Sentora® HASTRA

PROTOCOL REVIEW COLLATERAL ASSESSMENT

Hastra PRIME

Date	2026-05-06 (updated 2026-05-27)
Author	Sentora Research
Scope	Ethereum (live since 2026-04-17) primary; Solana (live, prior review baseline) and Provenance (host chain) secondary.

1. Executive Summary

PRIME is the staked-wYLDS yield-bearing token issued by Hastra, a DeFi protocol built by Figure Technologies and operated by the Provenance Blockchain Foundation. wYLDS wraps Provenance YLDS, an SEC-registered face-amount certificate issued by Figure Certificate Company. Yield originates from a single source, the Democratized Prime credit pool on Provenance, and is propagated to PRIME holders on both Solana and Ethereum via a unified NAV. PRIME runs as a parallel ERC-4626 vault on Ethereum (0x19ebb352...F7F6) since 2026-04-17, alongside the original Solana SPL deployment.

The 1:1 backing invariant rests on Hastra's operational custody of Provenance YLDS balances and a unified NAV. There is no atomic on-chain link between the Provenance `uylds.fcc` marker and the Ethereum or Solana wYLDS supplies. NAV is computed off-chain by Hastra, signed by the Chainlink Data Streams DON, and posted on-chain hourly. Each chain verifies the signed report independently.

Safe migration is complete on all four production Ethereum contracts. Safe `0x8D358B...6309` (Safe v1.4.1, 4-of-7 threshold, 7 owners) holds `DEFAULT_ADMIN_ROLE` and `UPGRADER_ROLE` on YieldVault, StakingVault, FeedVerifier, plus `owner()` on HastraNavEngine. The deployer EOA has been revoked. The operational EOA `0xA8C3CF61...0faCd` retains real-time roles (FeedVerifier UPDATER and equivalents) by Hastra design.

Sherlock has audited the live mainnet code across two collaborative engagements (March and April 2026), producing 0 Critical, 0 High, 4 Medium (2 resolved, 2 acknowledged with documented residual risk acceptance), 11 Low/Info (resolved). Final commit `52655033` matches deployed mainnet bytecode.

Key facts at a glance:

- **Issuance.** Singular yield source: Democratized Prime credit pool on Provenance. wYLDS supplies on Ethereum and Solana are independent mints under operational 1:1 custody.
- **Audit.** Sherlock collaborative audit completed 2026-04-27. 0 Critical, 0 High, 4 Medium (2 resolved, 2 acknowledged), 11 Low/Info (resolved).
- **Governance.** 4-of-7 Safe holds upgrade and admin roles on all four Ethereum contracts. No timelock between Safe execution and proxy upgrade. Solana Squads 4-of-7 with `time_lock = 0`.
- **Mint caps.** Layered: 75 BPS, per-call 1M wYLDS, 1-hour cooldown, 10M wYLDS lifetime. Caps constrain reward minting but not arbitrary `upgradeToAndCall`.
- **Oracle.** Chainlink Data Streams Schema v7, hourly cadence. Deposits and redemptions revert on stale or missing oracle. No last-good-price fallback.
- **Liquidation routing.** PRIME-to-wYLDS is permissionless. wYLDS-to-USDC requires a rewards admin to call `completeRedeem`. Structural admin gate independent of liquidity levels.
- **Critical risks.** No timelock on upgrades; oracle-revert lock on deposits and redemptions; admin-gated USDC exit at the YieldVault chokepoint.

2. Key Metrics

Metric	Value	Date
PRIME totalSupply (Ethereum)	74,381,819.33 PRIME (6 decimals)	2026-05-27
wYLDS totalSupply (Ethereum)	77,581,615.31 wYLDS (6 decimals)	2026-05-27
PRIME totalSupply (Solana)	284,846,062.43 PRIME (6 decimals)	2026-05-27
wYLDS totalSupply (Solana)	300,284,649.67 wYLDS (6 decimals)	2026-05-27
Ethereum PRIME holders	48	2026-05-27
Ethereum wYLDS holders	26	2026-05-27
YieldVault USDC balance	121,153.58 USDC	2026-05-27
Safe USDC balance	0 USDC	2026-05-27
Live PRIME / wYLDS exchange rate (Solana)	0.968541 PRIME per wYLDS	2026-04-23
HastraNavEngine `maxDifferencePercent`	100 percent (baseline)	2026-04-23 (read-contract not retrievable 2026-05-05; presumed unchanged)
HastraNavEngine rate band	1.0 to 3.0 (baseline)	2026-04-23 (presumed unchanged)
Oracle update cadence (Eth)	hourly via FeedVerifier `verifyReport`	2026-05-05
NavEngine update cadence (Eth)	hourly via `updateRate`	2026-05-05
DEX liquidity on Ethereum	Uniswap V3 PRIME/USDC 0.01% pool, ~$9.0M reserve (~$130k 24h vol)	2026-05-27

Metric	Value	Date
Lending market integrations (Eth)	None	2026-05-05
Multisig threshold (Eth)	**Safe** `0x8D358B8aE881F8ea92C3d07783aBCA21727C6309` **(Safe v1.4.1, 4-of-7, 7 owners, nonce 8)** holds DEFAULT_ADMIN and UPGRADER on YieldVault, StakingVault, FeedVerifier; HastraNavEngine owner() = Safe. Deployer EOA revoked. No timelock.	2026-05-06
Multisig threshold (Solana)	Squads v4, 4 of 7, time_lock 0	2026-04-23
Audit status	Sherlock collaborative audit, two engagements (2026-03-04 to 03-13 core vaults; 2026-04-09 to 04-12 Chainlink NAV integration). 0 Critical, 0 High, 4 Medium (2 resolved, 2 acknowledged), 11 Low/Info (resolved). Final commit `52655033` matches deployed mainnet.	2026-04-27
Bug bounty	None disclosed (no Immunefi listing)	2026-05-05
Cross-chain token transport	None implemented; CCIP token-pool bridging not in code	2026-05-05

3. Top Issues, Ranked

The 10 highest-priority items at 2026-05-06. Full list in §7.2. Findings concerning current liquidity, supply, and balance-sheet metrics are not severity-tagged at launch state; they appear in §8 and §9 as informational. The prior pass's F-1 (single-EOA admin) and F-5 (Safe-not-yet-deployed) are removed: the 4-of-7 Safe `0x8D358B...6309` now holds DEFAULT_ADMIN and UPGRADER on all four Ethereum contracts, and the deployer EOA has been revoked.

#	Issue	Mechanism	Severity
1	UUPS upgrade with no timelock on any of the four Ethereum contracts	`_authorizeUpgrade` gated on `UPGRADER_ROLE` only. No OpenZeppelin TimelockController in any admin chain. A 4-of-7 Safe quorum upgrades any contract in one block. Hastra response Q4 explicitly states no timelock will be implemented; layered mint caps cited as compensating control, but those caps do not constrain `upgradeToAndCall`.	Critical
2	Oracle revert locks deposits and redemptions on both chains	`StakingVault._convertToShares` calls `getVerifiedNav()` unconditionally on Ethereum; Solana `vault-stake.deposit` requires fresh `verify_price`. Stale or reverting oracle blocks all user mints and redeems with no last-good-price fallback.	Critical
3	Liquidation routing for an Ethereum lending market depends on admin-gated `completeRedeem`	The PRIME → wYLDS leg is permissionless. The wYLDS → USDC leg is `REWARDS_ADMIN_ROLE` only. Hastra has stated intent to move REWARDS_ADMIN on YieldVault to the Safe (monthly multisig approval). The chokepoint persists structurally.	High
4	Permissive HastraNavEngine defaults	`maxDifferencePercent = 100 percent`, rate band 1.0 to 3.0 at deployment. TVL can move 100 percent between updates without revert. Read-contract values not retrievable in this refresh; presumed unchanged from baseline.	High
5	wYLDS to USDC exit is admin-gated	`completeRedeem` is `REWARDS_ADMIN_ROLE` only on both chains. Users cannot force exit to USDC. Sherlock §3.3 acknowledges this as an operator-privileged path that defers fail-safety to operational discipline; remediation applied on Ethereum and acknowledged forward-looking on Solana.	High

