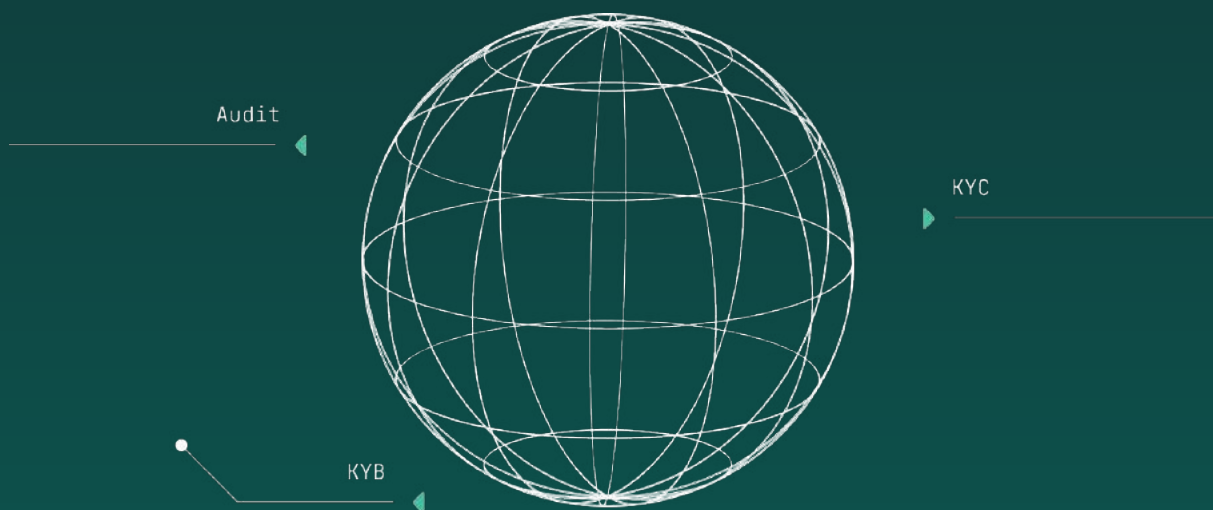




# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



CUSTOMER: COPIN.IO - DCP SYNTHETIX  
DATE: Mar 13th, 2024



## DISCLAIMERS

### **DAudit Disclaimer**

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or print and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

The smart contracts submitted for audit were examined in accordance with best industry practices at the time of this report in terms of cybersecurity vulnerabilities and issues in smart contract source code, which are detailed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no claims or guarantees about the code's security. It also cannot be deemed an adequate appraisal of the code's utility and safety, bug-free status, or any other contractual assertions. While we did our best in completing the study and generating this report, it is crucial to emphasize that you should not rely only on this report; we advocate doing many independent audits and participating in a public bug bounty program to assure smart contract security.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed

### **Technical Disclaimer**

Smart Contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed – upon a decision of the Customer.

## DOCUMENT

Name	Smart contract code review and security analysis report for Copin
Audit Team	DAudit.org team
Type	Smart contract
Platform	Optimism / Solidity
Methods	Architecture Review, Functional Testing, Manual Review
Repository	<a href="https://github.com/copin-protocol/onchain-copytrading/tree/snx-v2">https://github.com/copin-protocol/onchain-copytrading/tree/snx-v2</a>
Commit	8e5cd84df55d561185e4d638bc44b27280772c38
Deployed Contract	<a href="#">0xB27A14Fa98608A95d81C22023F09648f2Cb714C2</a> <a href="#">0x88680E90D1Bcb8Bf1AD5cd0F65f99851803F9A04</a> <a href="#">0xf608A4c1BADd8367C0D7A186923fe07AC2C018Fb</a> <a href="#">0x6c0D18C82E5AACAc466889bF433f766cd54281e1</a> <a href="#">0xa29314DB1D3b8705B74482775210a2f702a9f970</a>
JS tests	No
Website	<a href="https://app.copin.io/">https://app.copin.io/</a>
Timeline	Mar 06th, 2024
Changelog	Mar 12th, 2024 - Initial audit

