LIGONE / LIG1

Technical Security Documentation - V3

Prepared for Blockaid Security Team
Base Network | 12 September 2026

Purpose

This document consolidates the technical security evidence for the deployed LIGONE (LIG1) system on Base. It preserves the prior contract and Mainnet assessment, adds Blockaid's latest risk categories, and adds the documented functional-validation history performed before Mainnet use.

Evidence layers

Layer	Evidence
1. Deployed source	Five central contracts publicly verified on BaseScan
2. Live configuration	Contract links and one-time initialization state reviewed
3. Pre-deployment validation	Functional testing performed before production deployment
4. Base Sepolia validation	Contract interactions and protection paths tested in a test environment
5. Base Mainnet evidence	Successful buy, sell and Private LP deposit observed on-chain

No deployed contract has been modified for this documentation. LIGONE does not propose contract changes merely to accommodate generic scanner heuristics. A concrete vulnerability should be tied to a specific contract, function, privilege or observed behavior.

Important limitation

This is project-prepared technical security documentation. It is not an independent third-party audit, certification, guarantee of absence of vulnerabilities, or legal opinion.

1. Scope and Deployed Contracts

Component	Base address	Role / verification
LIG1Core	0x5b517A3d16213d1FD38e21CDEc3cFe0bE5b81Af9	BaseScan verified; token core
LiquidityVault	0xA760F0ba595ECc00BEF0a487562F98dDd2b2Db22	BaseScan verified; fee/system liquidity vault
RewardController	0xF82B42ca2F40c5b9836e2855Bf7Ed1047a08188A	BaseScan Exact Match; reward authorization
PrivateLPManager	0xe6290C358B80B72E8330389b0858e88d241b3724	BaseScan verified; private LP positions
SystemLPVault	0x799605e2d7Ba94f65568E8a328F8F56F6FA5a860	BaseScan verified; system LP custody

Additional live addresses

System LIG1/USDC pair: **0x91De242aB1a49A982d7Ab5bC0eE96Bd30983A7DD**
Base USDC: **0x833589fCD6eDb6E08f4c7C32D4f71b54bdA02913**
Initializer / Reward Oracle / LiquidityVault admin EOA: **0x5883C4013B4051e7f47624dC81B7118dE8fbD0FF**

Verification settings

Reviewed contracts were compiled with Solidity 0.8.34 (commit 80d5c536), optimizer enabled with 200 runs, EVM target Osaka.

2. Live Configuration Verification

LIG1Core: initialPool = system pair; privateLPManager = PrivateLPManager; systemLPVault = SystemLPVault.
LiquidityVault: lig1 = LIG1Core; privateLPManager = PrivateLPManager; systemPair = system pair.
PrivateLPManager: lig1 = LIG1Core; liquidityVault = LiquidityVault; pair = system pair; usdc = Base USDC.
RewardController: rewardOracle = known EOA; lig1Core = LIG1Core.
SystemLPVault: lpToken = system pair.

> Relevant setup functions are one-time initialization paths. Live values are populated and point to the intended deployed components.

3. Functional Validation History

The LIG1 system was functionally tested before production deployment and was subsequently exercised in a Base Sepolia test environment. The following matrix records the concrete test behavior documented during development. It is presented as functional evidence, not as an independent audit.

Area	Documented test / observation	Result
Deployment / initialization	SystemLPVault had to be initialized before Core pool initialization; an attempted wrong order reverted with 'system LP vault not initialized'. Correct order was then used.	Expected guard observed; correct initialization succeeded
System LP	Initial system liquidity mint / setup was executed after required initialization.	Successful
Purchase state	hasPurchasedLIG1 was checked after purchase.	Returned true
Maximum wallet	A large MockV2PairSwap was attempted against the wallet limit.	Reverted with 'max wallet exceeded'
Private LP approval	A deposit was first attempted without sufficient token allowance.	Allowance failure observed as expected
Private LP deposit	After approvals, a deposit of 10,000 LIG1 plus the required USDC amount was executed in the test environment.	Successful; LP tokens minted
Private LP withdrawal	Withdrawal path was exercised after deposit.	Successful
Reward authorization	approveReward was attempted from an unauthorized caller.	Reverted; only rewardOracle accepted
Reward execution marking	markExecuted was attempted outside the authorized Core path.	Reverted; only Core accepted
Reward execution	executeReward authorization was tested from a wallet other than the intended recipient/owner.	Reverted as expected
Trading / quoting	Swap / pair behavior and protection paths were exercised during testing.	Functional path tested; protection reverts observed where expected

Test-evidence boundary

The development record confirms the functional tests above. This document does not invent transaction hashes or exact testnet block references where they are not presently included in the evidence set. Mainnet transaction hashes are listed separately below.

