Propchain

SMART CONTRACTS REVIEW

Summary Version

zokyo

August 8th 2025 | v. 1.0

Security Audit Score

PASS

Zokyo Security has concluded that this smart contract passed a security audit.

ZOKYO AUDIT SCORING PROPCHAIN

1. Severity of Issues:
    - Critical: Direct, immediate risks to funds or the integrity of the contract. Typically, these would have a very high weight.
    - High: Important issues that can compromise the contract in certain scenarios.
    - Medium: Issues that might not pose immediate threats but represent significant deviations from best practices.
    - Low: Smaller issues that might not pose security risks but are still noteworthy.
    - Informational: Generally, observations or suggestions that don't point to vulnerabilities but can be improvements or best practices.
2. Test Coverage: The percentage of the codebase that's covered by tests. High test coverage often suggests thorough testing practices and can increase the score.
3. Code Quality: This is more subjective, but contracts that follow best practices, are well-commented, and show good organization might receive higher scores.
4. Documentation: Comprehensive and clear documentation might improve the score, as it shows thoroughness.
5. Consistency: Consistency in coding patterns, naming, etc., can also factor into the score.
6. Response to Identified Issues: Some audits might consider how quickly and effectively the team responds to identified issues.

SCORING CALCULATION:

Let's assume each issue has a weight:
- Critical: -30 points
- High: -20 points
- Medium: -10 points
- Low: -5 points
- Informational: 0 points

Starting with a perfect score of 100:
- 0 Critical issues: 0 points deducted
- 1 High issue: 1 resolved = 0 points deducted
- 6 Medium issues: 6 resolved = 0 points deducted
- 2 Low issues: 2 resolved = 0 points deducted
- 0 Informational issues: 0 points deducted

Thus, the score is 100

TECHNICAL SUMMARY

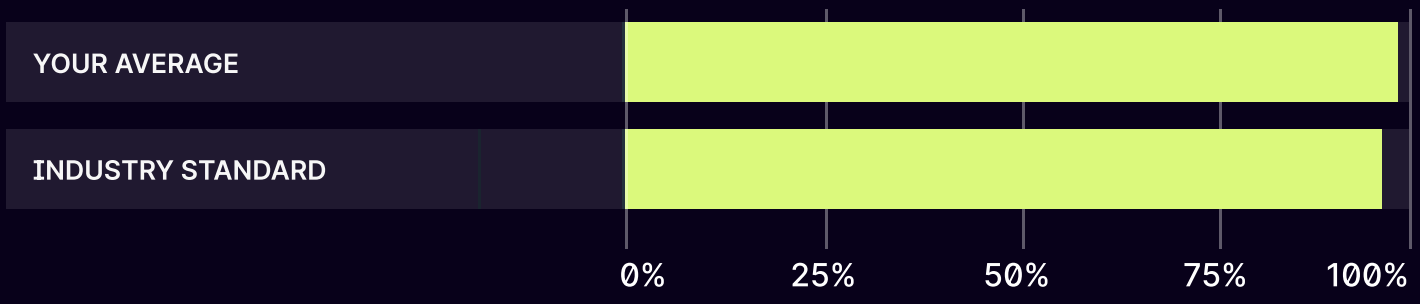
This document outlines the overall security of the Propchain smart contract/s evaluated by the Zokyo Security team.

The scope of this audit was to analyze and document the Propchain smart contract/s codebase for quality, security, and correctness.

Contract Status

There were 0 critical issues found during the review. (See Complete Analysis)

Testable Code



98,21% of the code is testable, which is above the industry standard of 95%.
The current version of the report is simplified. The full version is available upon request.

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract/s but rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that can withstand the Ethereum network's fast-paced and rapidly changing environment, we recommend that the Propchain team put in place a bug bounty program to encourage further active analysis of the smart contract/s.

