



DUE DILIGENCE SCAN

Public Evidence & Risk Screening

Automated mainnet review of visible technical, transparency, liquidity, holder, deployer, and control signals. Non-advisory input to further due diligence.

Project	CHT Mainnet Core + GasVault
Network	base
Environment	Mainnet
Scan type	Automated · no human audit
Date	2026-07-30

EXECUTIVE ASSESSMENT

● Multisig-backed administration, pre-issuance state

All 13 contracts in scope are publicly source-verified and have runtime code present at pinned Base block 49,309,312. High-impact administration is held by a Safe 1.4.1 configured 2-of-3, which controls 37 issuer/admin and enumerable-role relationships across the system. Three narrower operational authorities remain assigned to separate EOAs. The token remains unissued, GasVault is unfunded, and no CHT/WETH or CHT/USDC liquidity was observed on the probed venues.

SCAN VERDICT

SUBJECT

MIXED

ANALYSIS

COMPLETE

11 of 11 modules applicable

Primary run: 6 checks, 0 findings · system bytecode unchanged

No investment recommendation — this report does not evaluate expected return, suitability, price potential, or whether to buy, sell, hold, subscribe to, or avoid any token or offering.

13 / 13 Contracts source-verified;
bytecode unchanged

2-of-3
Safe

37 high-impact authority
relationships

0
roles

Current privileges retained by
deployer

Zero Supply, GasVault balance and
observed DEX pools

Top transparency indicators

Heuristic editorial reading of the evidence. The authoritative verdict basis is the verdict-axes table further down in this section; when an axis chip is present below it overrides the heuristic chip on disagreement.

TRANSPARENCY

OK

AXIS: PASS

Source code verified

Implementation logic is independently inspectable from explorer evidence.

REQUIRED

Manual code review remains the next step for any code-level conclusion.

CONTROL

IMPROVED

AXIS: PASS

High-impact authority moved to a 2-of-3 Safe

The Safe holds 37 issuer/admin or enumerable-role relationships; the deployment EOA now holds none.

REQUIRED

Keep the three remaining operational EOA permissions narrow and monitor Safe owner/module changes.

UPGRADEABILITY

LOCKED

AXIS: PASS

Contract is not a proxy

Logic cannot be replaced after deployment; what is on-chain is what will execute.

REQUIRED

Confirm immutability assumption against any future migration off-chain.

MARKET EVIDENCE

NOT OBSERVED

AXIS: SOFT FAIL

Pre-issuance state remains

Total supply, GasVault balance and CHT/WETH or CHT/USDC pool count remained zero.

REQUIRED

Repeat supply, holder, balance and liquidity checks after issuance or launch.

Coverage matrix

Contract inventory	CHECKED	Source code verification	CHECKED
Proxy and upgradeability	CHECKED	Ownership and admin	CHECKED
Access control roles	CHECKED	Deployer analysis	CHECKED
Multisig wallet detection	CHECKED	Holder distribution	CHECKED
DEX liquidity	CHECKED	Fund flow	CHECKED
Static analysis	CHECKED		

Scope — automated review of selected public technical and on-chain evidence available at scan time.

Not — Not investment, financial, legal, tax, regulatory, MiCA, or audit advice.

Verdict axes (authoritative basis)

The dashboard above summarises the report. The block below is the scan's ASVS-style verdict that the dashboard derives from: each transparency axis with its outcome, modality, and quantitative basis. If any dashboard chip appears to disagree with an axis outcome here, the axis outcome below is authoritative; the dashboard chip is a heuristic restatement.