#	Issue	Mechanism	Severity
6	Off-chain custodial backing without atomic link	wYLDS supply on Ethereum and Solana derives from Hastra custody of Provenance `uylds.fcc` marker balances. The unified NAV is the operational link, signed by Chainlink Data Streams; there is no atomic on-chain proof. No IBC, no Wormhole, no LayerZero, no CCIP token transport.	High
7	Pause power exercisable during a liquidation event	StakingVault and YieldVault are pausable by `PAUSER_ROLE` (Safe + operational EOA both hold). Exercised 2026-05-04 for ~2 hours, consistent with Sherlock §4 pause-reconfigure runbook. A pause during a Morpho liquidation event halts the redemption path.	High
8	Safe owners and custody mix not publicly disclosed	The 4-of-7 Safe at `0x8D358B...6309` (Safe v1.4.1) is verified on-chain with seven owner addresses listed in §6.2. Identity-to-address mapping, custody mix (HSM, institutional MPC, software), and geographic distribution are not publicly known. A 4-of-7 quorum compromise upgrades any contract in one block (no timelock).	High
9	Sherlock-acknowledged residual risk: reward distribution share-price discontinuity	Discrete single-block share-price change on `distributeRewards` is a sandwich/MEV vector on EVM and a virtual-shares dilution effect on Solana. Both formally acknowledged by Figure as accepted residual risk; not user-principal-threatening. Materiality scales with reward size and TVL.	Medium
10	Sherlock-acknowledged forward-looking item: Solana operator-privileged config does not fail closed	Per Sherlock §3.3, an operator-privileged configuration update path on the Solana side does not invalidate now-meaningless prior state when semantically-coupled inputs change. Remediation applied on Ethereum side; Solana side acknowledged forward-looking.	Medium

4. Product and Issuance Stack

PRIME is Hastra's staked-wYLDS yield-bearing token. wYLDS is the wrapped form of Provenance YLDS, an SEC-registered face-amount certificate issued by Figure Certificate Company. Yield accrues from Figure's HELOC / Democratized Prime credit pools on Provenance, flowing into wYLDS as `mintRewards` and into PRIME as a rising NAV.

Issuer / legal entity: Hastra (operating company specifics, jurisdiction, and registrations). YLDS issuer: Figure Certificate Company. Transfer agent: Figure Equity Solutions. Hastra and Figure share an equity-backing relationship reported in tradpress at approximately $19B.

Token flow diagram:

```
Figure Loans / Figure Certificate Company (Provenance)
   │
   ▼ x/marker module (native)
YLDS on Provenance, denom uylds.fcc, SupplyFixed
   │
   ▼ off-chain custodial link (no on-chain bridge)
   │
   ├─ Solana stack
   │ vault-mint 9WUyNREiPDMgwMh5Gt81Fd3JpiCKxpjZ5Dpq9Bo1RhMV
   │ USDC SPL → wYLDS (8fr7WGTV...kdih) 1:1
   │ vault-stake 97V7JsExNC6yFWu5KjK1FLfVkNVvtMpAFL5QkLWKEGxY
   │ wYLDS → PRIME (3b8X44fL...3Uu7) at Chainlink rate
   │
   └─ Ethereum stack (live 2026-04-17)
       YieldVault 0x6aD038cA6C04e885630851278ca0a856Ad9a66Cc
          USDC → wYLDS (1:1 hardcoded)
       StakingVault 0x19ebb35279A16207Ec4ba82799CC64715065F7F6
          wYLDS → PRIME at Chainlink rate
```

The two chains operate as independent parallel issuance stacks. They share no on-chain state. Total PRIME circulating equals Solana supply plus Ethereum supply, with reconciliation only possible off-chain.

Multi-chain deployment:

Network	PRIME totalSupply	wYLDS totalSupply	Holders (PRIME)
Solana mainnet	335,665,398 PRIME	359,251,799 wYLDS	many (live integrations on Kamino)
Ethereum mainnet	74,381,819 PRIME	77,581,615 wYLDS	48

5. Protocol Mechanics

5.1 Contract Set and Programs

Contract	Proxy	Implementation	Pattern
StakingVault (Eth, PRIME)	0x19ebb35279A16207Ec4ba82799CC64715065F7F6	0x90fd843c68db38e2de0618AcBB39341CbA5A5abD	UUPS / ERC1967
YieldVault (Eth, wYLDS)	0x6aD038cA6C04e885630851278ca0a856Ad9a66Cc	0xDA962f7a0308e9D4F2F60c5Aab94f173C26d1A1D	UUPS / ERC1967
HastraNavEngine (Eth)	0xfEd839B6BA09c1aBf4C768abA0ECA50746E4eca9	0x1376de100324d42337F1a2C08351d7242f30C3A7	UUPS / ERC1967
FeedVerifier (Eth)	0xdF4ab20fA7752Be52E41e42F1FD667f37964d6a3	0xbC6023cb49f8e8ca6cef563d5fd97ba4c6a5d937	UUPS
Vault-mint (Solana)	9WUyNREiPDMgwMh5Gt81Fd3JpiCKxpjZ5Dpq9Bo1RhMV	n/a (BPF)	BPF Upgradeable
Vault-stake (Solana)	97V7JsExNC6yFWu5KjK1FLfVkNVvtMpAFL5QkLWKEGxY	n/a (BPF)	BPF Upgradeable
vault-stake-auto (Solana)	Dz8K7J1UrCPv8ywqxe1FKkuHa8Vm8MQtP68ohf7wPjHB	undeployed	n/a

Framework versions, Ethereum side: Solidity 0.8.27, Hardhat plus Foundry, viaIR, 200 optimizer runs, OpenZeppelin Upgradeable v5.4. Both vaults extend `Initializable + ERC4626Upgradeable + ERC20PermitUpgradeable + AccessControlUpgradeable + PausableUpgradeable +`

`ReentrancyGuardUpgradeable + UUPSUpgradeable`. Storage gaps: StakingVault `uint256[41]`, YieldVault `uint256[42]`. Constructor calls `_disableInitializers()`. StakingVault uses internal `_totalManagedAssets` for `totalAssets()`, an inflation-attack guard. YieldVault hardcodes `convertToShares` and `convertToAssets` to 1:1.

Solana side: Anchor 0.31.1.

5.2 Mint and Issuance Path

StakingVault `deposit(assets, receiver)` (Ethereum):

- Pull wYLDS from caller.
- Read NAV via `getVerifiedNav()` which calls `FeedVerifier.priceOf(feedId)`.
- Mint PRIME equal to `assets * 1e18 / nav`.
- Modifiers: `whenNotPaused`, `nonReentrant`. Reverts on stale, zero, or missing oracle.

YieldVault `deposit(assets, receiver)` (Ethereum): USDC to wYLDS at 1:1. `whenNotPaused`, `nonReentrant`.

vault-stake `deposit` (Solana): wYLDS to PRIME at Chainlink rate, computed `shares_to_mint = (wYLDS_amount * price_scale) / price` with `checked_mul`/`checked_div`.

Role gating on mint: None at the user-call level. Permissionless deposits subject to YieldVault whitelist (USDC entry) and StakingVault freeze list.

Caps and cooldowns: No mint cap. No per-tx cap. Reward distribution to the vault has caps (BPS, period, lifetime), but those govern NAV uplift, not user deposit volume.

5.3 Redemption Path

PRIME to wYLDS (instant, both chains):

- StakingVault `redeem(shares, receiver, owner)`: burn PRIME, return wYLDS at NAV. No queue, no admin gating. Reverts if oracle fails.
- vault-stake `redeem` (Solana): same semantics.

wYLDS to USDC (admin-gated, both chains):

- YieldVault standard `withdraw` and `redeem`: disabled, revert with instruction to use `requestRedeem`/`completeRedeem`.
- `requestRedeem(shares)`: user-initiated, transfers shares to vault, stores `PendingRedemption`.
- `completeRedeem(user)`: `REWARDS_ADMIN_ROLE` only. Burns shares, transfers USDC to user.
- `cancelRedeem()`: user-initiated cancel before completion.

