LIGONE / LIG1

Technische Sicherheitsdokumentation - V3

Erstellt für das Blockaid Security Team
Base Network | 12. September 2026

Zweck

Dieses Dokument führt die technischen Sicherheitsnachweise für das auf Base bereitgestellte LIGONE-(LIG1)-System zusammen. Es übernimmt die bisherige Contract- und Mainnet-Bewertung, ergänzt die zuletzt von Blockaid genannten Risikokategorien und dokumentiert zusätzlich die vor der Mainnet-Nutzung durchgeführte funktionale Validierung.

Evidenzebenen

Ebene	Nachweis
1. Bereitgestellter Sourcecode	Fünf zentrale Contracts sind öffentlich auf BaseScan verifiziert
2. Live-Konfiguration	Contract-Verknüpfungen und Status der einmaligen Initialisierung wurden geprüft
3. Validierung vor Deployment	Funktionstests wurden vor dem produktiven Deployment durchgeführt
4. Base-Sepolia-Validierung	Contract-Interaktionen und Schutzmechanismen wurden in einer Testumgebung geprüft
5. Base-Mainnet-Nachweise	Erfolgreicher Kauf, Verkauf und Private-LP-Deposit wurden on-chain beobachtet

Für diese Dokumentation wurde kein bereitgestellter Contract verändert. LIGONE schlägt keine Contract-Änderungen allein zur Anpassung an allgemeine Scanner-Heuristiken vor. Eine konkrete Schwachstelle sollte einem bestimmten Contract, einer Funktion, einem Privileg oder einem beobachteten Verhalten zugeordnet werden.

Wichtige Einschränkung

Dies ist eine vom Projekt erstellte technische Sicherheitsdokumentation. Sie ist kein unabhängiges Third-Party-Audit, keine Zertifizierung, keine Garantie für die Abwesenheit von Schwachstellen und keine Rechtsberatung.

1. Umfang und bereitgestellte Contracts

Komponente	Base-Adresse	Rolle / Verifizierung
LIG1Core	0x5b517A3d16213d1FD38e21CDEc3cFe0bE5b81Af9	BaseScan verifiziert; Token-Core
LiquidityVault	0xA760F0ba595ECc00BEF0a487562F98dDd2b2Db22	BaseScan verifiziert; Gebühren-/Systemliquiditäts-Vault
RewardController	0xF82B42ca2F40c5b9836e2855Bf7Ed1047a08188A	BaseScan Exact Match; Reward-Autorisierung
PrivateLPManager	0xe6290C358B80B72E8330389b0858e88d241b3724	BaseScan verifiziert; Private-LP-Positionen
SystemLPVault	0x799605e2d7Ba94f65568E8a328F8F56F6FA5a860	BaseScan verifiziert; Verwahrung der System-LP

Weitere Live-Adressen

System LIG1/USDC Pair: **0x91De242aB1a49A982d7Ab5bC0eE96Bd30983A7DD**
Base USDC: **0x833589fCD6eDb6E08f4c7C32D4f71b54bdA02913**
Initializer / Reward Oracle / LiquidityVault-Admin EOA: **0x5883C4013B4051e7f47624dC81B7118dE8fbD0FF**

Verifizierungseinstellungen

Die geprüften Contracts wurden mit Solidity 0.8.34 (Commit 80d5c536), aktiviertem Optimizer mit 200 Runs und EVM-Ziel Osaka kompiliert.

2. Verifizierung der Live-Konfiguration

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 = bekannte EOA; lig1Core = LIG1Core.
SystemLPVault: lpToken = System-Pair.

Die relevanten Setup-Funktionen sind einmalige Initialisierungspfade. Die Live-Werte sind gesetzt und verweisen auf die vorgesehenen bereitgestellten Komponenten.

3. Historie der funktionalen Validierung

Das LIG1-System wurde vor dem produktiven Deployment funktional getestet und anschließend zusätzlich in einer Base-Sepolia-Testumgebung ausgeführt. Die folgende Matrix dokumentiert die während der Entwicklung festgehaltenen konkreten Testverläufe. Sie dient als funktionaler Nachweis und wird nicht als unabhängiges Audit dargestellt.