Public on-chain transparency · Verdict logic v6

Subject verdict: MIXED

Analysis verdict: COMPLETE (11 of 11 modules applicable)

Axes (ASVS-style):

Axis	Modality	Outcome	Detail
source visibility	MUST	PASS	
control concentration	MUST	PASS	addresses_probed = 4, safes_detected = 1
holder concentration	SHOULD	N_A	
liquidity visibility	SHOULD	SOFT_FAIL	pools_observed = 0
upgrade authority	MUST	PASS	

Priority findings:

- axis soft fail on `liquidity_visibility`

Verdict reflects the share of the public on-chain transparency surface that the scan was able to observe; it is not a merit ranking and does not assess whether the project is suitable for any particular use.

2. Modules examined

The framework checks eleven modules against the scan's evidence. The two tables below summarise the result for each module and the privileged accounts surfaced across modules; the per-module subsections that follow go into detail.

Module results — at a glance

Module	Status	Result at a glance
Contract inventory	Examined	1 primary + 12 related contract(s) in scope
Source code verification	Examined	13 of 13 verified on the explorer
Proxy and upgradeability	Examined	no recognised proxy pattern
Ownership and admin	Examined	no Ownable owner observed
Access control roles	Examined	yes (5 role(s))
Deployer analysis	Examined	EOA; no privileged role(s) detected
Multisig wallet detection	Examined	1 of 4 privileged address(es) backed by a multisig
Holder distribution	Examined	not assessed
DEX liquidity	Examined	no pools observed on probed venues
Fund flow	Examined	1 direct funder(s) at 1-hop
Static analysis	Examined	current primary run: 6 checks, 0 findings; all 13 bytecodes unchanged

Privileged accounts

Address	Type	Privileges held	Source
0x20718fc920da7e8ee5388b472bc8d83551cc0dbe	multisig (Safe, 2/3)	37 issuer/admin or enumerable-role relationships across the system	access_control, ownership_admin, safe_detection
0x6d39f9f42af67a67e2abac5b3dcd6b44ca14fb0a	EOA (not a Safe)	GasVault.GAS_OPERATOR_ROLE	access_control, safe_detection
0x081d62d59ee34b0bea968ef3c7ba4a40db33e6c5	EOA (not a Safe)	KYCRegistry.KYC_OPERATOR_ROLE	custom authority readback, safe_detection
0x8904058040dafd307d2176f8b79182f107d46173	EOA (not a Safe)	VoucherRedeemer.AUTHORIZED_SIGNER	custom authority readback, safe_detection

Type column legend. EOA = externally-owned account; contract = smart contract (not classified further); multisig (Safe, M/N) = identified Gnosis Safe with M-of-N threshold; X (not a Safe) = contract probed but did not match Safe bytecode; Not assessed = type not classified.

The scan probed 4 privileged addresses for Gnosis Safe bytecode patterns and identified 1 Safe(s); detected Safes are shown as multisig (Safe, M/N) in the Type column. Timelock detection is not implemented in the current scanner.

Per-module detail

Each module subsection has the same shape: what it checks (Purpose), what was found in this scan (deterministic), why it matters in general plus scan-specific elaboration, and what the result means for this scan specifically.

2.1 Contract inventory

Purpose — Lists every contract addressed by this scan: the primary token contract and any related contracts (sale, vesting, treasury) discovered during evidence collection.

What was found — Status: *Examined*

- Primary contract: 0x5C090Fb0eC462f029144E644EA698175f49521c9 (ERC-20 standard surface)
- Related contracts in scope: **12**

Role	Address	Source verification
treasury	0x919a7f3E1b4735b37899189cFc5AD1e910Faa79d	verified
treasury	0x90669C861083ec6a4849Cd881Cb13f8ef4E398C3	verified
distribution	0x162453987E8DF00725d88e7a15bdD0232C3919eD	verified
distribution	0xFBD1b3bff6bF6b295c147B6eA022CBAA340c10ea	verified
registry	0x994c6fCEB994Ef90F9b5b570d30846A519FC7fa2	verified
oracle	0x7Bb29a410168aca4Fc3fDF506DB63FE44bf7D073	verified
sale	0x4f2FDaaEAa10152f43322D66cb9d481D7b7becb0	verified
referral	0x616a2468c8EBB16022d67aa2fE5AC0fc741B6EBD	verified
distribution	0x40c63a2a53d5A39842928a6dDEfCf6f4a5d78381	verified
staking	0x559e1DAe39f5dBc39B9570752A2f74a9B683Bd2A	verified
registry	0x342Bf2061ebA91f7522F4C02F459c05308282d41	verified
other	0x3c15c4bea893fec8277f8d884250a0f0291bfa18	verified

