QuillAudits

AUDIT REPORT

March, 2025

For

Zynk Labs

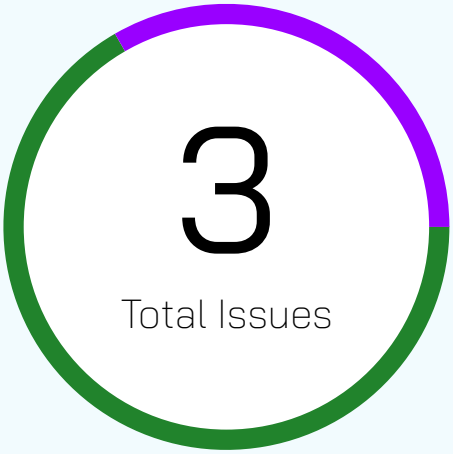
Table of Content

Executive Summary

Project name	Zynk Labs
Project URL	https://www.zynklabs.xyz/
Overview	The Zynk Protocol is a token transfer and repayment system that facilitates sending tokens between operators and partners. The protocol enables an operator (zynk_op_wallet) to send tokens to a partner's operational wallet while recording the partner's deposit wallet for future repayments. Partners can then replenish tokens by transferring them from their deposit wallet to a designated payback wallet. Each transaction is tracked through unique order IDs, and multiple repayments can be made against a single order. The protocol includes administrative controls for wallet updates, emergency pausing, and order closure.
Audit Scope	The scope of this Audit was to analyze the Zynk Smart Contracts for quality, security, and correctness.
Source Code link	https://github.com/MasterAtWork/zynk-solana-contract/blob/main/zynk_protocol/contracts/programs/zynk-protocol/src/lib.rs
Contracts in Scope	lib.rs
Branch	main
Commit Hash	d240cbe1433e90c519bff5576f62241f7f050e26
Language	Rust

Blockchain	Solana
Method	Manual Analysis, Functional Testing, Automated Testing
Review 1	20th March 2025 - 24th March 2025
Updated Code Received	27th March 2025
Review 2	27th March 2025 - 28th March 2025
Fixed In	17bf202fc44654b6259d08502910d1d07059af72

Number of Issues per Severity



High	0 (0.00%)
Medium	0 (0.00%)
Low	2 (66.67%)
Informational	1 (33.33%)

Severity

Issues	High	Medium	Low	Informational
Open	0	0	0	0
Resolved	0	0	**2**	**1**
Acknowledged	0	0	0	0
Partially Resolved	0	0	0	0

Checked Vulnerabilities

- ☑ Signer authorization
- ☑ Account data matching
- ☑ Sysvar address checking
- ☑ Owner checks
- ☑ Type cosplay
- ☑ Initialization
- ☑ Arbitrary cpi
- ☑ Duplicate mutable accounts
- ☑ Bump seed canonicalization
- ☑ PDA Sharing
- ☑ Incorrect closing accounts
- ☑ Missing rent exemption checks
- ☑ Arithmetic overflows/underflows
- ☑ Numerical precision errors
- ☑ Solana account confusions
- ☑ Casting truncation
- ☑ Insufficient SPL token account verification
- ☑ Signed invocation of unverified programs.

Techniques and Methods

Throughout the audit of Solana Programs, care was taken to ensure:

- The overall quality of code.
- Use of best practices
- Code documentation and comments, match logic and expected behavior
- Token distribution and calculations are as per the intended behavior mentioned in the whitepaper
- Implementation of ERC standards
- Efficient use of gas
- Code is safe from re-entrancy and other vulnerabilities

The following techniques, methods, and tools were used to review all the smart contracts:

Structural Analysis

In this step, we have analysed the design patterns and structure of Solana programs. A thorough check was done to ensure the Solana program is structured in a way that will not result in future problems.

Static Analysis

Static analysis of Solana programs was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of Solana programs.

Techniques and Methods

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analysed, and their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption

In this step, we have checked the behaviour of Solana programs in production. Checks were done to know how much gas gets consumed and the possibilities of optimising code to reduce gas consumption.

Types of Severity

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below

High Severity Issues

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational Issues

These are four severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

Security vulnerabilities identified that must be resolved and are currently unresolved.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/ impact of the security issue, but are not completely resolved.

Low Severity Issues

Absence of null address validity check

Resolved

Path

lib.rs

Function

update_zynk_op_wallet, update_payback_wallet, transfer_admin

Description

This function allows for the admin to update critical addresses in the function yet fails to ensure that a null address is not made one of these addresses.

Recommendation

Add validate_address function to prevent null address being set.

Multiple config account vulnerability due to missing PDA constraints

Resolved

Path

lib.rs

Function

Config

Description

The Config account is initialized as a regular account rather than a program derived address (PDA). The current implementation allows for the creation of multiple Config accounts. The absence of PDA constraints means any address can be used to create a Config account, as long as it's signed by an admin.

Recommendation

Modify the Config account to use a PDA with a known seed so only one singleton account can be created.

Informational Severity Issues

Remove unused error message

Resolved

Description

All other error messages where used for appropriate error handling however, there is one declared but was not used in the program.

Recommendation

Remove any error message not used in the program.

Functional Tests

Some of the tests performed are mentioned below:

- Should create multiple config account
- Should update relevant addresses to Pubkey default value
- Should check that execution is impossible when paused by admin

Automated Tests

No major issues were found. Some false positive errors were reported by the tools. All the other issues have been categorized above according to their level of severity.

Closing Summary

In this report, we have considered the security of Zynk Labs. We performed our audit according to the procedure described above.

issues of Low and Informational severity issues were found.

Disclaimer

At QuillAudits, we have spent years helping projects strengthen their smart contract security. However, security is not a one-time event—threats evolve, and so do attack vectors. Our audit provides a security assessment based on the best industry practices at the time of review, identifying known vulnerabilities in the received smart contract source code.

This report does not serve as a security guarantee, investment advice, or an endorsement of any platform. It reflects our findings based on the provided code at the time of analysis and may no longer be relevant after any modifications. The presence of an audit does not imply that the contract is free of vulnerabilities or fully secure.

While we have conducted a thorough review, security is an ongoing process. We strongly recommend multiple independent audits, continuous monitoring, and a public bug bounty program to enhance resilience against emerging threats.

Stay proactive. Stay secure.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem

7+ Years of Expertise	**1M+** Lines of Code Audited
$30B+ Secured in Digital Assets	**1400+** Projects Secured

Follow Our Journey

AUDIT REPORT

March, 2025

For

Zynk Labs

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com audits@quillaudits.com