Settlement timing observed: Test-deposit phase only. No production-volume redemptions on Ethereum at 2026-05-05.

Critical implication: PRIME holders can always exit to wYLDS instantly (modulo oracle health). Conversion of wYLDS to USDC requires the rewards admin to execute `completeRedeem`, off-chain

funded. There is no pull-based USDC exit. This admin gate is the same chokepoint that constrains liquidation routing for any Ethereum lending market that lists PRIME.

5.4 Yield and Reward Mechanics

Source: Figure HELOC / Democratized Prime credit pools on Provenance, accruing into the underlying YLDS marker.

Distribution path (Ethereum): `StakingVault.distributeRewards(amount)` is `REWARDS_ADMIN_ROLE`. It calls `YieldVault.mintRewards(address(this), amount)`, which mints fresh wYLDS into the StakingVault share pool, raising NAV for all PRIME holders. Caps:

Parameter	Default
Cooldown	3,540 seconds (59 minutes)
Per-period cap	1,000,000 wYLDS
Lifetime cap	10,000,000 wYLDS
BPS cap	75 bps (0.75 percent of TVL)

These match the Solana side's defaults. All four are mutable by upgrade authority.

Distribution path (Solana): vault-stake `publish_rewards` CPIs into vault-mint `external_program_mint`, identified via PDA `[b"external_mint_authority"]`. Same effective cap structure.

NAV impact: Rewards mint new wYLDS into the StakingVault and raise PRIME's exchange rate. PRIME holders do not need to claim. Merkle-claim flow exists for separate reward epochs (`createRewardsEpoch`, `claimRewards`).

5.5 Oracle and Pricing Architecture

Feed: Chainlink Data Streams Schema v7. Feed ID `0x000700f43b35146a1cb16373ac6225ad597535e928e6dc4d179c3b4225f2b6d3` (Ethereum and Solana share the same feed ID).

Posting cadence (Ethereum, 2026-05-05): Hourly. FeedVerifier keeper EOA `0xF0a5baEB...ae6cd73cd` calls `verifyReport` approximately once per hour. NavEngine updater EOA `0xD5a28795...21e9FB4c8` calls `updateRate` approximately once per hour. Total `verifyReport` transactions on FeedVerifier since deployment: 761 over ~18 days, consistent with hourly cadence.

Posting cadence (Solana): verify_price callable by rewards administrators only.

Staleness: FeedVerifier default 3,600 seconds, per-feed override available. Solana side measures staleness against the report's `observations_timestamp`.

Deviation bounds (Ethereum, baseline): HastraNavEngine `maxDifferencePercent = 100 percent`, `minRate = 1.0e18`, `maxRate = 3.0e18`. Read-contract values not retrievable in this refresh; presumed unchanged from baseline.

Deviation bounds (Solana): None enforced in code. `verify_price` accepts any `price > 0` plus a fresh `observations_timestamp`.

Failure mode: Revert on stale, zero, or missing report. No last-good-price fallback. No degraded-mode pause that allows withdrawals. The pauser role can stop the vault entirely but cannot enable a sub-NAV exit.

Keeper architecture: Keeper is an EOA on Ethereum. Custody disclosure pending.

5.6 Cross-chain and Bridge Architecture

Bridge: None. No CCIP token-pool, no LayerZero, no Wormhole, no Axelar, no IBC. PRIME and wYLDS are independently issued on Solana and Ethereum.

Cross-chain supply control: Independent. There is no on-chain cross-chain supply ceiling, and an admin error or compromise on one chain is not detectable by the other. Cross-chain reconciliation is off-chain.

5.7 NAV and Backing Mechanism

On-chain vs off-chain NAV: The NAV is computed by Hastra's NAV Engine off-chain, signed by the Chainlink Data Streams DON, then submitted on-chain hourly. HastraNavEngine on Ethereum stores the latest verified rate and applies a TVL-change tolerance check (`maxDifferencePercent`) and a hard min/max band. Solana stores the price in `StakePriceConfig` with no min/max band.

Posting cadence: Hourly, verified above.

Deviation bounds: Permissive. 100 percent TVL tolerance and 1.0 to 3.0 rate band on Ethereum constitute very loose sanity checks.

Proof-of-reserves: None public. The Provenance `uylds.fcc` marker supply, the Solana wYLDS supply, and the Ethereum wYLDS supply have no on-chain attestation cross-checking the relationship. The 1:1 backing claim rests on Hastra's operational custody of Provenance YLDS balances.

6. Access Controls and Governance

6.1 Privileged Roles Inventory

Safe migration is complete as of 2026-05-06. The deployer EOA has been revoked from DEFAULT_ADMIN and UPGRADER on all four Ethereum contracts. The 4-of-7 Safe `0x8D358B8aE881F8ea92C3d07783aBCA21727C6309` (Safe v1.4.1) holds DEFAULT_ADMIN and UPGRADER on YieldVault, StakingVault, FeedVerifier, plus `owner()` on HastraNavEngine. Operational EOAs retain real-time roles by Hastra design (Q2 in the Hastra response): YieldVault REWARDS_ADMIN and WITHDRAWAL_ADMIN, StakingVault REWARDS_ADMIN and NAV_ORACLE_UPDATER,

FeedVerifier UPDATER, HastraNavEngine `updater()`. PAUSER and FREEZE_ADMIN are dual-held by the Safe and an operational EOA. WHITELIST_ADMIN on YieldVault is dual-held.

Ethereum, on-chain-verified at 2026-05-06:

Contract	Role	Holder	Signer Type
YieldVault	DEFAULT_ADMIN_ROLE	Safe 0x8D358B...6309	Safe v1.4.1 (4-of-7)
YieldVault	UPGRADER_ROLE	Safe 0x8D358B...6309	Safe
YieldVault	PAUSER_ROLE, FREEZE_ADMIN_ROLE, WHITELIST_ADMIN_ROLE	Safe + operational EOA 0xA8C3CF61...0faCd	Safe + EOA
YieldVault	REWARDS_ADMIN_ROLE, WITHDRAWAL_ADMIN_ROLE	Operational EOA only by design (Hastra plans to move YieldVault REWARDS_ADMIN to Safe for monthly distribution)	EOA
StakingVault	DEFAULT_ADMIN_ROLE	Safe 0x8D358B...6309	Safe
StakingVault	UPGRADER_ROLE	Safe 0x8D358B...6309	Safe
StakingVault	PAUSER_ROLE, FREEZE_ADMIN_ROLE	Safe + operational EOA	Safe + EOA
StakingVault	REWARDS_ADMIN_ROLE, NAV_ORACLE_UPDATER_ROLE	Operational EOA only by design (real-time operations)	EOA
HastraNavEngine	owner() (Ownable2Step)	Safe 0x8D358B...6309	Safe
HastraNavEngine	updater()	EOA (operational hot keeper, hourly NAV writer)	EOA
FeedVerifier	DEFAULT_ADMIN_ROLE	Safe 0x8D358B...6309	Safe
FeedVerifier	PAUSER_ROLE, UPGRADER_ROLE	Safe 0x8D358B...6309 per Hastra response	Safe

Contract	Role	Holder	Signer Type
FeedVerifier	UPDATER_ROLE	Operational EOA 0xA8C3CF61...0faCd (per Hastra response) plus hourly keeper 0xF0a5baEB...ae6cd73cd	EOA

6.2 Multisig Configuration

Ethereum Safe `0x8D358B8aE881F8ea92C3d07783aBCA21727C6309` (verified on-chain 2026-05-06):

Field	Value
Address	0x8D358B8aE881F8ea92C3d07783aBCA21727C6309
Pattern	Safe Proxy (master copy 0xa619486e..., EIP-1167-style minimal proxy with Safe-1.4.1 master)
Implementation version	**1.4.1**
Threshold	**4**
Owners (count: 7)	0xb257106ffd8290d3f5fdeaed9f603ef2d0630c26, 0x13b29ad44c9f859764378e2325b2aa9725e71fe3, 0x4b8d18095cb48125d0d9106c8c1162bceb8558c7, 0x3f7aa6e9bd048b97c9b0914ae317a1814b9381b2, 0xc4d5491382138e9a0bcd37c1a8ebd46c753253f1, 0xcd1ef81ccb5aab7d96c083f48ff859385eb65a36, 0x840560f38e5cdca96bf4042e6ee45407a303eea1
Lifetime tx count (nonce)	8
Timelock	None on the Safe-to-proxy path

The Safe is structurally clean: 4-of-7, well above the bare-majority bar; mainstream Safe implementation; non-trivial signer count. The unresolved governance gaps are (i) the absence of any timelock between Safe execution and proxy upgrade, and (ii) the lack of public attribution for the seven signers and their custody mix. Hastra response Q4 explicitly defends the absence of a timelock.