Why it matters — A reader needs to know which addresses are in scope before drawing any conclusion. A token contract that depends on related sale or vesting contracts must be evaluated as a system.

The same 13-address deployment set was rechecked at Base block 49309312. Every address still had runtime code and a successful deployment receipt, with no bytecode change from the previous pinned block.

What it means —

The re-scan covers the same deployed system rather than only the token. The absence of runtime-code changes means the substantive delta is in live configuration and authority custody, not deployed logic.

2.2 Source code verification

Purpose — Checks whether the contracts' source code is publicly verified on the blockchain explorer. Verified source means anyone can read and audit the actual logic; unverified means only the compiled bytecode is visible.

What was found — Status: *Examined*

- Verified on the explorer: **13** contract(s) — `0x5C090Fb0eC462f029144E644EA698175f49521c9` , `0x919a7f3E1b4735b37899189cFc5AD1e910Faa79d` , `0x90669C861083ec6a4849Cd881Cb13f8ef4E398C3` , `0x162453987E8DF00725d88e7a15bdD0232C3919eD` , `0xFBD1b3bff6bF6b295c147B6eA022CBAA340c10ea` , `0x994c6fCEB994Ef90F9b5b570d30846A519FC7fa2` , `0x7Bb29a410168aca4Fc3fDF506DB63FE44bf7D073` , `0x4f2FDaaEAa10152f43322D66cb9d481D7b7becb0` , `0x616a2468c8EBB16022d67aa2fE5AC0fc741B6EBD` , `0x40c63a2a53d5A39842928a6dDEfCf6f4a5d78381` , `0x559e1DAe39f5dBc39B9570752A2f74a9B683Bd2A` , `0x342Bf2061ebA91f7522F4C02F459c05308282d41` , `0x3c15c4bea893fec8277f8d884250a0f0291bfa18`
- Unverified: **0** contract(s)

Why it matters — Verified source is the precondition for every other code-level check, including static analysis and independent audit. Without it, no one outside the development team can read what the contract actually does.

Etherscan v2 re-confirmed verified source for all 13 scoped addresses. Exact runtime-bytecode comparison against the prior scan found no changed contract.

What it means —

The deployed logic remains publicly inspectable and reproducible against the same 13 addresses. Source verification and unchanged bytecode support comparison, but they do not establish correctness or replace manual review.

2.3 Proxy and upgradeability

Purpose — Determines whether the primary contract is a proxy that delegates to a separate implementation contract, and if so, who controls upgrades.

What was found — Status: *Examined*

- Is a proxy: **no**
- Implementation address: *n/a*
- Upgrade administrator: *n/a*

Why it matters — An upgradeable contract can change behaviour after deployment. The address (or governance) controlling the upgrade is therefore as important as the current code.

Pinned reads found zero values in the EIP-1967 implementation, admin and beacon slots for every scoped contract. No recognised proxy upgrade path was observed.

What it means —

No standard EIP-1967 upgrade mechanism was observed. Migration to new addresses or mechanisms outside the checked slots remains possible and would require another scan.

2.4 Ownership and admin

Purpose — Identifies the contract owner (the address with elevated administrative power under the Ownable pattern) and whether ownership has been renounced.

What was found — Status: *Examined*

- Ownable owner: **not exposed by the verified ABI**
- Custom issuer administrator: `0x20718fc920da7e8ee5388b472bc8d83551cc0dbe` (Safe, 2-of-3)
- Ownership renounced: **no**

Why it matters — The owner address holds privileged powers defined by the contract (e.g., minting, transfer pause, ownership transfer). Ownership status directly bounds operational risk.