Table of Contents

AUDITING STRATEGY AND TECHNIQUES APPLIED

The source code of the smart contract was taken from the Propchain repository:
Repo: https://github.com/propchain-global/propchain-solidity-contracts-new

Last commit - 873dd7f9e384b6327ee001c9db0ba7f499e65518

Within the scope of this audit, the team of auditors reviewed the following contract(s):

- PropchainStakingV3.sol

During the audit, Zokyo Security ensured that the contract:

- Implements and adheres to the existing standards appropriately and effectively;
- The documentation and code comments match the logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices, efficiently using resources without unnecessary waste;
- Uses methods safe from reentrance attacks;
- Is not affected by the most recent vulnerabilities;
- Meets best practices in code readability, etc.

Zokyo Security has followed best practices and industry-standard techniques to verify the implementation of Propchain smart contract/s. To do so, the code was reviewed line by line by our smart contract developers, who documented even minor issues as they were discovered. Part of this work includes writing a test suite using the Foundry testing framework. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

01	Due diligence in assessing the overall code quality of the codebase.
02	Cross-comparison with other, similar smart contract/s by industry leaders.
03	Testing contract/s logic against common and uncommon attack vectors.
04	Thorough manual review of the codebase line by line.

Executive Summary

Propchain is revolutionising the defi landscape by introducing on chain real estate for users. Zokyo was tasked with auditing the PropchainStakingV3 contract, which can be seen as digital saving accounts which allows the users to lock up tokens and earn rewards for keeping them locked. Users are able to choose three different lock periods, short term staking which involves a 6 month lock period, mid term which is 12 months and longer term staking which will incur a 24 month lock period. Penalties for early withdrawal are 2%, 5% and 10% respectively.

Overall the code is well engineered and well thought out in order to achieve the goals of the users and the contract administrators. Issues found ranged from High in severity down to Low. These issues were mostly resolving around the boundaries which should've been implemented and edgecases around the migration functionality.

The security team at Zokyo recommends that the protocol team carefully checks the issues and implements the suggested fixes to which a fix review will occur to check these fixes and ensure that they do not introduce any further issues into the code.

The current version of the report is simplified. The full version is available upon request.

STRUCTURE AND ORGANIZATION OF THE DOCUMENT

For the ease of navigation, the following sections are arranged from the most to the least critical ones. Issues are tagged as “Resolved” or “Unresolved” or “Acknowledged” depending on whether they have been fixed or addressed. Acknowledged means that the issue was sent to the Propchain team and the Propchain team is aware of it, but they have chosen to not solve it. The issues that are tagged as “Verified” contain unclear or suspicious functionality that either needs explanation from the Client or remains disregarded by the Client. Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

Critical

The issue affects the contract in such a way that funds may be lost, allocated incorrectly, or otherwise result in a significant loss.

High

The issue affects the ability of the contract to compile or operate in a significant way.

Medium

The issue affects the ability of the contract to operate in a way that doesn’t significantly hinder its behavior.

Low

The issue has minimal impact on the contract’s ability to operate.

Informational

The issue has no impact on the contract’s ability to operate.

COMPLETE ANALYSIS

FINDINGS SUMMARY

#	Title	Risk	Status
1	Staked Amount Accrues Rewards Even After End Time	High	Resolved
2	Users Might Be Unintentionally Blocked From Using migrateWithdrawAll()	Medium	Resolved
3	totalClaimedRewards Not Updated On migrateWithdrawAll	Medium	Resolved
4	Insufficient Validation On cleanupCheckpoints Will Cause Rewards To be Deleted	Medium	Resolved
5	Platform Administrators Can Set Unreasonable Penalty Rates Which Apply Immediately And Therefore Rug The Users Of Their Principle	Medium	Resolved
6	Users Can Backrun Admin Calls To disableMigrationMode To Avoid Paying Penalties	Medium	Resolved
7	userMigrationCursor Not Being Reset After Withdrawing From All Pools Leads To User Not Being Able To Withdraw In The Next Migration	Medium	Resolved
8	If Certain Edge Cases Involving The rewardsWallet Are Met, Users May Not Be Able To Withdraw From The Staking Contract	Low	Resolved
9	Insufficient Checks In setInitialPenaltyBps	Low	Resolved

We are grateful for the opportunity to work with the Propchain team.

The statements made in this document should not be interpreted as an investment or legal advice, nor should its authors be held accountable for the decisions made based on them.

Zokyo Security recommends the Propchain team put in place a bug bounty program to encourage further analysis of the smart contract by third parties.

zokyo