Solana Squads v4 `FCdUkkK7YcsyW24H1Sjba1jgK53nuMMqqjqaHYAoSgJm`:

- Threshold: 4 of 7.
- Time lock: 0 seconds.
- Config authority: `11111111111111111111111111111111` (None, autonomous).
- Lifetime tx count: 7.
- Members: `6DwG5XKa67Q8L9C9mrv67XUwCB7hSdBvcaF4zGyVNnn`, `37TZMqhCbgiCsdR3SrG2kxKgHTSkrKngQisDQTon2txH`, `3zfdJ8eA4nUZvADhgeh9PtxiALqxwJvrqwJHfhbscQcX`, `5qAfz14RSGRipSUvzrzzsGBRmj1LxgmpVhBDNTMmF7Kx`, `9BXLcZUDUsdQqjJcDibkGGM3hzZH4vgBsdZTZPNzYhyd`, `9jJKMdGCXbP3TcPPzynwh9s4TZxbFyJnCpjWfvfcbALk`, `BGdxjVXGvjdA47xG3ojeHaFkBjARdtaMsHwABRVt2KRm`.
- Permissions: all 7 hold Initiate plus Vote plus Execute.

6.3 Upgrade Paths

Contract	Pattern	Authorized Caller	Timelock
StakingVault	UUPS	UPGRADER_ROLE held by Safe 0x8D358B...6309	None
YieldVault	UUPS	UPGRADER_ROLE held by Safe 0x8D358B...6309	None
HastraNavEngine	UUPS	owner() (Ownable2Step) = Safe 0x8D358B...6309	None
FeedVerifier	UUPS	DEFAULT_ADMIN_ROLE held by Safe 0x8D358B...6309	None
vault-mint	BPF Upgradeable	Squads 4-of-7 vault PDA	0 seconds
vault-stake	BPF Upgradeable	Squads 4-of-7 vault PDA	0 seconds

The absence of any timelock on any contract is the architectural fact that keeps governance findings Critical. A 4-of-7 Safe quorum on Ethereum, or a 4-of-7 Squads quorum on Solana, executes implementation upgrades in the same block or slot. There is no detection or exit window. Hastra defends the absence with layered mint caps (BPS, per-call, cooldown, lifetime), but those caps are mutable by the same upgrade authority and do not constrain arbitrary implementation logic.

6.4 Emergency Levers

Per Hastra response (2026-05), `PAUSER_ROLE` and `FREEZE_ADMIN_ROLE` are dual-held by the Safe and the operational EOA hot wallet on YieldVault and StakingVault, so pause and freeze can be triggered by either. WHITELIST_ADMIN on YieldVault is dual-held. Real-time operational roles (REWARDS_ADMIN, NAV_ORACLE_UPDATER, FeedVerifier UPDATER, NavEngine `updater`, YieldVault WITHDRAWAL_ADMIN) sit on EOAs only by Hastra design.

Lever	Function	Who Can Trigger	Threshold	Used Historically
Global pause (StakingVault)	pause()	PAUSER_ROLE: Safe + operational EOA	1 Safe tx (4-of-7) OR 1 EOA tx	Yes, 2026-05-04, ~2 hours by operational EOA
Global pause (YieldVault)	pause()	PAUSER_ROLE: Safe + operational EOA	same	Yes, 2026-05-04, ~2 hours
Per-account freeze (StakingVault)	freezeAccount(address)	FREEZE_ADMIN_ROLE: Safe + operational EOA	1 EOA tx or 4-of-7 Safe tx	None observed since 2026-04-17
Per-account freeze (YieldVault)	freezeAccount(address)	FREEZE_ADMIN_ROLE: Safe + operational EOA	same	None observed since 2026-04-17
Whitelist mutation (YieldVault)	addToWhitelist, removeFromWhitelist	WHITELIST_ADMIN_ROLE: Safe + operational EOA	1 EOA tx	Yes, 2026-04-28 and 2026-05-01
USDC withdrawal (YieldVault)	withdrawUSDC (to, amount)	WITHDRAWAL_ADMIN_ROLE: operational EOA only by design, to must be whitelisted	1 EOA tx	Yes, 2026-05-01, 903 + 100 USDC to operational EOA
Reward distribution (StakingVault)	distributeRewards(amount)	REWARDS_ADMIN_ROLE: EOA only (real-time)	1 EOA tx, capped (BPS 75, per-call 1M wYLDS, cooldown 1h, lifetime 10M wYLDS)	Yes, hourly cadence
Reward distribution (YieldVault)	distributeRewards (planned move to Safe)	REWARDS_ADMIN_ROLE: EOA today; Hastra plans	1 EOA tx → planned 4-of-7 Safe	Hastra response Q2

Lever	Function	Who Can Trigger	Threshold	Used Historically
		to move to Safe (monthly distribution)		
NAV oracle update (StakingVault)	setNavOracle(...) and rate ingestion	NAV_ORACLE_UPDATER_ROLE: EOA only by design	1 EOA tx	Hourly NAV writes by dedicated keeper EOA
Implementation upgrade (any of four contracts)	upgradeToAndCall	UPGRADER_ROLE (or owner() for NavEngine): Safe 0x8D358B...6309 only	4-of-7 Safe tx, no timelock	None observed since deployment
Per-mint freeze (Solana)	SPL FreezeAccount	freeze authority PDA	per program upgrade-authority gating	Held but unused on PRIME; used 3 times on wYLDS in 2025
Provenance circuit-breaker	x/marker pause without gov vote	foundation/team addresses	n/a	Holders undisclosed, not exercised on uylds.fcc

6.5 Operational EOA Topology and Hastra Design Rationale

Hastra's stated design (response Q2, Q3) treats EOAs as legitimate operational components rather than legacy holders. Real-time operations that "cannot be multisigned" are kept on dedicated EOAs by design: REWARDS_ADMIN on StakingVault (hourly distribution), NAV_ORACLE_UPDATER (hourly NAV write), FeedVerifier UPDATER (hourly Chainlink report verification), HastraNavEngine `updater`, and YieldVault WITHDRAWAL_ADMIN. PAUSER, FREEZE_ADMIN, and WHITELIST_ADMIN are dual-held by the Safe and the operational EOA hot wallet. DEFAULT_ADMIN and UPGRADER sit on the Safe only. YieldVault REWARDS_ADMIN is currently EOA but planned to move to Safe-only (monthly multisig-approved distribution).

The deployer EOA `0x5f134E02...59b3` was described by Hastra as "the temp deployer." It has now been revoked from `DEFAULT_ADMIN_ROLE` and `UPGRADER_ROLE` on all four production contracts. Hastra has stated intent to add more operational EOAs as off-chain infrastructure expands.

This topology is reasonable for operational ergonomics. The collateral-risk implication is that an arbitrary upgrade (DEFAULT_ADMIN or UPGRADER) requires a 4-of-7 Safe quorum, materially stronger than the prior single-key state. The remaining structural concern is the absence of any timelock between Safe execution and proxy upgrade.