The controlling interface is the custom `issuerAdmin()` path rather than Ownable. On the primary token, that path now resolves to Safe `0x20718fc920da7e8ee5388b472bc8d83551cc0dbe` instead of the deployment EOA.

What it means —

Administration has not been renounced; it has been transferred to a multisig-backed custom authority. This is a material reduction in single-key exposure for the high-impact issuer/admin surface.

2.5 Access control roles

Purpose — Inspects role-based permissions defined under the OpenZeppelin AccessControl pattern: which roles exist and which addresses hold each role. Roles typically govern minting, burning, pausing, and upgrades.

What was found — Status: *Examined*

- AccessControl detected: **yes**
- Distinct roles defined: **5** — `DEFAULT_ADMIN_ROLE`, `FEE_MANAGER_ROLE`, `ISSUER_ADMIN_ROLE`, `LIQUIDITY_LAUNCHER_ROLE`, `REWARDS_FUNDER_ROLE`
- Unique addresses across all roles: **1**
- Cross-contract authority probe: **11 of 12** related contracts expose issuer, role, operator, manager or signatory authority. Enumerable memberships were read from all verified ABIs; the Safe holds 37 issuer/admin or enumerable-role relationships across the system.

Why it matters — Role-based access control distributes contract powers across multiple addresses. Concentration of multiple sensitive roles in one address reduces the operational checks the contract was designed to provide.

The Safe now occupies 37 issuer/admin or enumerable-role relationships across the system, including all five primary-token roles. The deployment EOA occupies none of the detected current privilege slots.

What it means —

The principal handover requested after the previous scan is visible on-chain: the deployment EOA has been removed from detected privilege slots and the 2-of-3 Safe now holds the dominant authority surface. The GasVault operator, KYC operator and voucher signer remain single-signature operational paths and should be governed according to their narrower impact.

2.6 Deployer analysis

Purpose — Identifies the address that deployed the primary contract and whether the deployer retained any administrative privileges after deployment.

What was found — Status: *Examined*

- Deployer address: `0xd356fc6b589667b815f452ed27ee988cc2e65817` (EOA)
- Deployer transaction count: 76
- Deployer holds privileged roles: 0

Why it matters — The deployer often becomes the initial admin. If the deployer also holds privileged roles after deployment, the launching team retains single-point operational control.

All 13 deployments still resolve to the same EOA, but current role and issuer-admin readbacks show zero retained privileges for that address. The deployment provenance is therefore separated from current high-impact administration.

What it means —

Deployment provenance remains public, but deployment and current administration are now separated. A compromise of the original deployer key would no longer exercise any privilege detected by this scan.

2.7 Multisig wallet detection

Purpose — Probes every privileged address (deployer, owner, upgrade administrator, AccessControl role members) for the bytecode of recognised multisig wallet contracts — primarily Gnosis Safe — and reports which administrative keys are multisig-protected versus single-signer EOAs or other contracts.

What was found — Status: *Examined*

- Privileged addresses probed: 4
- Multisig wallets confirmed: 1
- Probed but not identified as multisig: 3
- Safe at `0x20718fc920da7e8ee5388b472bc8d83551cc0dbe` (Safe v1.4.1, threshold 2-of-3, no enabled modules at the pinned block)

Why it matters — A multisig wallet (e.g., a Gnosis Safe configured with an M-of-N threshold) requires multiple co-signers to authorise any administrative action; this provides operational resilience against the loss or compromise of a single key. Privileged addresses that are EOAs or non-multisig contracts can act under a single-signature path.

Safe `0x20718fc920da7e8ee5388b472bc8d83551cc0dbe` reported version 1.4.1, three owners, a threshold of two and no enabled modules at the pinned block. Three narrower direct authorities — GasVault operator, KYC operator and voucher signer — remain EOAs.

