SHERLOCK

Security Review For Figure

Collaborative Audit Prepared For: **Figure**
Lead Security Expert(s): **0xeix**
Oblivionis
Date Audited: **April 9 - April 12, 2026**

Introduction

Hastra is a DeFi protocol built by Figure Technologies, a fintech company focused on blockchain-based financial products and is operated by the Provenance Blockchain Foundation. Figure is expanding its on-chain infrastructure to Solana and Ethereum.

The Hastra protocol provides institutional-grade tokenized vaults for yield generation and staking. Users deposit a base asset (USDC) into the Yield Vault and receive wYLDS – a liquid, transferable yield-bearing token redeemable 1:1 for the underlying asset. wYLDS holders can then stake into the Staking Vault to receive PRIME tokens, whose value appreciates over time as rewards accumulate and NAV increases.

The protocol is designed with regulatory compliance in mind: vaults include account freeze/thaw controls, whitelisted withdrawals, and two-step redemption flows. Rewards are distributed via Merkle-tree-based epoch claims, ensuring efficient and verifiable on-chain distribution at scale.

Hastra is currently deployed on Solana mainnet and Ethereum testnet, with mainnet Ethereum deployment pending audit and security review. The protocol is architected for multi-chain expansion, and an active integration with the Chainlink Decentralized Oracle Network is underway to publish verified NAV rates on-chain – enabling the staking vault share price to reflect real-world asset values trustlessly.

Scope

Repository: provenance-io/hastra-eth-vault

Audited Commit: 2ef9fe9b8bd96c51d0a556df1f31f890e53c33c9

Final Commit: 52655033264d37225929cf0059fba478fed69795

Files:

- chainlink-hub/contracts/FeedVerifier.sol
- contracts/chainlink/HastraNavEngine.sol
- contracts/StakingVault.sol
- contracts/YieldVault.sol

Final Commit Hash

52655033264d37225929cf0059fba478fed69795
Each issue has an assigned severity:

- High issues are directly exploitable security vulnerabilities that need to be fixed.
- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.

- Low/Info issues are non-exploitable, informational findings that do not pose a security risk or impact the system's integrity. These issues are typically cosmetic or related to compliance requirements, and are not considered a priority for remediation.

Executive Summary

Distribution notice. This document is a redacted version of the full technical reports prepared for Figure Technologies. Proof-of-concept code, reproduction steps, exploit mechanics, environment-specific identifiers, and source-level references have been removed. Full technical details, including remediation diffs and reproduction artifacts, are available from Sherlock under NDA upon request.

Across two collaborative engagements in March and April 2026, Sherlock audited the Hastra protocol – Figure Technologies' institutional-grade tokenized vault system (USDC → wYLDS yield vault → PRIME staking vault) – covering both its Ethereum (Solidity) and Solana (Anchor/Rust) implementations. Hastra targets multi-chain deployment with a Chainlink-integrated NAV pricing layer, regulatory-compliance controls (account freeze/thaw, whitelisted withdrawals, two-step redemption), and Merkle-based reward epoch distribution.

The two engagements were sequenced to cover, first, the core vault implementation across both chains, and second, the new Chainlink Data Streams NAV integration on the Ethereum side along with the corresponding Solana price-verification path. Together they examined the surfaces where economic correctness, oracle trust, and operator privilege intersect.

Overall outcome: No Critical or High-severity findings were identified across either engagement. All Medium-severity findings were either resolved by the team or formally acknowledged with a documented rationale for accepting the residual risk. All Low/Informational findings were resolved. The protocol's overall security posture at the close of the engagements is assessed as **strong**, contingent on the operational disciplines noted in §4.

1. Severity Summary (Combined)

Severity	Engagement 1	Engagement 2	Total
Critical	0	0	0
High	0	0	0
Medium	2	2	4
Low / Info	7	4	11
Total	**9**	**6**	**15**

Remediation status at report date: 0 Critical/High open. 2 Mediums resolved, 2 Mediums acknowledged with documented acceptance. 11 Low/Info resolved.