> The validation sequence is therefore: pre-deployment functional testing -> Base Sepolia testing -> Base Mainnet production evidence.

4. Token Supply, Minting and Trading Controls

Maximum supply is **1,000,000,000 LIG1**. Initial system-liquidity mint is **20,000,000 LIG1**; maximum reward supply is **980,000,000 LIG1**. The reviewed Core contains the one-time initial system-liquidity mint and the constrained reward execution path. No unrestricted owner/admin mint function was identified.

Reward execution is constrained by Core rules including maximum reward supply, maximum total supply, per-wallet limits, rolling issuance limits, maximum-wallet enforcement and recipient-wallet execution of an approved reward.

Trading rules

Fixed rules include maximum wallet **2,000,000 LIG1 (0.2%)**, buy fee **0.1%**, sell fee **1%** before 100 days and **0.1%** after 100 days. Purchases create timestamped tranches and sell-fee calculation follows FIFO logic.

> The 100-day mechanism is a fee rule, not a sell lock. Live Mainnet evidence confirms that LIG1 can be sold for USDC.

5. What Administrators Can and Cannot Do

Capability	Result	Technical meaning
Mint arbitrary LIG1	NO	No unrestricted owner/admin mint path identified
Change buy/sell fees	NO	Fixed rules; no fee setter identified
Blacklist arbitrary wallets	NO	No callable wallet blacklist setter identified
Pause all trading	NO	No global pause function identified
Withdraw System LP	NO	SystemLPVault exposes no withdrawal/transfer function
Sweep LiquidityVault arbitrarily	NO	No arbitrary rescue/sweep recipient path identified
Approve/cancel rewards	LIMITED	Immutable rewardOracle authorization; cannot directly mint
Execute reward mint	CONSTRAINED	Recipient wallet via Core and subject to Core limits
Withdraw Private LP	USER ONLY	Voluntary user position, not System LP

6. Liquidity Architecture and Protection

LIG1 has two distinct liquidity mechanisms that must not be conflated in a withdrawal-risk assessment.

System LP

System liquidity is added through the fixed system pair. LP tokens from the system path are directed to **SystemLPVault**. The reviewed SystemLPVault contains an immutable LP-token reference and an lpBalance() view function; no LP withdrawal or transfer function exists.

> System LP is not ordinary unlocked owner-held LP. No callable SystemLPVault function was identified that can transfer or withdraw those LP tokens.

Private LP

PrivateLPManager permits voluntary user-owned LIG1/USDC liquidity. Deposit requires a prior LIG1 purchase and the configured pool ratio. Withdrawal is intentionally available to the respective provider and charges a 0.1% LIG1 and USDC fee to LiquidityVault. Returned/claimed LIG1 receives a new tranche timestamp.

Mainnet Private LP evidence

Successful Deposit transaction: **0x0bc45b4dfbb0755d27318036a10f7d5a307fa0cfa43cf32e0f8cca206d5e6529**. LIG1 and USDC were transferred through PrivateLPManager to the system pair and LP tokens were minted.

Liquidity depth

Liquidity depth is a dynamic market condition rather than an administrator privilege. LIGONE intends liquidity growth through organic activity and voluntary Private LP participation, not artificial volume or price activity.

7. Direct Response to Blockaid's Latest Risk Categories

Blockaid category	LIG1 evidence / response	Status
Secure Liquidity	System LP is held by SystemLPVault; reviewed vault has no withdrawal/transfer function. Private LP is separate user-owned liquidity.	System LP protection implemented
Dangerous Privileges	No unrestricted mint, fee setter, callable wallet blacklist, global pause, arbitrary vault sweep or System LP withdrawal identified.	No generic owner-style privilege identified
Independent Audit	This documentation is project-prepared and does not claim to be a third-party audit.	External evidence remains separate
Verification Issues	Five central deployed contracts, addresses, roles and compiler settings are documented.	Request exact discrepancy if still detected
Liquidity & Stability	Liquidity is intended to grow organically and through voluntary Private LP.	Ongoing market-development item
Transparency	Supply, fees, roles, mint constraints, liquidity architecture and live transaction evidence are documented.	Substantially documented; holder data dynamic

Requested technical specificity

If a category remains an active malicious/rug-pull signal after review, LIGONE requests the affected contract address, callable function or privilege, relevant source/bytecode pattern, observed on-chain behavior, and why that specific behavior is considered malicious or indicative of rug-pull risk.