What it means —

High-impact administration now requires two of three Safe owners, and no module-based execution path was enabled at the pinned block. The remaining operational EOAs are not multisig-protected, so their permissions should stay narrowly scoped and monitored.

2.8 Holder distribution

Purpose — Measures how the token's supply is spread across addresses. Highly concentrated supply means a small number of wallets can move the market or dominate governance.

What was found — Status: *Examined*

- Holders observed: **0**
- Total supply (raw units): 0.0
- Top 1 holder: *n/a* of supply
- Top 10 holders: *n/a* of supply
- Top 100 holders: *n/a* of supply

Why it matters — High supply concentration creates market and governance risk. A single large holder can move price unilaterally; a small group can dominate any token-weighted vote.

The primary token still returned `totalSupply() = 0`, and Moralis returned no holder records. Holder concentration remains mathematically not applicable before issuance.

What it means —

No holder-concentration conclusion can be drawn while supply is zero. Repeat the holder module after minting or distribution; `N_A` is not a favourable concentration result.

2.9 DEX liquidity

Purpose — Searches major decentralized exchanges for liquidity pools that pair the token against well-known assets, and reports the reserves observed.

What was found — Status: *Examined*

- Liquidity pools observed: **none**

Why it matters — Visible DEX liquidity is one objective signal that the token can be exchanged today. Absence of liquidity does not mean a token is non-functional, but it removes one transparency anchor.

Pinned CHT/WETH and CHT/USDC factory probes returned the zero address, and Dexscreener returned no pairs. The public market state remains pre-liquidity.

What it means —

No public liquidity was visible on the probed venues. This may be expected before launch, but it is the remaining reason the scanner's subject verdict is `MIXED` rather than `HIGH`.

2.10 Fund flow

Purpose — Traces the addresses that funded the primary contract or the deployer one hop back, helping identify the operational origin of the deployment.

What was found — Status: *Examined*

- Funders observed at 1-hop: **1**
- Funder: `0xa5a5491bca93dd4c076e4906e79e7673f4a5a142` (`unknown` , 1 tx)
- **Funder-set historicity note.** The scan emits funder addresses without per-funder transaction timestamps. For contracts deployed years before the scan, this list reflects the deployer's historical

funding graph rather than current operational counterparties; for recently deployed contracts it reflects current funding origins. Interpret the list with the contract's deployment age in mind.

Why it matters — Funder identity at one hop is a transparency anchor. Funding from a well-known exchange or a public team address contextualizes deployment operations differently from funding routed through privacy mixers.

The deployment EOA history grew from 63 to 76 observed transactions, but the one-hop inbound funder set did not change. The same address supplied 0.004720039531974592 ETH in one transaction.

What it means —

The historical funding origin remains publicly traceable for one hop and unchanged from the prior scan. The additional deployer transactions do not alter the observed direct-funder set or identify its beneficial controller.

2.11 Static analysis

Purpose — Runs the configured suite of automated source-code analyzers against the verified contract source to flag known vulnerability patterns. The exact tool set is enumerated in the §2.11 detail bullets; findings of zero do not prove the code is safe — only that the patterns those tools recognize did not match.

What was found — Status: *Examined*

- Tools attempted: `slither` (0.11.5, status `completed`); `slither-check-upgradeability` (None, status `completed`); `slither-check-erc` (None, status `completed`); `mythril` (Mythril version v0.24.8, status `completed`); `aderyn` (aderyn 0.6.8, status `completed`); `semgrep` (1.163.0, status `completed`)
- Findings reported for the current primary-token run: **0**
- Prior system matrix remains applicable because all 13 runtime bytecodes are unchanged: **54 completed tool runs; 0 reported matches**

Why it matters — Automated analyzers catch a fixed set of known anti-patterns quickly. Their value in this report is binary: either they ran and produced findings (then the findings are listed), or they could not run and the report explains why.