Bereich	Dokumentierter Test / Beobachtung	Ergebnis
Deployment / Initialisierung	SystemLPVault musste vor der Core-Pool-Initialisierung initialisiert sein; bei falscher Reihenfolge erfolgte der Revert 'system LP vault not initialized'. Danach wurde die korrekte Reihenfolge verwendet.	Erwarteter Schutz beobachtet; korrekte Initialisierung erfolgreich
System LP	Initiales System-Liquidity-Minting / Setup wurde nach den erforderlichen Initialisierungsschritten ausgeführt.	Erfolgreich
Kaufstatus	hasPurchasedLIG1 wurde nach einem Kauf geprüft.	true zurückgegeben
MaxWallet	Ein großer MockV2PairSwap wurde gegen das Wallet-Limit getestet.	Revert 'max wallet exceeded'
Private-LP-Approval	Deposit wurde zunächst ohne ausreichende Token-Allowance versucht.	Allowance-Fehler wie erwartet
Private-LP-Deposit	Nach den Approvals wurden 10.000 LIG1 plus der erforderliche USDC-Betrag in der Testumgebung eingezahlt.	Erfolgreich; LP-Token gemintet
Private-LP-Withdrawal	Der Withdrawal-Pfad wurde nach einem Deposit ausgeführt.	Erfolgreich
Reward-Autorisierung	approveReward wurde von einem nicht autorisierten Caller versucht.	Revert; nur rewardOracle akzeptiert
Reward-Ausführungsmarkierung	markExecuted wurde außerhalb des autorisierten Core-Pfads versucht.	Revert; nur Core akzeptiert
Reward-Ausführung	executeReward-Autorisierung wurde von einer anderen Wallet als dem vorgesehenen Empfänger/Eigentümer getestet.	Revert wie erwartet
Trading / Quoting	Swap-/Pair-Verhalten und Schutzpfade wurden während der Tests ausgeführt.	Funktionspfade getestet; erwartete Schutz-Reverts beobachtet

Grenzen der Test-Evidenz

Die Entwicklungsaufzeichnungen bestätigen die oben aufgeführten Funktionstests. Dieses Dokument erfindet keine Transaktionshashes oder exakten Testnet-Blockreferenzen, wenn diese im derzeit vorliegenden Evidenzsatz nicht enthalten sind. Mainnet-Transaktionshashes werden separat aufgeführt.

> Die Validierungskette lautet damit: Funktionstests vor Deployment -> Base-Sepolia-Tests -> Base-Mainnet-Produktionsnachweise.

4. Token Supply, Minting und Handelsregeln

Der maximale Supply beträgt **1.000.000.000 LIG1**. Der initiale Mint für die Systemliquidität beträgt **20.000.000 LIG1**; der maximale Reward-Supply beträgt **980.000.000 LIG1**. Der geprüfte Core enthält den einmaligen initialen System-Liquidity-Mint und den begrenzten Reward-Ausführungspfad. Eine uneingeschränkte Owner-/Admin-Mint-Funktion wurde nicht identifiziert.

Die Reward-Ausführung wird durch Core-Regeln begrenzt, darunter maximaler Reward-Supply, maximaler Gesamt-Supply, Wallet-Limits, rollierende Ausgabelimits, MaxWallet-Durchsetzung und die Ausführung eines genehmigten Rewards durch die Empfänger-Wallet.

Handelsregeln

Zu den festen Regeln gehören MaxWallet **2.000.000 LIG1 (0,2 %)**, Kaufgebühr **0,1 %**, Verkaufsgebühr **1 %** vor 100 Tagen und **0,1 %** nach 100 Tagen. Käufe erzeugen zeitgestempelte Tranchen; die Berechnung der Verkaufsgebühr folgt FIFO.