6.6 Blast Radius Analysis

Safe `0x8D358B...6309` quorum compromise (4 of 7 keys):

1. Upgrade implementation of any of the four contracts (StakingVault, YieldVault, HastraNavEngine, FeedVerifier) via `upgradeToAndCall`. Arbitrary replacement logic enabling unbounded mint, USDC drain, freeze. No timelock.
2. Replace the FeedVerifier implementation; return any price for any feed ID.
3. Replace HastraNavEngine implementation; bypass `[minRate, maxRate]` band entirely.
4. Pause both vaults; freeze any holder; mutate whitelist; trigger NavEngine owner actions.
5. Resolves within one block once 4-of-7 sign. No detection or exit window.

The layered mint caps (BPS 75, per-call 1M wYLDS, cooldown 1 hour, lifetime 10M wYLDS) prevent unbounded NAV-uplift via legitimate `distributeRewards` calls but do not constrain a malicious `upgradeToAndCall` that replaces the contract logic entirely.

Operational hot-wallet EOA compromise (`0xA8C3CF61...0faCd`, holds PAUSER, FREEZE_ADMIN, WHITELIST_ADMIN, WITHDRAWAL_ADMIN, FeedVerifier UPDATER per Hastra design):

1. Pause both vaults at will. Sherlock §3.3 frames pause-then-reconfigure-then-unpause as the documented operational pattern; an attacker can pause indefinitely until the Safe revokes the role.
2. `withdrawUSDC` to any whitelisted address. If the operational EOA also holds WHITELIST_ADMIN, it can self-add a destination, then drain. (At launch state YieldVault USDC float is small.)
3. Freeze any holder.
4. Submit malicious `verifyReport` data via FeedVerifier UPDATER, subject to Chainlink DON signature validation (which the on-chain wrapper enforces). The UPDATER can submit a stale-but-Chainlink-signed report under the staleness window; effect is bounded by Chainlink-signed price reality.

StakingVault REWARDS_ADMIN / NAV_ORACLE_UPDATER EOA compromise:

1. Mint rewards into StakingVault subject to BPS/per-call/cooldown/lifetime caps; cumulative reward mint capped at 10M wYLDS, but that is still a material economic move.
2. Set NAV oracle parameters within the rate band.

Comparison with Solana Squads compromise (4 of 7 of 7 keys):

1. Upgrade vault-mint or vault-stake; identical blast radius to the Ethereum Safe case.
2. Execute immediately (`time_lock = 0`).

SPL versus ERC-20 deltas (folded from prior review): Despite the lower-than-ideal Solana threshold (4 of 7 with 0-second lock), the Solana side has been in operation longer, used multiple lifetime executions, and has an enumerable signer set. The Ethereum Safe is fresher, does not yet have a public threshold, and operates without a timelock in front. The collateral implication is that until the Safe is disclosed, the Ethereum side cannot be confirmed as more governance-protected than the Solana side, and may be materially less so.

No-second-signer dependencies: None at the Safe level for StakingVault and YieldVault (every privileged action is one Safe transaction at the disclosed-pending threshold). On NavEngine and FeedVerifier, the dependency collapses to a single EOA signature.

7. Code Audit Findings

7.1 Audit History

Artifact	Status
Independent audit firm	**Sherlock** (collaborative audit, leads 0xeix and Oblivionis)
Engagement 1	Core vault implementation (EVM + SVM), 2026-03-04 to 2026-03-13. 0 Critical, 0 High, 2 Medium, 7 Low/Info.
Engagement 2	Chainlink Data Streams NAV integration (EVM + SVM price-verification), 2026-04-09 to 2026-04-12. 0 Critical, 0 High, 2 Medium, 4 Low/Info.
Combined totals	0 Critical, 0 High, 4 Medium, 11 Low/Info. 2 Mediums resolved, 2 Mediums acknowledged with documented residual-risk acceptance. All Low/Info resolved.
Audited final commit	52655033264d37225929cf0059fba478fed69795. This matches the Hastra commit log entry on 2026-04-22 ("mainnet deploy scripts and addresses, #30") observed in the public repo, indicating that the live mainnet bytecode at 0x19ebb352..., 0x6aD038cA..., 0xfEd839B6..., and 0xdF4ab20f... corresponds to the audited code state.
Audit scope	StakingVault.sol, YieldVault.sol, HastraNavEngine.sol, FeedVerifier.sol on Ethereum; vault-mint and vault-stake programs on Solana; the Chainlink Data Streams integration on both chains.
Public release form	Redacted summary (PoC code, exploit mechanics, environment-specific identifiers, and source-level references removed). Full technical report available from Sherlock
Repo /audits directory	Not yet present in provenance-io/hastra-eth-vault at 2026-05-05. Hastra response Q1: "When we get the final report, yes" (will publish).
provenance-io/hastra-eth-vault README	Still flags "Not audited" at 2026-05-05; stale. Should be updated to reflect Sherlock engagement on receipt of public report.

Artifact	Status
Bug bounty	None disclosed. No Immunefi listing at immunefi.com/explore/?query=hastra (2026-05-05).
Internal test coverage	Foundry fuzz tests present (StakingVault.fuzz.t.sol, YieldVault.fuzz.t.sol). Anchor test suite present in Solana repo.
Formal verification	None disclosed.
Verifiable builds	Solana program source attestations now registered via solana-verify for every deployment, enabling on-chain bytecode-to-source verification

Sherlock high-level themes (per report §3):

1. **EVM-Solana semantic drift** (oracle staleness anchoring, unbonding flow). The dominant surface across both engagements. EVM was the canonical reference; Solana side required corrections.
2. **Reward distribution share-price discontinuity.** Single-block share-price change on `distributeRewards` is a sandwich/MEV vector on EVM and a virtual-shares dilution effect on Solana. Both **acknowledged by Figure as accepted residual risk** under the current operational model. Not user-principal-threatening; materiality scales with reward size and TVL.
3. **Operator-privileged configuration paths defer fail-safety to operational discipline.** Sherlock recommends fail-closed by default. Some items remediated on EVM side; Solana side has at least one remaining acknowledged forward-looking item.

Sherlock §4 operational recommendations: cross-chain parity reviews; privileged-action runbooks (pause-then-verify); event-driven monitoring; forward-looking design review of reward distribution.

The combined posture is **substantially stronger than the prior baseline**, which had assumed unaudited code on mainnet. Sentora can now treat StakingVault, YieldVault, HastraNavEngine, and FeedVerifier as independently reviewed by a credible firm, with the residual-risk profile concentrated in (a) the share-price MEV / dilution accepted residuals, (b) the Solana acknowledged forward-looking item, and (c) operational reliance on documented runbooks for pause-then-reconfigure flows. Outstanding gaps that Sherlock's scope did not cover: **operational EOA custody disclosure**, **Safe deployment plan**, **YieldVault USDC float and replenishment SLA**, **proof-of-reserves attestation cadence**.

7.2 Code Review Findings: Comprehensive Table

Every §3 row appears here, plus long-tail findings.