The current primary-token run completed six configured checks with zero findings. Because all 13 runtime bytecode blobs are unchanged, the prior 54-run system matrix remains applicable and reported zero matches.

What it means —

No configured analyzer reported a match for the current primary run, and no contract bytecode changed since the prior system-wide analysis. Automated zero-finding output does not replace manual code review, adversarial testing or an independent security audit.

3. Limitations and further-diligence conditions

3.1 Known limitations (framework summary)

The framework lists every limitation already recorded by the scan, plus every module whose coverage status is anything other than `checked`. The LLM-written prose below (§3.2) elaborates on these and translates each `further_diligence_condition` into plain English.

No limitations or coverage gaps were recorded by the scan for this report.

3.2 Plain-language elaboration

All eleven report modules are complete after pinned-RPC and public-indexer readbacks. The scanner's generic explorer read path returned provider errors for several non-source calls, so the report uses separately persisted Base RPC, Etherscan v2, Moralis, Blockscout and DEX readbacks at block 49309312; the framework consumer schemas validate these corrected artifacts. The committed producer evidence schema still lags the runtime payload in seven known fields, while both current LLM-pack schemas and the framework evidence schema pass. This is a schema-versioning issue, not an on-chain finding. The result remains point-in-time: repeat role custody, Safe configuration, supply, holder, GasVault balance and liquidity checks after any authority, issuance, funding or launch change.

Appendix A: Contracts in scope

Address	Role	Source verification
0x5C090Fb0eC462f029144E644EA698175f49521c9	token (primary)	verified
0x919a7f3E1b4735b37899189cFc5AD1e910Faa79d	treasury	verified
0x90669C861083ec6a4849Cd881Cb13f8ef4E398C3	treasury	verified
0x162453987E8DF00725d88e7a15bdD0232C3919eD	distribution	verified
0xFBD1b3bff6bF6b295c147B6eA022CBAA340c10ea	distribution	verified
0x994c6fCEB994Ef90F9b5b570d30846A519FC7fa2	registry	verified
0x7Bb29a410168aca4Fc3fDF506DB63FE44bf7D073	oracle	verified
0x4f2FDaaEAa10152f43322D66cb9d481D7b7becb0	sale	verified
0x616a2468c8EBB16022d67aa2fE5AC0fc741B6EBD	referral	verified
0x40c63a2a53d5A39842928a6dDEfCf6f4a5d78381	distribution	verified
0x559e1DAe39f5dBc39B9570752A2f74a9B683Bd2A	staking	verified
0x342Bf2061ebA91f7522F4C02F459c05308282d41	registry	verified
0x3c15c4bea893fec8277f8d884250a0f0291bfa18	other	verified

Appendix B: Methodology and signal mapping

Methodology

This report is **Tier 1** automated tool output. The verdict is emitted upstream by the `token-scan-data-engine` (ASVS-style tiered checklist) and rendered verbatim by this framework — the framework does **not** compute a verdict locally. Per-module findings in §2 are reported from the same scan evidence.

Verdict construction (scanner-side)

Each scan produces two labels:

- **Subject verdict** — `HIGH` / `MIXED` / `LIMITED` / `LOW` / `INSUFFICIENT` — composed from per-axis outcomes by a boolean rule (no weighted score):
 - any `HARD_FAIL` → **LOW**
 - ≥ 2 `SOFT_FAIL` → **LIMITED**
 - 1 `SOFT_FAIL` → **MIXED**
 - all `PASS` (axes in `N_A` excluded from the denominator) → **HIGH**
 - `applicable / total < 0.5` → **INSUFFICIENT**
- **Analysis verdict** — `COMPLETE` / `PARTIAL` / `SPARSE` / `INSUFFICIENT` — reflects the share of evidence modules that ran successfully (independent of the subject verdict).