> Der 100-Tage-Mechanismus ist eine Gebührenregel und keine Verkaufssperre. Live-Mainnet-Nachweise bestätigen, dass LIG1 gegen USDC verkauft werden kann.

5. Was Administratoren können und nicht können

Fähigkeit	Ergebnis	Technische Bedeutung
Beliebig LIG1 minten	NEIN	Kein uneingeschränkter Owner-/Admin-Mint-Pfad identifiziert
Kauf-/Verkaufsgebühren ändern	NEIN	Feste Regeln; kein Fee-Setter identifiziert
Beliebige Wallets blacklisten	NEIN	Kein aufrufbarer Wallet-Blacklist-Setter identifiziert
Gesamten Handel pausieren	NEIN	Keine globale Pause-Funktion identifiziert
System-LP entnehmen	NEIN	SystemLPVault stellt keine Withdrawal-/Transfer-Funktion bereit
LiquidityVault beliebig leeren	NEIN	Kein beliebiger Rescue-/Sweep-Pfad zu frei wählbaren Empfängern identifiziert
Rewards genehmigen/stornieren	BEGRENZT	Immutable rewardOracle-Autorisierung; kein direktes Minting
Reward-Mint ausführen	BEGRENZT	Empfänger-Wallet über Core und unter Core-Limits
Private LP entnehmen	NUR NUTZER	Freiwillige Nutzerposition, nicht System-LP

6. Liquiditätsarchitektur und Schutz

LIG1 verfügt über zwei unterschiedliche Liquiditätsmechanismen, die bei der Bewertung eines Withdrawal-Risikos nicht miteinander vermischt werden dürfen.

System LP

Systemliquidität wird über das feste System-Pair hinzugefügt. LP-Token aus dem Systempfad werden an den **SystemLPVault** geleitet. Der geprüfte SystemLPVault enthält eine immutable LP-Token-Referenz und die View-Funktion lpBalance(); eine LP-Withdrawal- oder Transfer-Funktion existiert nicht.

> System-LP ist daher nicht mit gewöhnlicher, ungesperrter Owner-LP gleichzusetzen. Es wurde keine aufrufbare SystemLPVault-Funktion identifiziert, die diese LP-Token übertragen oder entnehmen kann.

Private LP

Der PrivateLPManager ermöglicht freiwillige, nutzereigene LIG1/USDC-Liquidität. Ein Deposit erfordert einen vorherigen LIG1-Kauf und das konfigurierte Poolverhältnis. Ein Withdrawal steht bewusst dem jeweiligen Anbieter zur Verfügung und führt 0,1 % LIG1- und USDC-Gebühr an den LiquidityVault ab. Zurückgegebene bzw. geclaimte LIG1 erhalten einen neuen Tranche-Zeitstempel.

Mainnet-Nachweis für Private LP

Erfolgreiche Deposit-Transaktion: **0x0bc45b4dfbb0755d27318036a10f7d5a307fa0cfa43cf32e0f8cca206d5e6529**. LIG1 und USDC wurden über den PrivateLPManager an das System-Pair übertragen und LP-Token wurden gemintet.

Liquiditätstiefe

Die Liquiditätstiefe ist eine dynamische Marktbedingung und kein Administratorprivileg. LIGONE beabsichtigt Liquiditätswachstum durch organische Aktivität und freiwillige Private-LP-Teilnahme, nicht durch künstliches Volumen oder künstliche Preisaktivität.

