ClarityAlliance

Zest Bitcoin Collateral Vaults Demo Security Review

Conducted by:
Kristian Apostolov

September 15th, 2026

Contents

1. About Clarity Alliance

Clarity Alliance is a team of expert whitehat hackers specialising in securing protocols on Stacks.

They have disclosed vulnerabilities that have saved millions in live TVL and conducted thorough reviews for some of the largest projects across the Stacks ecosystem.

Learn more about Clarity Alliance at clarityalliance.org.

2. Disclaimer

This report is not, and should not be considered, an endorsement or disapproval of any project, team, product, or asset, nor does it reflect on their economics, value, business model, or legal compliance. It does not provide any warranty regarding the absolute bug-free nature or functionality of the analyzed technology.

Nothing in this report should be used to make investment or participation decisions. It does not constitute investment advice. Instead, it reflects an extensive assessment process intended to help clients improve code quality and reduce the inherent risks associated with cryptographic tokens and blockchain systems.

Blockchain technology presents ongoing and significant risk, and each company or individual remains responsible for their own due diligence and security posture. Clarity Alliance aims to reduce attack vectors and technological uncertainty but does not guarantee the security or performance of any system we review.

All assessment services are subject to dependencies and active development. Your access to and use of any services, reports, or materials is at your sole risk on an as-is and as-available basis.

Cryptographic tokens are emergent technologies with high technical uncertainty, and assessment results may include false positives, false negatives, or other unpredictable outcomes. Smart contracts may depend on multiple external parties, remain vulnerable to internal or external exploitation, and may carry elevated risks if owner privileges remain active. Accordingly, Clarity Alliance does not guarantee the explicit security of any audited smart contract, regardless of the reported verdict.

3. Introduction

A time-boxed security review of Zest Protocol's Bitcoin Collateral Vaults Demo, where Clarity Alliance reviewed the scope and provided insights on improving the protocol.

4. About Zest

Zest Protocol Overview

How Zest Protocol turns Bitcoin from an idle asset into productive capital through Bitcoin Collateral Vaults and its Stacks product suite.

Zest Protocol is the capital layer for Bitcoin, turning Bitcoin from an idle asset into productive capital.

Bitcoin Collateral Vaults let holders borrow stablecoins against BTC or put it to work on any chain that can read a proof. The team has built on Bitcoin since 2021 and previously ran a $100M+ Bitcoin credit market on Stacks.

Explore Zest Protocol's products below.

Bitcoin Collateral Vaults

Bitcoin Collateral Vaults let BTC remain on Bitcoin while its value works wherever it is needed. Holders lock BTC in a vault on Bitcoin and borrow stablecoins against it on a destination chain.

Lending against Bitcoin has always meant giving up custody first: wrapping it into a token or handing it to a custodian. Bitcoin's base layer couldn't verify what happened to collateral elsewhere. BitVM changes that. It lets Bitcoin L1 verify the state of a lending market on another chain, so BTC can back a loan without ever leaving the base layer.

Bitcoin Collateral Vaults

Stacks

Zest Protocol is the DeFi superapp for Stacks, bringing lending, automated yield strategies and token swaps into one product suite.

Zest Protocol Stacks Market

Stacks Market is the lending market Zest Protocol has operated since March 2024. It has processed $100M+ in peak TVL over two years with zero bad debt and no BTC lost.

Users can supply Stacks assets such as sBTC, STX and stSTX to earn yield, or use them as collateral for overcollateralised loans.

Stacks Market

Zest Protocol Stacks Vaults

Stacks Vaults package automated yield strategies into single-deposit products. The vault manages the position, rebalancing and compounding for the user.

The first is the Levered Bitcoin Staking Vault. Its strategy posts stBTC as collateral on Zest Protocol, borrows sBTC against it, stakes the borrowed sBTC into more stBTC and repeats within its risk limits. The strategy targets 6-8% APY, depending on realised Bitcoin Staking yield, borrow rates, utilisation and risk parameters. Withdrawals are paid in stBTC.

Stacks Vaults

Zest Protocol Stacks Swap

Stacks Swap is a DEX aggregator for Stacks. It compares prices across supported DEXes, can split swaps across pools and routes through intermediate tokens when needed. Every swap settles atomically with onchain minimum-received protection. The best swap experience on Stacks.

Stacks Swap

5. Risk Classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

5.1. Impact

- High - leads to a significant material loss of assets in the protocol or significantly harms a group of users.
- Medium - only a small amount of funds can be lost (such as leakage of value) or a core functionality of the protocol is affected.
- Low - can lead to any kind of unexpected behavior with some of the protocol's functionalities that's not so critical.

5.2. Likelihood

- High - attack path is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount of funds that can be stolen or lost.
- Medium - only a conditionally incentivized attack vector, but still relatively likely.
- Low - has too many or too unlikely assumptions or requires a significant stake by the attacker with little or no incentive.