Axis outcomes

Each axis carries a **modality** and an **outcome**:

- Modality: `MUST` (dealbreaker — any `HARD_FAIL` drives Subject verdict to `LOW`) or `SHOULD` (best practice — accumulates `SOFT_FAILS`).
- Outcome: `PASS` / `SOFT_FAIL` / `HARD_FAIL` / `N_A`.

Profile-specific axis sets:

Profile	Axes
mainnet	<code>source_visibility</code> , <code>control_concentration</code> , <code>holder_concentration</code> (HHI; Hacken/antitrust convention <1500 deconcentrated, 1500–2500 moderate, $\geq$ 2500 concentrated), <code>liquidity_visibility</code> , <code>upgrade_authority</code>
testnet	<code>source_visibility</code> , <code>role_separation</code> , <code>upgrade_authority_separation</code> , <code>access_control_pattern</code> (deployment-readiness semantics)

Determinism and versioning

The verdict is a deterministic function of `(evidence, derived_signals, verdict_logic_version)`. The scanner bumps `verdict_logic_version` on every axis / threshold / composition rule change; the version applicable to this scan is recorded in Appendix C alongside the scanner version, so report vintage is fully traceable.

Reader caveat

The verdict reflects the share of the public on-chain transparency surface that the scan could assess against its codified checklist. It is **not** a merit ranking and **does not** assess whether the project is suitable for any particular use. In this report, the `MIXED` label is driven only by the absence of observed DEX liquidity; high-impact control moved from a single deployment EOA to a 2-of-3 Safe. It is not a code-quality, security or investment-merit rating.

Appendix C: Versions and timestamps

- Framework version: `1.3.0`
- Scanner version: `0.3.1`
- Evidence profile: corrected pinned RPC and public-indexer readbacks
- Evidence block: `49309312`
(`0xa17d67ea56106b9d449b9c6c3a6d5746f262921b9e15510dce271f3e36cb47d9`)
- Comparison block: `49272838`
(`0xee9a76a3c16f1e213ef5c9c54ca3eae7f5de56934d40632fa996b0f7d491fe28`)
- Runtime comparison: 13 of 13 contract bytecodes unchanged
- State comparison: 190 zero-argument view functions compared; 12 authority changes plus 3 date-index rollovers
- Safe readback: v1.4.1, 2-of-3 owners, nonce 1, no enabled modules
- Schema validation: framework evidence + both LLM-pack schemas pass; committed producer evidence schema has 7 known runtime-drift errors
- Verdict logic version: `6` (scanner-emitted)
- Scan id: `f7c26f26-5d3e-43ea-825d-e2e39a41a631`
- Scan started: `2026-07-30T10:38:14.228Z`
- Scan completed: `2026-07-30T10:38:47.530Z`
- Input source: `manual`
- Methodology references: `docs/methodology/04-smart-contract-methodology.md` , `docs/methodology/08-onchain-verification-methodology.md` , `docs/methodology/09-chain-specific-checks.md` , `docs/methodology/12-multi-contract.md`
- Schemas: `scan-evidence-v1` , `llm-pack-v1` (`docs/scan-service/schemas/`)

Appendix D: Disclaimer

This document is the output of an **automated tool** (xcactus Scan, Tier 1). It is generated without human review per request and is provided as a transparency aid for technical and on-chain due diligence.

- **Not a security audit.** A full audit (Tier 2) is a separate, human-signed deliverable. Tier 1 does not replace it.
- **Not a MiCA-compliant deliverable.** MiCA compliance is assessed only within Tier 2 audits where the scope explicitly includes it.
- **Not investment advice.** This document does not recommend any action. Readers must form their own conclusions.
- **Not a guarantee.** Coverage is bounded by public on-chain evidence and the limitations enumerated in §3.

Findings reflect the state of the queried public data sources at the timestamps in Appendix C. Subsequent on-chain or off-chain changes are out of scope.