ID	Title	Severity	Source	Location	Description	Impact
F-2	Sherlock-acknowledged residual risk: reward distribution share-price discontinuity	Medium	Sherlock Audit	StakingVault `distributeRewards` (EVM); vault-stake `publish_rewards` (Solana)	Per Sherlock §3.2: discrete single-block share-price change. Sandwich/MEV vector on Ethereum, virtual-shares dilution on Solana. Formally acknowledged by Figure as accepted residual risk under the current operational model.	Affects distribution of rewards among stakers under specific conditions. Does not threaten user principal or protocol solvency. Materiality scales with reward size, TVL, and MEV-infrastructure maturity.
F-3	UUPS upgrade with no timelock	Critical	Internal Review	`_authorizeUpgrade` on StakingVault, YieldVault, HastraNavEngine, FeedVerifier; BPF upgrade authority on vault-mint, vault-stake	No OpenZeppelin TimelockController in the admin chain on either chain; Solana Squads has `time_lock = 0`. Ethereum Safe at `0x8D358B...6309` has no timelock between Safe execution and proxy upgrade. Hastra response Q4 explicitly states no timelock is planned, with layered mint caps cited as compensating control. The mint caps do not constrain `upgradeToAndCall`. (See planned execution table in section 12)	Implementation swap completes in the same block on Ethereum (4-of-7 Safe quorum) or same slot on Solana (4-of-7 Squads quorum). No detection or exit window.
F-4	Oracle revert locks	Critical	Internal Review	StakingVault._convertToShares and	Both call NAV unconditionally. Stale,	A keeper outage,

ID	Title	Severity	Source	Location	Description	Impact
	deposits and redemptions			_convertToAssets (Eth); vault-stake.deposit (Solana)	zero, or reverting oracle blocks deposit and redeem with no last-good-price fallback. Default Ethereum staleness 3,600 s. (See planned execution table in section 12)	signed-report rotation, or DON incident halts user mint and redeem on both chains. PRIME holders cannot exit even at a discounted price.
F-5	Safe owners and custody mix not publicly disclosed	High	Internal Review	Safe 0x8D358B8aE881F8ea92C3d07783aBCA21727C6309	The Safe is verified on-chain (Safe v1.4.1, 4-of-7 threshold, 7 owners enumerated, nonce 8). Owner addresses are publicly readable; identity-to-address mapping, custody mix (HSM, institutional MPC, software), and geographic distribution are not publicly known. One signer address (0x13b29ad4...) appears in early YieldVault test deposits, suggesting Hastra-team operational use of one signer key for testing.	A 4-of-7 quorum compromise upgrades any contract in one block (no timelock per F-3). Without custody-disclosure visibility, Sentora cannot evaluate the practical resistance of the multisig to a coordinated compromise.
F-6	Liquidation routing depends on admin-gated redemption	High	Internal Review	StakingVault redeem; YieldVault requestRedeem plus admin completeRedeem	The PRIME → wYLDS leg is permissionless. The wYLDS → USDC leg is REWARDS_ADMIN_ROLE only. Hastra has stated intent to move the YieldVault REWARDS_ADMIN to the Safe, requiring multisig approval for monthly	Liquidator capital that converts PRIME to wYLDS instantly must then wait on admin execution to settle in USDC. Without explicit SLA and

ID	Title	Severity	Source	Location	Description	Impact
					distribution. The chokepoint is structural and persists regardless of liquidity levels. (See planned execution table in section 12)	pause-policy carve-out, a liquidation event can stall mid-flow.
F-8	Permissive HastraNavEngine defaults	High	Internal Review	HastraNavEngine constructor parameters	maxDifferencePercent = 100 percent, rate band 1.0 to 3.0. Read-contract values not retrievable in this refresh; presumed unchanged from baseline. (See planned execution table in section 12)	TVL can move 100 percent between updates without revert; the rate band tolerates a 200 percent excursion across the full 1.0 to 3.0 range.
F-9	Admin-gated USDC exit	High	Internal Review	YieldVault.completeRedeem	REWARDS_ADMIN_ROLE only; users cannot force settlement. Same gating on Solana. (See planned execution table in section 12)	A rewards admin outage, key loss, or pause stalls all USDC exits, including liquidator settlement on a Sentora Morpho vault.
F-10	Off-chain custodial backing without atomic link	High	Internal Review	Provenance uylds.fcc marker; Ethereum and Solana wYLDS supplies	wYLDS supplies on the two chains are independent mints; backing relies on Hastra custody of Provenance YLDS marker balances. No on-chain proof, no IBC, no Wormhole, no LayerZero, no CCIP.	A Hastra operational error or custody failure on any of the three locations breaks the 1:1 backing claim with no on-chain detection.
F-11	Pause power	High	Internal Review	StakingVault.pause and	Both vaults paused for ~2 hours on 2026-05-04,	A pause during a Morpho

ID	Title	Severity	Source	Location	Description	Impact
	available during liquidation events			YieldVault.pause	consistent with Sherlock §4 operational recommendation (pause-then-reconfigure-then-unpause runbook). Pause is held by deployer EOA + operational hot-wallet EOA today; planned to also include the Safe.	liquidation halts the redemption-based liquidation route. Liquidator capital can sit trapped while NAV continues to move.
F-12	No PRIME supply cap	**Medium**	Internal Review	StakingVault	distributeRewards caps reward amount per period (1M wYLDS) and lifetime (10M wYLDS), but global PRIME supply is unbounded. Caps themselves resettable by upgrade. Hastra response Q4 emphasizes the layered caps as the primary protection against runaway minting. (See planned execution table in section 12)	Repeated deposits at falling NAV grow share count indefinitely; governance must externally manage expected supply. The lifetime cap (10M wYLDS) effectively bounds reward-driven NAV uplift even though raw share count is unbounded.
F-13	YieldVault WITHDRAWAL_ADMIN sits on EOA only	**High**	Internal Review	YieldVault withdrawUSDC and whitelist functions	Per Hastra response: WITHDRAWAL_ADMIN held by operational EOA only by design (intentional, real-time). WHITELIST_ADMIN is Safe + EOA. If the operational EOA also holds WHITELIST_ADMIN, the same EOA can self-add a	Operational EOA compromise enables USDC withdrawal subject to whitelist; if the same EOA holds WHITELIST_ADMIN, it can self-add. At

ID	Title	Severity	Source	Location	Description	Impact
					destination, then drain whitelisted USDC. (See planned execution table in section 12)	launch state, USDC float in YieldVault is small ($1.15 at 2026-05-05); risk scales with vault TVL.
F-14	Permissive Solana price config (no min/max band)	Medium	Internal Review	vault-stake.StakePriceConfig	Chainlink Data Streams price accepted if > 0 and fresh. No analogue to Ethereum's minRate and maxRate. (See planned execution table in section 12)	An oracle misconfiguration or extreme price excursion cannot be bounded on-chain on Solana.
F-15	Coordinated 2-hour pause on 2026-05-04	Informational	Internal Review	StakingVault and YieldVault Pause events 2026-05-04 21:50 to 23:54 UTC	Both vaults paused for approximately two hours by the operational EOA. Sherlock §4 documents pause-then-reconfigure-then-unpause as the recommended operational pattern, suggesting routine maintenance. No Upgraded event in the window.	Operational opacity for an external observer. With Sherlock's runbook context, the pause is consistent with normal operations.
F-19a	Sherlock-acknowledged forward-looking item: Solana operator-privileged config does not fail closed	Medium	Sherlock Audit	Solana operator-privileged path per Sherlock §3.3	Per Sherlock: a privileged configuration update path on Solana does not invalidate now-meaningless prior state when semantically-coupled inputs change. Remediation applied on Ethereum side; Solana side is acknowledged forward-looking.	Operator must follow pause-then-reconfigure-then-verify-then-unpause runbook for safety. Time window between configuration change and next verification

ID	Title	Severity	Source	Location	Description	Impact
						is the residual risk.
F-16	Freeze-after-requestRedeem bricks user shares	Medium	Internal Review	YieldVault.completeRedeem and _update override	completeRedeem checks frozen[user] and reverts. If a user is frozen post-request and cancelRedeem is also gated by the freeze check, shares are stuck with no admin recovery path documented.	Edge-case loss of access for individual users. Limited blast radius per incident.
F-17	HastraNavEngine.initialize accepts minRate > maxRate	Medium	Internal Review	HastraNavEngine.initialize, _setMinRate, _setMaxRate	First-init footgun: _setMinRate skips the maxRate cross-check (maxRate still 0 at first init); _setMaxRate does not cross-check minRate. Subsequent updateRate would always revert.	Misconfiguration during deployment bricks the engine.
F-18	StakingVault initialize does not set NAV oracle	Medium	Internal Review	StakingVault.initialize	Vault is deployed in a state where getVerifiedNav() reverts until admin calls setNavOracle(oracle, feedId). First user deposit fails until wiring is complete.	Operational footgun for new deployments and recovery scenarios.
F-19	Solana complete_redeem is rewards-admin only	Medium	Internal Review	vault-mint/processor.rs complete_redeem	Same forced-exit gap as Ethereum. User locks PRIME shares; only a rewards admin can finalize. (See planned execution table in section 12)	Equivalent admin-gated USDC-exit chokepoint as F-9.
F-20	Solana external_program_mint validates admin via	Medium	Internal Review	vault-mint/processor.rs external_program_mint	The admin-identity parameter is checked against config.rewards_administrators. The	A single compromised admin-list key triggers unbounded

