1Dw	9,977.95594473	Replayed	Inactive	Dec-26	9977.95
34	L3ypmcKoxypG7DhHbByWeMHva9pgMaKN96	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	LajVFU5UxMyK6xrkH1nfdbDd8p3WSDC3m	8,009.98287288	Replayed	Inactive	Dec-26	8009.98
38	L3DqLExk9Vy8AtckeN6wpJZF2ZMPgHa4K	7,699.590858	Replayed	Inactive	Dec-26	7699.59
39	LBe3Vm9r5sNNVMMH8v49Df5qMHAk3DhXdv	7,550.36176524	Replayed	Reactivated	Dec-26	7550.36
40	KwirGW1xht9GYgbA2PsiHweySf7Ks1N79tA	7,458.4409786	Replayed	Inactive	Dec-26	7458.44
41	LCK6mNR5H6vymUoP6DKJGPDujQWPsJrV	7,220.968044	Replayed	Inactive	Dec-26	7220.96
42	LDuiS4Zjsc2CxDrB4Qs9L9gEqNVVY3iuK2	6,865.70	Replayed	Inactive	Dec-26	6865.7
43	L3CXXMVXusE3gdERtWnoL8whxZnP4fYcNq	6,628.89663879	Replayed	Reactivated	Dec-26	6628.89
44	LD3ytEQuN2hg4VwZfRVACH8SDAWNKKsGV	6,583.1723475	Replayed	Reactivated	Dec-26	6583.17
45	L6iD41By13cKfKRammN1F1SDrk45og7Vfe	6,357.80155379	Replayed	Inactive	Dec-26	6357.8
46	LF9mdjkZE15wX36JCGG1WBh31u4uKdn8k	6,326.9721399	Replayed	Reactivated	Dec-26	6326.9
47	KwXhjGP6MJ8Z9ME9ryUzsGt8agZHyPssVH	6,295.41170754	Replayed	Reactivated	Dec-26	6295.41
48	Kxpz6GFRabRxfRMmQ3X23Z85PhdFFUfUfa	5,992.21123701	Replayed	Reactivated	Dec-26	5992.21
49	LcT5GfbtUbrYf2GVLXpCITGq72URsCrTP	5,983.94328229	Replayed	Reactivated	Dec-26	5983.94
50	LFYm4KJfbwfa4sSmEPQ1nDlFzLnY8FTat8	5,870.8182482	Replayed	Inactive	Dec-26	5870.81
51	Kyi9AC3fMG1XoSgEWy6jcGRg51x2Cvxk1L	5,829.93173262	Replayed	Inactive	Dec-26	5829.93
52	L3XQ7dhQrXLWAS2vZn2FwuNZtT6iwyw5fA	5,798.94133274	Replayed	Inactive	Dec-26	5798.94
53	L3QpG8HPowoe9T8eH5685Zrm8ftcUPA8q	5,743.82893133	Replayed	Inactive	Dec-26	5743.82
54	LEn59yqQjdD1mTbZq9nPr7DSz29bEFNF55	5,729.29593286	Replayed	Inactive	Dec-26	5729.29
55	LGvfmTYcSdMyPZtaoiTzgUnHa2pgtHnc	5,687.60858495	Replayed	Reactivated	Dec-26	5687.6
56	L7UNbXHSWJhJhQcDyG5bpQgocAWYL6uyT	5,655.70745282	Replayed	Reactivated	Dec-26	5655.7
57	L3FQzh4Jo2qGFkqxJZutugvaezgjpi5FF	5,569.13929976	Replayed	Inactive	Dec-26	5569.14
58	L9uTwFt6kAKDp6ajTXBLu6Hr32ibCre4HQ	5,393.73168321	Replayed	Inactive	Dec-26	5393.73
59	KvNvqLXxuwCL8g59BX2tVNGMWPrPnuLEh	5,362.55112771	Replayed	Inactive	Dec-26	5362.55
60	L4Z9rYrZt6GCZALXgQxadMYshREAgJdbaf	5,349.26785591	Replayed	Reactivated	Dec-26	5349.27
				total		4174368.31

上述表格中标记为“未激活”（Inactive）的状态，表示无法证明该地址归攻击者所有，暗示这些交易可能只是为了制造公众混乱与迷惑而执行的。

附录 B：当前活跃持币者与总持币者统计



图表中“总地址数”（Total）与“活跃地址数”（Active）之间的差额，代表“休眠”钱包数量（复活初期为5651个地址，重放攻击后降至4561个地址）。

附录 C：“Murad” 风格指标

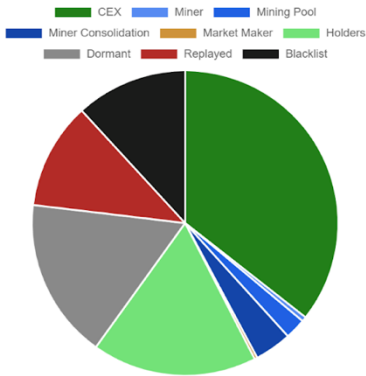
💎👤-EDNESS METRICS	
ALL WALLETS	
Holders	13659
All-Time Wallets Holding > \$100K	178
Wallets still Holding > 50% of peak coins	80
Wallets still holding > 50% of peak coins (%-age)	45%
ACTIVE WALLETS	
Active Holders ⓘ	9098
Active All-Time Wallets Holding > \$100K	108
Active Wallets still Holding > 50% 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

截至 2025 年 6 月 12 日

附录 D：当前持币者分布情况

TOP 100 HOLDERS STATISTICS		
	Amount of coins in top 100 addresses	14,623,068.43
	Percentage of total circulating 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

Top 100 Addresses (%-age)



截至 2025 年 6 月 12 日