2. Scope and Methodology (High-Level)

2.1 In-Scope Components

The combined scope across both engagements covered:

- **Ethereum (Solidity):** the yield vault contract, the staking vault contract, the Chainlink NAV engine, and the Chainlink feed verifier.
- **Solana (Anchor / Rust):** the vault-mint program and the vault-stake program, including their account structures, guards, processors, and on-chain state.
- **Cross-chain:** the Chainlink Data Streams price-verification path on both chains, and the operational equivalence between the two implementations.

Specific commit hashes, file paths, and repository references are documented in the full report available under NDA.

2.2 Methodology

The engagements followed Sherlock's standard manual review methodology, supplemented where appropriate by targeted property-level reasoning. Review activities included:

- Threat modeling of the vault lifecycle (deposit, stake, reward distribution, unbond, redeem) and of the Chainlink price ingestion path.
- Manual line-by-line review of all in-scope source files.
- Cross-chain semantic comparison between the EVM and Solana implementations of equivalent primitives (oracle staleness, vault accounting, unbonding flow).
- Review of operator-privileged paths against a fail-closed standard.
- Review of event emission and off-chain observability against on-chain state mutations.
- Verification of remediation PRs after initial findings were reported.

No automated fuzzing harnesses or formal verification artifacts were within scope of these engagements.

3. High-Level Themes

Three themes recurred across the two engagements and are presented here at the level appropriate for external distribution. Underlying technical specifics are reserved for the NDA-protected report.

3.1 EVM - Solana Semantic Drift

The dominant risk surface across both engagements was divergence between the Ethereum and Solana implementations of equivalent protocol primitives. In several cases, a primitive was implemented correctly on one chain and incorrectly on the other – including in the oracle-staleness anchoring logic and in the unbonding flow. The Ethereum implementation was generally the canonical reference, with the Solana side requiring corrections to align.

Business impact. Multi-chain protocols accrue risk at a rate that scales with the number of independent implementations of the same logical invariant. Without a sustained discipline of cross-chain parity review, divergences of this kind tend to compound over time.

High-level remediation guidance. Treat each EVM/Solana primitive pair as a single specification with two implementations, and verify parity for every change to either side. Where divergence is intentional (e.g., for chain-specific reasons), document it explicitly in code and in operator runbooks.

3.2 Reward Distribution and Share-Price Discontinuity

The staking vault's reward distribution mechanism produces a discrete, single-block change in share price on both chains – surfacing as a sandwich/MEV vector on the Ethereum side and as a virtual-shares dilution effect on the Solana side. Both findings were formally acknowledged by Figure as accepted residual risk under the current operational model.

Business impact. The accepted vectors are economic rather than safety-critical: they affect the distribution of rewards among stakers under specific conditions, but do not threaten user principal or protocol solvency. Their materiality scales with reward size, vault TVL, and the maturity of MEV infrastructure on the relevant chain.

High-level remediation guidance. A future iteration of the reward distribution mechanism that smooths reward accrual over a configurable window would eliminate both vectors structurally. This is recorded as a forward-looking design recommendation rather than a remediation requirement.

3.3 Operator-Privileged Configuration Paths

Several findings involved operator-privileged configuration paths that defer fail-safety to off-chain operational discipline rather than enforcing it on-chain. The canonical case is a configuration update path that does not invalidate now-meaningless prior state when its semantically-coupled inputs change.

Business impact. Operationally-disciplined invocation (pause → reconfigure → re-verify → unpause) fully mitigates these issues in practice. The residual risk is concentrated in the time window between configuration change and the next verification step, and in the reliability of the operational runbook.

High-level remediation guidance. On-chain code should fail closed by default when a privileged configuration change renders prior state semantically invalid. Operational discipline should remain in place as a complement, not as the sole control. Where the issue identified during these engagements followed this pattern, remediation has been applied on the Ethereum side and remains an acknowledged forward-looking item on the Solana side.