ID	Title	Severity	Source	Location	Description	Impact
	list membership, not Signer				external_mint_authority PDA proves caller program origin, but a compromised rewards admin key still gives unlimited wYLDS reward mint subject to StakeRewardConfig caps.	reward mint; caps are themselves resettable by upgrade authority.
F-21	Solana sweep_redeem_vault_funds requires only one rewards-admin signature	Medium	Internal Review	vault-mint sweep flow	Single admin-list member can drain the redeem vault.	Operational risk: one key compromise allows USDC drain on the Solana side.
F-22	No hard upper bound on max_reward_bps (Solana)	Medium	Internal Review	vault-stake.update_max_reward_bps	Upgrade authority can raise the BPS cap to 10,000 (100 percent) in one Squads proposal.	Cap looseness combined with time_lock = 0 allows immediate execution.
F-23	Provenance circuit-breaker module (Provenance)	Medium	Internal Review	app/upgrades.go setupCircuitBreakerPermissions	Foundation/team addresses can pause specific message types, including potentially x/marker mint and burn, without governance vote. Holder identities undisclosed.	A circuit-breaker pause on uylds.fcc halts YLDS minting and burning, propagating into wYLDS minting on both Solana and Ethereum.
F-24	Provenance Nakamoto coefficient ~8	Medium	Internal Review	cosmos/staking/v1beta1/validators	Eight validators control 33.4 percent of bonded stake; Figure operates four of the top 10.	A coordinated halt of eight entities, or a Figure-internal operational incident, removes 20 to

ID	Title	Severity	Source	Location	Description	Impact
						33 percent of voting power.
F-25	depositWithPermit silent fallback (Eth)	Low	Internal Review	StakingVault.depositWithPermit	Catches permit revert and proceeds with prior allowance (comment-documented, intentional).	Integrator footgun for those relying on atomic permit-then-deposit semantics.
F-26	Merkle leaf format footgun (Eth)	Low	Internal Review	YieldVault.claimRewards	Claim leaf uses keccak256(bytes.concat(keccak256(abi.encode(...)))). Off-chain tree must match exactly.	Wrong proofs if abi.encodePacked is used off-chain.
F-27	vault-stake-auto declared but undeployed	Low	Internal Review	Anchor.toml; address Dz8K7J1U...wjHB	Account null on Solana mainnet at 2026-04-23. Scope unknown until deployment.	Future-feature uncertainty.
F-28	Price stored as i128 on Solana	Low	Internal Review	vault-stake.StakePriceConfig	Negative values filtered by require!(price > 0). Storing signed is cosmetic.	None.
F-29	Provenance block cap (200 KB / 60M gas at ~5 s)	Low	Internal Review	app.go consensus parameters	Conservative, becomes a throughput bottleneck under scaled YLDS activity.	Throughput ceiling; not a near-term issue at current Provenance activity.

7.3 Operational Security Findings

- **Deployment hygiene.** Solidity 0.8.27, viaIR, 200 optimizer runs, OpenZeppelin Upgradeable v5.4. `_disableInitializers` called in constructors. Storage gaps reserved (StakingVault `[41]`, YieldVault `[42]`).
- **Keeper EOAs.** NavEngine updater `0xD5a28795...21e9FB4c8`; FeedVerifier `verifyReport` keeper `0xF0a5baEB...ae6cd73cd`. Custody, alerting, and failover for both keepers.
- **Init-ordering footguns.** F-17 and F-18 above: `initialize` accepts `minRate > maxRate`; `initialize` does not set NAV oracle.

- **Off-chain components.** Hastra NAV Engine; Chainlink Data Streams DON; Replicator bot per the 2026-04-24 design PDF. Custody and operational SLA.

7.4 Economic and Mechanism Findings

- **Depeg vectors for PRIME.** (i) NAV mispricing via oracle compromise or extreme `maxDifferencePercent` excursion. (ii) wYLDS-to-USDC redemption queue overflow (admin SLA failure). (iii) Pause-during-stress event. (iv) Provenance YLDS custody event (off-chain).
- **Oracle manipulation profit math.** Given `maxDifferencePercent = 100 percent` and rate band 1.0 to 3.0 on Ethereum, an oracle that returns 3.0 (assuming current NAV near 1.0) lets a depositor mint PRIME at NAV 1.0 and immediately redeem at NAV 3.0, capturing `~3x`. Solana lacks a min/max band entirely; a malicious price `>0` is accepted. Mitigation: any meaningful Morpho-vault listing requires the rate band tightened (recommended 0.95 to 1.10 for the next 12 months).
- **Redemption cliffs.** PRIME-to-wYLDS is instant on both chains. wYLDS-to-USDC is admin-gated with no documented SLA. The cliff is the wYLDS leg.
- **Incentive misalignments.** Reward distribution is at admin discretion within caps; a backdated NAV uplift could be timed to favor specific accounts. Detection requires off-chain monitoring of `distributeRewards` calls relative to large deposits.

8. Holder Concentration and On-chain Distribution

Ethereum (2026-05-27):

Rank	Address	Identity	Balance
1	`0x19ebb35279A16207Ec4ba82799CC64715065F7F6`	StakingVault contract	~77,329,470 wYLDS held inside the vault as PRIME share backing (2026-05-27)
2+	various	47 further PRIME holders / 25 further wYLDS holders (incl. YieldVault 0x6aD038… holding ~51,978 wYLDS)	Distribution broadened materially since launch (2026-05-27)

PRIME has 48 holders. wYLDS has 26 holders. Holder distribution has broadened materially from the 2 to 4 holders observed at launch.

Ethereum holder concentration is informational at this launch state, not severity-tagged. Hastra has communicated intent to grow holder distribution; re-verify before any meaningful debt-cap increase on the Sentora Morpho vault.

Solana (2026-05-27):

Token	Mint	Supply
PRIME	`3b8X44fL...3Uu7`	284,846,062.43 (2026-05-27)
wYLDS	`8fr7WGTV...kdih`	300,284,649.67 (2026-05-27)

9. Minting and Redemption Mechanics

Capacity-and-flow lens. Complements the instruction-level trace in §5.2 and §5.3.

9.1 Minting

- **Eligibility:** Permissionless deposits at the StakingVault and YieldVault user calls. YieldVault `deposit` requires whitelist on the user side (non-default); StakingVault `deposit` requires the user not be frozen.
- **Caps:** No mint cap. No per-tx or per-period cap on user deposits. Reward distributions to the vault have caps (BPS 75, period 1M wYLDS, lifetime 10M wYLDS).
- **Circuit breakers:** `pause()` on either vault halts `deposit` and `redeem`. Exercised 2026-05-04.
- **Cross-chain hop count:** None. Ethereum and Solana mint independently.
- **Where mint authority resolves:** StakingVault `_mint` is gated by `deposit` and `distributeRewards` paths. Effective mint authority for PRIME is the Safe (now). `MINT` permission for the underlying YLDS is held by the `uylds.fcc` marker access list on Provenance, controlled by Figure Certificate Company.