5.3. Action required for severity levels

- Critical - Must fix as soon as possible (if already deployed)
- High - Must fix (before deployment if not already deployed)
- Medium - Should fix
- Low - Could fix

6. Security Assessment Summary

Scope

This security review covered Zest Bitcoin Collateral Vaults Demo, hosted in a private internal repository.

Solidity Contracts

- src/Gateway.sol
- src/Reserve.sol
- src/SimplePool.sol
- src/StaticSupplyCounter.sol
- src/PythLazerPriceAdapter.sol
- src/tokens/AToken.sol
- src/tokens/DebtToken.sol
- src/rates/InterestRateStrategy.sol

Initial Commit Reviewed

- `bc463cbb12273fbc7fca672de16ae575463bd5c0`

Final Commit Reviewed

- `e7eba2943e822a6f3c1617a4d48f3638da3db641`

7. Executive Summary

Over the course of the security review, Kristian Apostolov engaged with Zest Protocol to review Zest. In this period of time a total of **6** issues were uncovered.

Protocol Summary

Protocol Name	Zest
Report Date	September 15th, 2026

Findings Count

Severity	Amount
High	2
Medium	4
Total Findings	**6**

Summary of Findings

ID	Title	Severity	Status
[H-01]	Pool and Reserve Settlement Can Diverge	High	Resolved
[H-02]	Bitcoin Transaction ID Aliases Duplicate Collateral	High	Resolved
[M-01]	Verified Position Owner Can Differ From Mint Owner	Medium	Resolved
[M-02]	Stamp Storage Can Be Poisoned With Another Position	Medium	Resolved
[M-03]	Claims Across Multiple Vaults Cannot Be Settled by the Frontend	Medium	Resolved
[M-04]	Unauthenticated Prepare Requests Can Consume Ceremony Sessions	Medium	Resolved

8. Findings

8.1. High Findings

[H-01] : Pool and Reserve Settlement Can Diverge

Location:

- Reserve.sol#L254-L326
- SimplePool.sol#L330-L397

Description: Pool debt settlement and Reserve collateral settlement are executed in separate transactions and enforce different conditions. As a result, the Reserve may consume collateral after the Pool rejects an expired claim or a claim whose debt has already been fully repaid. This can strand user funds or leave outstanding debt without corresponding collateral.

Recommendation: Perform debt reconciliation and collateral settlement via a single atomic contract entry point, using identical claim validation logic.

[H-02] : Bitcoin Transaction ID Aliases Duplicate Collateral

Location:

- api.rs#L603-L669
- Reserve.sol#L633-L638

Description : The signer parses a Bitcoin transaction ID (txid) for verification but signs the original string. Because Bitcoin txids are case-insensitive, mixed-case representations can refer to the same transaction while producing different Ethereum collateral keys. As a result, a depositor could register the same UTXO multiple times, inflate borrowing power, and suppress liquidation.

Recommendation: Enforce a canonical lowercase txid prior to signing, and derive Ethereum collateral keys from a canonical byte representation.

8.2. Medium Findings

[M-01] : Verified Position Owner Can Differ From Mint Owner

Location:

- api.rs#L650-L664

Description : The signer validates the vault using the position owner, but signs a different Ethereum owner provided by the caller. As a result, honest signers may authorize collateral for an owner that does not match the verified position.

Recommendation: Derive the Ethereum owner from the verified position and reject any separately supplied owner value.

[M-02] : Stamp Storage Can Be Poisoned With Another Position

Location:

- http.rs#L302-L345
- store.rs#L698-L735

Description : The guardian endpoints validate the owner without verifying that the provided position is actually associated with that owner. As a result, an attacker can submit a valid stamp for a different position. The attester then stores the first stamp permanently, preventing the rightful owner from submitting or replacing it.

Recommendation: Verify the binding between the position and the owner before signing or storing a stamp.

[M-03] : Claims Across Multiple Vaults Cannot Be Settled by the Frontend

Location:

- use-pending-withdrawal.ts#L42-L65
- Reserve.sol#L640-L691

Description
A withdrawal claim may span multiple collateral NFTs. The frontend displays each NFT allocation as a separate pending claim and settles only a single root. As a result, valid multi-vault claims cannot be completed through the standard flow and remain locked until recovery or expiry.

Recommendation: Group withdrawals by claim ID and settle all encumbered NFTs using the authoritative claim amount.

[M-04] : Unauthenticated Prepare Requests Can Consume Ceremony Sessions

Location:

- proxy.ts#L14-L27
- ceremony.rs#L1621-L1673

Description: Same-origin ceremony routes forward authenticated member mutations without verifying control of the position. An attacker can submit a valid, conflicting `prepare` request before the legitimate owner. The first accepted request permanently reserves the session, allowing the attacker to block the owner's ceremony.

Recommendation: Require the position owner to sign the route, request body digest, and nonce before reserving or mutating member state.