# Table Of Content

Disclaimer.....	.....2
Introduction.....	.....5
Scope.....	.....5
Executive Summary....	.....7
Audit overview.....	.....9
Conclusion.....	.....10

## INTRODUCTION

DAudit.org (Consultant) was contracted by Copin.io (Customer) to conduct a Smart Contract Code Review and Security Analysis. Copin (Customer) hired DAudit.org (Consultant) to do a Smart Contract Code Review and Security Analysis. This report details the conclusions of the Customer's smart contract security assessment and code review, which took place on Mar 06th, 2024.

## SCOPE

The scope of the project is smart contracts in the repository:

### Repository:

<https://github.com/copin-protocol/onchain-copytrading/tree/snx-v2>

### Commit:

8e5cd84df55d561185e4d638bc44b27280772c38

### JS tests: No

### Contracts:

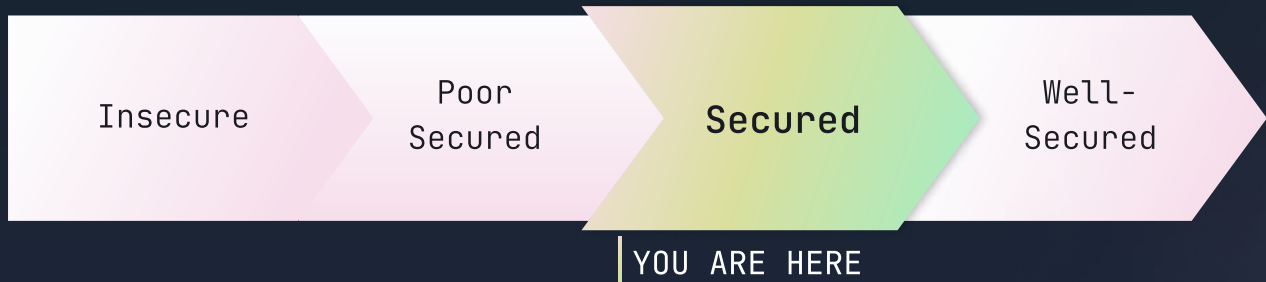
Factory.sol  
Config.sol  
Events.sol  
TaskCreator.sol  
CopyWalletProxy.sol  
core/CopyWallet.sol  
CopyWalletSNXv2.sol

We have scanned this smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check items
Code review	<ul style="list-style-type: none"> <li>▪ Reentrancy</li> <li>▪ Ownership Takeover</li> <li>▪ Timestamp Dependence</li> <li>▪ Gas Limit and Loops</li> <li>▪ DoS with (Unexpected) Throw</li> <li>▪ DoS with Block Gas Limit</li> <li>▪ Transaction-Ordering Dependence</li> <li>▪ Style guide violation</li> <li>▪ Costly Loop</li> <li>▪ Unchecked external call</li> <li>▪ Unchecked math</li> <li>▪ Unsafe type inference</li> <li>▪ Implicit visibility level</li> <li>▪ Deployment Consistency</li> <li>▪ Repository Consistency</li> <li>▪ Data Consistency</li> </ul>
Functional review	<ul style="list-style-type: none"> <li>▪ Business Logics Review</li> <li>▪ Functionality Checks</li> <li>▪ Access Control &amp; Authorization</li> <li>▪ Escrow manipulation</li> <li>▪ Token Supply manipulation</li> <li>▪ Assets integrity</li> <li>▪ User Balances manipulation</li> <li>▪ Data Consistency manipulation</li> <li>▪ Kill-Switch Mechanism</li> <li>▪ Operation Trails &amp; Event Generation</li> </ul>