4. Operational Recommendations

The following operational recommendations carry forward from the engagements and apply to ongoing protocol operation:

1. **Cross-chain parity reviews.** Any change to a protocol primitive on one chain should trigger a parity review against the corresponding primitive on the other chain before deployment.
2. **Privileged-action runbooks.** Operator-privileged actions affecting oracle configuration, reward distribution, or vault accounting should follow documented pause-and-verify runbooks, with on-chain pause as a hard prerequisite.
3. **Event-driven monitoring.** Off-chain monitoring should consume the protocol's emitted events as the source of truth for state transitions. Where events were corrected during the engagement, the monitoring layer should be re-validated against the corrected schemas.
4. **Forward-looking design review of reward distribution.** The accepted reward-distribution findings are best addressed structurally in a subsequent design iteration rather than incrementally.

5. Engagement Appendices

The two appendices below summarize each engagement at a high level. Detailed technical findings are reserved for the NDA-protected reports.

Appendix A — Engagement 1: Core Vault Implementation (March 4–13, 2026)

- **Focus.** The core vault implementation on both Ethereum and Solana, including the yield and staking vaults on the Ethereum side and the full vault-mint and vault-stake programs on the Solana side.
- **Outcome.** 0 Critical, 0 High, 2 Medium, 7 Low/Info.
- **Themes.** The two Mediums concerned reward distribution mechanics and the unbonding flow design respectively, both formally acknowledged by Figure. The Lows clustered around event/state observability accuracy, validation correctness on privileged paths, and an EVM permit-handling robustness improvement.

Appendix B — Engagement 2: Chainlink NAV Integration (April 9–12, 2026)

- **Focus.** The new Chainlink Data Streams NAV integration on the Ethereum side, the corresponding Solana price-verification path, and updates to the staking and yield vaults required by the integration.

- **Outcome.** 0 Critical, 0 High, 2 Medium, 4 Low/Info.
- **Themes.** Both Mediums were oracle-correctness issues at the configuration boundary of the feed verifier and the NAV engine, both resolved. The Lows surfaced the EVM/Solana semantic drift theme (§3.1) directly in the oracle layer, alongside specification/implementation alignment items.

Attestation of Security Review

This following one-pager attests that **Sherlock** performed independent security reviews of the Hastra protocol on behalf of Figure Technologies across two engagements in March and April 2026. The reviews were led by Sherlock's security experts **0xeix** and **Oblivionis**.

Scope (High-Level)

The combined scope of the two engagements covered:

- The Hastra **yield vault** and **staking vault** smart contracts on Ethereum (Solidity).
- The Hastra **vault-mint** and **vault-stake** programs on Solana (Anchor / Rust).
- The **Chainlink Data Streams NAV integration**, including the feed verifier and NAV engine on the Ethereum side and the corresponding price-verification path on the Solana side.

Specific commit hashes and file-level scope are documented in the full technical reports.

Methodology (High-Level)

Reviews were conducted through manual line-by-line code review, threat modeling of the vault lifecycle and oracle ingestion path, cross-chain semantic comparison between the Ethereum and Solana implementations of equivalent primitives, and review of operator-privileged paths against a fail-closed standard. Remediation pull requests were verified against the originally reported findings.

Dates of Testing

Engagement	Focus	Dates
1	Core vault implementation (EVM + SVM)	March 4–13, 2026
2	Chainlink NAV integration	April 9–12, 2026

Severity Summary

Severity	Engagement 1	Engagement 2	Total
Critical	0	0	0
High	0	0	0
Medium	2	2	4
Low / Info	7	4	11

Remediation Status

As of the date of this letter, and based on Figure's reported remediation status:

- **No Critical or High-severity findings remain open.** No findings of these severities were identified during either engagement.
- **All Medium-severity findings have been either resolved by Figure or formally acknowledged** with a documented rationale for accepting the residual risk.
- **All Low-severity and Informational findings have been resolved.**

Disclaimers

Sherlock does not provide guarantees nor warranties relating to the security of the project.

Usage of all smart contract software is at the respective users' sole risk and is the users' responsibility.