> General security recommendations should be distinguished from LIG1-specific technical findings.

8. Scanner-Relevant Characteristics

Concern	Observed behavior	Assessment
Hidden owner / privilege	Immutable or one-time roles exist; no unrestricted owner-style control over minting, trading or System LP withdrawal identified.	Custom access control
Transfer pausable	No global transfer pause; LP context flags limited to fixed system flows.	Not general pause
Blacklist	No callable wallet blacklist setter identified.	No callable blacklist identified
Anti-whale	Fixed 0.2% maximum-wallet rule; test evidence includes expected max-wallet revert.	Intentional fixed restriction
Honeypot / sell restriction	Successful Mainnet sell returned USDC; 100-day rule changes fee only.	Live evidence contradicts honeypot behavior
Minting	One-time system mint plus constrained rewards; no unrestricted admin mint identified.	Bounded issuance
Liquidity withdrawal	SystemLPVault has no withdrawal; PrivateLPManager withdrawal is user-position scoped.	System/private LP distinction

9. Mainnet Transaction Evidence

BUY: 0x0d06d246687752f214ab36a932174a9ddb5f90f0cc85e145cafe1ddc38e3410f - Success. Buyer transferred 7 USDC; observed fee matched 0.1%.

SELL: 0x0721262ec8d102039ae6c0011e89f3305ce25316c5647f3c5244026e3ff5eaa6 - Success. Pair returned 0.495012 USDC; observed fee matched 1.0% pre-100-day fee.

PRIVATE LP DEPOSIT: 0x0bc45b4dfbb0755d27318036a10f7d5a307fa0cfa43cf32e0f8cca206d5e6529 - Success. User assets entered the system pair through PrivateLPManager and LP tokens were minted.

10. Transparency and Evidence Gaps

ligone.ch is intended to provide public verification information in addition to explanatory content. Contract addresses, supply rules, fees, reward issuance, System LP, Private LP and live market information should remain easy to locate and consistent with on-chain state.

Evidence that should not be overstated

Item	Treatment
Independent third-party audit	Not claimed; remains separate external evidence
Dynamic holder distribution	Should be provided as a dated on-chain snapshot if requested
Historical testnet transaction hashes	Not invented where not presently included in the evidence set
Absence of all possible vulnerabilities	Not guaranteed by project-prepared functional testing

11. Security Findings

Severity	Finding / observation	Assessment
Critical	None identified	No Critical finding identified in reviewed scope
High	None identified	No High finding identified in reviewed scope
Informational	Private LP withdrawal/claim resets returned LIG1 tranche timestamp	Intentional; disclose to users
Informational	Custom immutable/one-time setup and reward roles	Limited scope
Informational	Maximum-wallet restriction	Intentional fixed anti-whale rule
External evidence gap	Independent third-party audit not included	Not represented as an independent audit

12. Conclusion and Request for Reassessment

The consolidated evidence covers verified deployed source code, live configuration, functional validation before Mainnet use, Base Sepolia testing, and successful Base Mainnet buy, sell and Private LP behavior. The reviewed architecture shows constrained reward issuance, fixed trading rules, a SystemLPVault without a withdrawal function, and separate voluntary user-owned Private LP.

LIGONE respectfully requests reassessment of the current classification using the actual deployed source code and the documented test/on-chain evidence.

> If the flag remains, please identify the exact unresolved LIG1-specific technical condition: contract address, function or privilege, source/bytecode pattern, observed on-chain behavior, and reason for the risk classification.

No contract modification commitment

The deployed contracts will not be modified merely to conform to generic scanner heuristics. If a concrete vulnerability is identified, LIGONE requests sufficient technical detail for independent assessment.

Independent audit

An independent third-party audit is acknowledged as a separate form of evidence. Its absence should not be conflated with a demonstrated malicious function. If Blockaid requires an independent audit as a policy condition for reassessment, LIGONE requests that this requirement be stated separately from contract-specific findings.

Prepared by: LIGONE / LIG1
Contact: René Herrchen
Date: 12 September 2026

Important limitation: This document is project-prepared technical security documentation. It is not an independent third-party audit, certification, guarantee of absence of vulnerabilities, or legal opinion.