7. Direkte Antwort auf Blockaids aktuelle Risikokategorien

Blockaid-Kategorie	LIG1-Nachweis / Antwort	Status
Secure Liquidity	System-LP liegt im SystemLPVault; der geprüfte Vault besitzt keine Withdrawal-/Transfer-Funktion. Private LP ist getrennte, nutzereigene Liquidität.	System-LP-Schutz implementiert
Dangerous Privileges	Kein uneingeschränktes Minting, kein Fee-Setter, keine aufrufbare Wallet-Blacklist, keine globale Pause, kein beliebiges Vault-Sweep und keine System-LP-Entnahme identifiziert.	Kein allgemeines Owner-Privileg identifiziert
Independent Audit	Diese Dokumentation wurde vom Projekt erstellt und beansprucht nicht, ein unabhängiges Third-Party-Audit zu sein.	Externer Nachweis bleibt separat
Verification Issues	Fünf zentrale bereitgestellte Contracts, Adressen, Rollen und Compiler-Einstellungen sind dokumentiert.	Bei weiterem Befund wird die genaue Diskrepanz angefordert
Liquidity & Stability	Liquidität soll organisch und über freiwillige Private LP wachsen.	Laufender Marktentwicklungspunkt
Transparency	Supply, Gebühren, Rollen, Mint-Limits, Liquiditätsarchitektur und Live-Transaktionsnachweise sind dokumentiert.	Weitgehend dokumentiert; Holder-Daten dynamisch

Anforderung technischer Konkretisierung

Wenn eine Kategorie nach Prüfung weiterhin als aktives Malicious-/Rug-Pull-Signal gilt, bittet LIGONE um Angabe der betroffenen Contract-Adresse, der aufrufbaren Funktion oder des Privilegs, des relevanten Source-/Bytecode-Musters, des beobachteten On-Chain-Verhaltens sowie der Begründung, warum genau dieses Verhalten als bösartig oder als Hinweis auf ein Rug-Pull-Risiko eingestuft wird.

> Allgemeine Sicherheitsempfehlungen sollten von konkreten LIG1-spezifischen technischen Findings getrennt werden.

8. Scanner-relevante Eigenschaften

Bedenken	Beobachtetes Verhalten	Bewertung
Hidden Owner / Privileg	Immutable oder einmalige Rollen existieren; keine uneingeschränkte Owner-Kontrolle über Minting, Handel oder System-LP-Entnahme identifiziert.	Spezifische Zugriffskontrolle
Transfer pausable	Keine globale Transfer-Pause; LP-Kontextflags sind auf feste Systempfade begrenzt.	Kein allgemeiner Pause-Mechanismus
Blacklist	Kein aufrufbarer Wallet-Blacklist-Setter identifiziert.	Keine aufrufbare Blacklist identifiziert
Anti-Whale	Feste 0,2-%-MaxWallet-Regel; Test-Evidenz enthält erwarteten MaxWallet-Revert.	Beabsichtigte feste Beschränkung
Honeypot / Sell Restriction	Erfolgreicher Mainnet-Sell lieferte USDC; die 100-Tage-Regel ändert nur die Gebühr.	Live-Evidenz widerspricht Honeypot-Verhalten
Minting	Einmaliger System-Mint plus begrenzte Rewards; kein uneingeschränktes Admin-Minting identifiziert.	Begrenzte Ausgabe
Liquidity Withdrawal	SystemLPVault ohne Withdrawal; PrivateLPManager-Withdrawal ist auf Nutzerpositionen begrenzt.	System-/Private-LP-Trennung

9. Mainnet-Transaktionsnachweise

BUY: 0x0d06d246687752f214ab36a932174a9ddb5f90f0cc85e145cafe1ddc38e3410f - Success. Käufer übertrug 7 USDC; die beobachtete Gebühr entsprach 0,1 %.

SELL: 0x0721262ec8d102039ae6c0011e89f3305ce25316c5647f3c5244026e3ff5eaa6 - Success. Das Pair zahlte 0,495012 USDC an die verkaufende Wallet; die beobachtete Gebühr entsprach 1,0 % vor Ablauf der 100 Tage.

PRIVATE LP DEPOSIT: 0x0bc45b4dfbb0755d27318036a10f7d5a307fa0cfa43cf32e0f8cca206d5e6529 - Success. Nutzer-Assets gelangten über den PrivateLPManager in das System-Pair und LP-Token wurden gemintet.