## EXECUTIVE SUMMARY

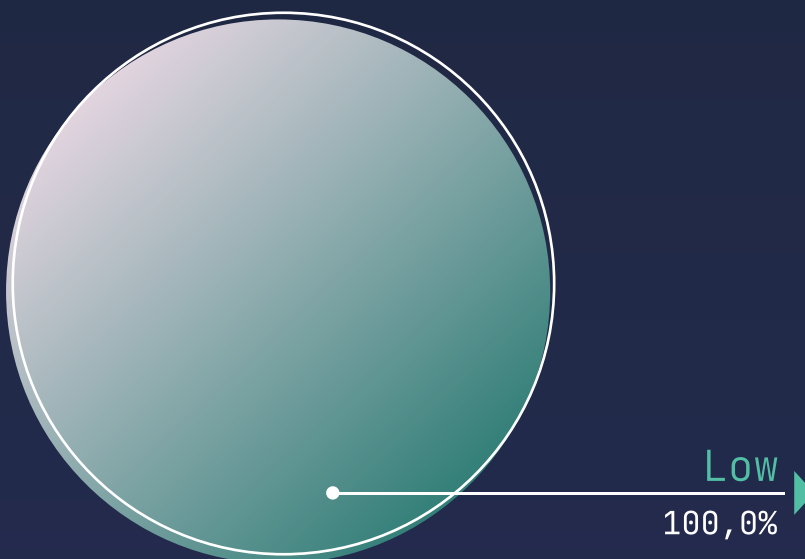
According to the assessment, the Customer's smart contracts are well-secured.



With Mythril, SmartCheck, Solgraph, and Slither, DAudit did a code analysis, manual audit, and automated checks. All concerns discovered during automated analysis were carefully examined, and the Audit summary section contains critical vulnerabilities. The audit summary section contains a list of all problems discovered.

Security engineers discovered one low-severity problems as a result of the audit.

Graph 1. The distribution of vulnerabilities after the audit.



## Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to asset loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to asset loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.



## AUDIT OVERVIEW

### Critical



► 02 critical issues were found.

### High



► No high issues were found.

### Medium



► No medium issues were found.

### Low



► 01 low issue was found.

## AUDIT DETAIL

### Critical



#### 1. Owner can set executor fee and protocol fee without limited

- Contract: Config.sol
- Function: setExecutorFee, setProtocolFee
- Description: Configuring fees without limitations could potentially harm users if the set fee exceeds the usual usage fee.
- Solution: It is advisable to add a feature to limit the maximum fee that can be set. This maximum limit could be set by the platform, government regulations, and should be transparent to all users.



#### 2. The market whitelist address, when set, should be verified to ensure its functionality is currently operational or not.

- Contract: Config.sol
- Function: setTokenWhitelistStatus
- Description: Setting the market whitelist address without verifying if it corresponds to the actual market contract may lead to inadvertently setting a contract with different functionality.
- Solution: It's advisable to add a verification step to ensure that the market whitelist address set corresponds to the correct trading contract and that this contract is currently operational.



## AUDIT DETAIL

Low



1. The fee receiver address should not be zero address or dead address.

- Contract: Config.sol
- Function: setFeeReceiver
- Description: Setting the fee receiver should not be zero dead to avoid fee loss due to incorrect setting
- Solution: Should add a check to see if the address is zero address or dead address



THIS ISSUE IS FIXED

DECENTRALAB PTE.LTD.

160 Robinson Road, #14-04 Singapore  
Singapore (068914)  
support@daudit.org



## CONCLUSION

SMART CONTRACTS WITHIN THE SCOPE WERE MANUALLY REVIEWED AND ANALYZED WITH STATIC ANALYSIS TOOLS.

THE AUDIT REPORT CONTAINS ALL FOUND SECURITY VULNERABILITIES AND OTHER ISSUES IN THE REVIEWED CODE.

AS A RESULT OF THE AUDIT, SECURITY ENGINEERS FOUND 02 CRITICAL SEVERITY ISSUES AND 01 LOW SEVERITY ISSUE.

AFTER RESPONDING TO THE CLIENT AND CONSULTING, THESE ISSUES HAVE BEEN FIXED.