9.2 Redemption

- **Sync vs async.** PRIME-to-wYLDS is synchronous (instant burn-and-return at NAV). wYLDS-to-USDC is asynchronous with admin-gated completion.
- **Queueing.** YieldVault stores `PendingRedemption` per user; no batched epoch.
- **Observed settlement timing under normal load.** No production-volume settlement events observed on Ethereum at 2026-05-05.
- **Large-redemption behavior.** Untested at scale on Ethereum. Solana `request_redeem` plus `complete_redeem` flow has run in test deposits at modest scale.
- **Admin-gating.** `completeRedeem` is `REWARDS_ADMIN_ROLE` only. If the rewards admin does not execute, USDC settlement does not occur. There is no permissionless fallback.

9.3 Market Liquidity in DeFi

Ethereum DEX venues at 2026-05-27.

Venue	PRIME pool	wYLDS pool
Uniswap V3	PRIME/USDC 0.01% — 0x5b70...3115 (~$9.0M reserve, ~$130k 24h vol)	None found
Uniswap V4	None found	None found
Curve	None found	None found
Balancer	None found	None found

Lending-market integrations:

Protocol	Status (Ethereum)	Status (Solana)
Aave V3 / Horizon	Not listed	n/a
Morpho	Listed on Sentora PRIME Main	n/a
Euler V2	Not listed	n/a
Spark / sparklend	Not listed	n/a
Pendle	Not listed	n/a
Maple	Not listed	n/a
Kamino	n/a	Listed

Permissioned vs permissionless secondary: Ethereum YieldVault `deposit` is whitelist-gated. PRIME secondary (transfer between holders) is permissionless except for frozen accounts. The wYLDS-to-USDC exit is admin-gated.

9.4 Replenishment Rates and SLAs

- **YieldVault cash buffer at 2026-05-27. 121,153.58 USDC inside the YieldVault contract; the operational EOA (0xA8C3CF61...0faCd) holds ~984 USDC. Float has grown materially from the ~$1 launch-state buffer; still informational, not severity-tagged.**
- **Replenishment cadence after large redemption.** No documented SLA. No observed production-volume event.
- **Documented redemption SLA.** None public.

- **Off-chain dependency.** Liquidation on a Sentora Morpho vault depends on (i) StakingVault `redeem` (instant, oracle-gated), (ii) YieldVault `requestRedeem` (instant), (iii) admin `completeRedeem` execution (admin-gated, dependent on USDC float and operational availability).

Operational implication for the Sentora Morpho vault. Liquidation routing requires a contractual minimum USDC float in YieldVault sized to the Morpho debt cap, plus an explicit `completeRedeem` SLA, plus a pause-policy carve-out for liquidation events. Without these, a lever-up event coinciding with a NAV move can trap liquidator capital and accumulate bad debt against the Morpho vault.

10. Tokenomics and Governance Token Design

N/A. Skipped per template. PRIME has no native governance token. wYLDS is a wrapper. YLDS is an SEC-registered face-amount certificate issued by Figure Certificate Company; it is a security, not a governance token. Hastra has not announced a governance token, lockup mechanism, or fee-accrual structure tied to a token.

11. Team and Legal

11.1 Team

- **Operating relationships (per Sherlock audit introduction, 2026-04-27):** "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**."
- **Named principals:** Mike Cagney (Figure CEO and co-founder, public profile via Figure IR, LinkedIn). Hastra-specific named operational leadership not publicly disclosed.
- **Prior protocols:** Figure (HELOC, Democratized Prime, YLDS, Provenance Blockchain). Mike Cagney previously co-founded SoFi.
- **Anonymous vs doxxed signers.** Solana Squads 7 keys: not publicly tied to named individuals. Ethereum Safe owners: pending Safe deployment per §6.2.
- **Operational presence.** Figure operates four Provenance validators (`Figure`, `arbiter34 | Figure`, `Provenance East`, `Provenance West`); combined ~20 percent of bonded stake. Hastra operational headcount not publicly disclosed.

11.2 Legal Entity

- **Operating company:** Hastra (built by Figure Technologies, operated by Provenance Blockchain Foundation per Sherlock report). `hastra.io` and `help.hastra.io` are live. **Per Hastra's Terms of Use, Hastra is owned by Signum Ltd, a BVI company wholly owned by the Provenance Cayman Foundation (ownership attaches to Hastra, not "Hastra LLC").**
- **Regulatory registrations (YLDS):** YLDS is filed at SEC EDGAR under Figure Certificate Company. Class registration as a face-amount certificate.
- **Counterparties.**

- Transfer agent: Figure Equity Solutions.
- Custodian: Hastra (operational).
- Fund administrator: pending.
- Auditor: pending (different from the security audit gap noted in §7.1; refers to financial-audit on Figure Certificate Company's books).

- **Token issuer (separate entities):** Figure Certificate Company issues YLDS; Hastra issues wYLDS and PRIME via the on-chain vault.

11.3 Disclosure Gaps

- Provenance circuit-breaker authority list.
- End-user recourse path in a dispute or insolvency: Hastra LLC versus Figure Certificate Company, securities-law treatment of wYLDS in custody and PRIME secondary, and the operational link between Provenance YLDS marker balance and on-chain wYLDS supply.

12. Remediation Status and Planned Execution

The following table consolidates the remediation items raised in this assessment against Figure/Hastra's due-diligence response. Planned items are stated by Figure to be executed end-of-Q3-2026 target.

Update Item	Description	Status
Safe deployment & EVM admin-role migration	Safe 0x8D358B...6309 granted DEFAULT_ADMIN + UPGRADER on YieldVault, StakingVault, FeedVerifier; HastraNavEngine owner() migrated; deployer EOA revoked. [Verified on-chain 2026-05-06]	**Completed**
Upgrade timelock (EVM + Solana)	24-hour timelock for all EVM UUPS upgrades (via OpenZeppelin TimelockController holding UPGRADER_ROLE) and Solana program upgrades. Reverses the prior position that no timelock was planned.	**Planned — Q3 2026**
Independent security audit	Sherlock collaborative audit received: 0 Critical, 0 High, 4 Medium (2 acknowledged residuals), 11 Low/Info resolved. Final commit matches deployed mainnet bytecode.	**Completed**
NavEngine deviation-bound tightening	Per-update rate-delta limit independent of TVL drift (covering both TVL and supply) plus a minimum update interval to prevent same-block rate walking.	**Planned — Q3 2026**

Oracle fallback / degraded-mode exit	No last-good-price fallback or sub-NAV exit path; deposits and redemptions revert on stale or missing oracle. Not addressed in the DD response.	**Pending**
Bug bounty program	No Immunefi listing or disclosed bug bounty program.	**Pending**
Solana upgrade-authority migration	Solana program upgrade authority migrated to a 4-of-7 Squads multisig.	**Completed**
Rewards administration → multisig	Merkle-based wYLDS reward administration (monthly interest distribution) to be moved to a 4-of-7 multisig on both Solana (Squads) and Ethereum (Safe).	**Planned — Q3 2026**
Solana role segregation (freeze vs rewards)	freeze_administrators and rewards_administrators to be separated into distinct addresses.	**Planned — Q3 2026**
EVM role segregation (whitelist vs withdrawal)	WHITELIST_ADMIN_ROLE and WITHDRAWAL_ADMIN_ROLE to be split across different addresses; WHITELIST_ADMIN moved to a multisig with a 24-hour timelock for new destinations.	**Planned — Q3 2026**
Rewards minter role restriction	Direct minting access restricted — future minting limited to the StakingVault contract or moved to a timelocked multisig.	**Planned — Q3 2026**
Solana verifiable builds	Source attestations registered via solana-verify for every deployment, enabling bytecode-to-source verification.	**Completed**
Reward verification guardrails	On-chain binding aggregate cap plus per-epoch cumulative claim tracking to bound rewards distributed per epoch.	**Planned — Q3 2026**
Solana redemption security	Account constraint requiring user_vault_token_account.owner == user.key() to prevent redirection of redemptions.	**Planned — Q3 2026**
Hastra ownership disclosure	Hastra disclosed as owned by Signum Ltd (BVI), wholly owned by the Provenance Cayman Foundation (per Hastra's Terms of Use). Ownership attaches to Hastra, not "Hastra LLC".	**Completed**