10. Transparenz und Evidenzlücken

ligone.ch soll neben Erklärinhalten auch öffentliche Verifizierungsinformationen bereitstellen. Contract-Adressen, Supply-Regeln, Gebühren, Reward-Ausgabe, System LP, Private LP und Live-Marktdaten sollen leicht auffindbar und mit dem On-Chain-Stand konsistent sein.

Evidenz, die nicht übertrieben dargestellt werden darf

Punkt	Behandlung
Unabhängiges Third-Party-Audit	Wird nicht behauptet; bleibt separater externer Nachweis
Dynamische Holder-Verteilung	Soll bei Bedarf als datierter On-Chain-Snapshot bereitgestellt werden
Historische Testnet-Transaktionshashes	Werden nicht erfunden, wenn sie im aktuellen Evidenzsatz nicht vorliegen
Abwesenheit aller denkbaren Schwachstellen	Wird durch projektinterne Funktionstests nicht garantiert

11. Sicherheits-Findings

Schweregrad	Finding / Beobachtung	Bewertung
Critical	Keine identifiziert	Kein Critical Finding im geprüften Umfang identifiziert
High	Keine identifiziert	Kein High Finding im geprüften Umfang identifiziert
Informational	Private-LP-Withdrawal/Claim setzt den Tranche-Zeitstempel zurückgegebener LIG1 neu	Beabsichtigt; gegenüber Nutzern offenlegen
Informational	Spezifische immutable/einmalige Setup- und Reward-Rollen	Begrenzter Umfang
Informational	MaxWallet-Beschränkung	Beabsichtigte feste Anti-Whale-Regel
Externe Evidenzlücke	Unabhängiges Third-Party-Audit nicht enthalten	Wird nicht als unabhängiges Audit dargestellt

12. Schlussfolgerung und Antrag auf Neubewertung

Die zusammengeführten Nachweise umfassen verifizierten bereitgestellten Sourcecode, Live-Konfiguration, funktionale Validierung vor der Mainnet-Nutzung, Base-Sepolia-Tests sowie erfolgreiche Buy-, Sell- und Private-LP-Abläufe auf Base Mainnet. Die geprüfte Architektur zeigt begrenzte Reward-Ausgabe, feste Handelsregeln, einen SystemLPVault ohne Withdrawal-Funktion und davon getrennte freiwillige nutzereigene Private LP.

LIGONE bittet um Neubewertung der aktuellen Klassifizierung auf Grundlage des tatsächlich bereitgestellten Sourcecodes sowie der dokumentierten Test- und On-Chain-Nachweise.

Falls der Flag bestehen bleibt, bitten wir um Angabe der exakten ungelösten LIG1-spezifischen technischen Bedingung: Contract-Adresse, Funktion oder Privileg, Source-/Bytecode-Muster, beobachtetes On-Chain-Verhalten und Begründung der Risikoklassifizierung.

Keine Verpflichtung zu Contract-Änderungen

Die bereitgestellten Contracts werden nicht allein deshalb verändert, um allgemeinen Scanner-Heuristiken zu entsprechen. Wird eine konkrete Schwachstelle identifiziert, bittet LIGONE um ausreichende technische Details für eine unabhängige Bewertung.

Unabhängiges Audit

Ein unabhängiges Third-Party-Audit wird als separate Form von Evidenz anerkannt. Sein Fehlen darf nicht mit dem Nachweis einer bösartigen Funktion gleichgesetzt werden. Falls Blockaid ein unabhängiges Audit als Policy-Voraussetzung für eine Neubewertung verlangt, bittet LIGONE darum, diese Voraussetzung getrennt von Contract-spezifischen Sicherheits-Findings auszuweisen.

Erstellt von: LIGONE / LIG1
Kontakt: René Herrchen
Datum: 12. September 2026

Wichtige Einschränkung: Dieses Dokument ist eine vom Projekt erstellte technische Sicherheitsdokumentation. Es ist kein unabhängiges Third-Party-Audit, keine Zertifizierung, keine Garantie für die Abwesenheit von Schwachstellen und keine Rechtsberatung.