Security review

Scope

The review covers wstETH custody, TINE emissions, term bonuses and governance. It also covers the backing index, ETH router, Lens, NFT renderer, Uniswap v4 hook, liquidity launch and the website's deposit, renewal and withdrawal flows.

The reviewed source is Git revision f48be1a. Production bytecode, the live site's deployment configuration and control of the signing keys require separate verification.

Git revision
f48be1a59a2b4299cb90d1d7e9f69b79d1073931
Tracked repository archive · SHA-256
259b7a0941ef5c8f936dbe151bd9ecb37f2630a3d2d7b81bb3ca91cace3962c5
contracts/TineSavings.sol · SHA-256
241dbd8a572892b4b7a6191ed410be56e398061064392f947ffd35474f3c350c
contracts/TineRouter.sol · SHA-256
85b632236ebb13ed964b623d01ab2a0a53b98098f8c9ff4213ff0e4d881cbdf7
web/assets/app.js · SHA-256
d4d6fe21d575639f15cde8aa39a48013aa36308a17b9ac35358cc788aad9d509
Verify the archive from a checkout
git -c tar.umask=0002 archive --format=tar f48be1a | sha256sum

Accepted findings

ECO-1 · A new deposit shares the pool's capture clock

Potentially high impact if the backing rate is wrong. CaptureLimit.retention(elapsed) sets the minimum fraction of pool units that _capture must retain. Its fixed 50% annual compounded growth ceiling means that after one year at least two thirds stay as principal, even if the index reports tenfold growth. New deposits share the pool's elapsed time, so a long gap between positive captures weakens that protection. **Why accepted.** The project identified this risk during design and considers the cap sufficient for wstETH given its choice of asset and reviewed backing index.

GOV-1 · Governance can shorten the initial 48-hour delay

The launch configuration uses a two-of-three Safe. The developer controls two keys. Changing the delay must itself wait out the current delay. Once the change takes effect, later proposals can execute sooner. **Why accepted.** The project wants governance to be able to evolve after launch and accepts that 48 hours is an initial setting.

CORE-1 · A new term immediately shares in forfeited bonuses

If another saver leaves early just after you start a term, your weight counts toward their forfeited bonus. Other eligible savers then receive a smaller share. You must keep the corresponding funds through your own maturity to collect yours. **Why accepted.** The project considers that commitment sufficient. Longer terms carry more weight, and immediate eligibility keeps the allocation rule simple.

Savings bonuses

CORE-5 · A yield update can cross a maturity

When an update spans a maturity, the pool allocates that interval's yield using the weights in force before the first expiry. If two positions have equal weight and one matures between updates, each receives six of twelve bonus shares for that interval. Update timing can therefore affect the final bonus. **Decision.** The project chose to give both equal-weight positions their full share of that interval.

Website and integrations

WEB-1 · TINE valuation

The displayed APR values TINE at its current Uniswap price. The ETH you receive when selling depends on trade size and available liquidity. **Why accepted.** Tine uses the market price because trades can move it in either direction.

WEB-6 · Portfolio totals

If the website cannot read one position's TINE rewards, the total can omit them without indicating that it is incomplete. The position's onchain entitlement is unaffected. **Why accepted.** The project considers an isolated read failure too unusual to warrant separate handling in the total.

UX-3 · One-wei conversions

For a withdrawal quoted at one wei, a 0.1% slippage allowance rounds the minimum down to zero. The router requires a positive minimum and rejects that conversion. **Why accepted.** The project considers one wei economically negligible and keeps the positive minimum.

WEB-2 · Wallet reconnection

Returning with a previously connected wallet can send its public address to the configured RPC provider when the website refreshes balances. **Why accepted.** Restoring an authorised wallet lets savers reload the page and keep working without reconnecting.

PER-2 · NFT images

A marketplace can keep showing a cached card after you renew. The savings contract records the current maturity. **Decision.** Tine retains the existing events and accepts that a marketplace image may lag.

CORE-3 · Renewal data

The renewal event records the position ID and its new maturity. **Why accepted.** The Lens already exposes the position state, so the project keeps the event small.

Methodology and test results

The review traced deposits, yield capture, bonus allocation, renewals and withdrawals through the contracts and the website. It combined source inspection, independent compilation, automated tests and transactions on a local Ethereum fork.

Automated suite

446 passed / 0 failed / 1 skipped

The protocol and website suite ran 447 tests across 38 files. The skipped test checks a wallet switch during an approval. Direct withdrawals have no approval step.

Independent checks

Build reproducibility

Native and WebAssembly builds of Solidity 0.8.28 produced matching ABIs, creation bytecode and runtime templates for all 16 production artifacts compared.

Savings accounting

Two randomised runs checked 316 states for custody, treasury liabilities, shares and emissions. They compared 2,754 expiry snapshots and checked 39 renewals against a close at the same timestamp. Both runs ended with zero recorded liabilities after every position closed.

Ethereum integration

On a fork at Ethereum block 26,483,556, two withdrawals of 0.01 wstETH through Lido paid the exact quoted minimum in stETH at zero slippage. One recipient started with stETH and the other had none.

Website flows

In desktop Chrome, a partial withdrawal returned 25 wstETH from a 100-share position. In a mobile viewport, a recovery withdrawal with the index unavailable returned the remaining 75 wstETH and closed the position.

Static analysis

Slither ran 101 detectors and reported 87 alerts. All 16 alerts the tool labelled high were reviewed. None was confirmed as a high-severity implementation flaw. ECO-1 concerns the economic consequences of an incorrect backing rate.