HACKEN Request an audit

Hacken → Audits → Zenqira → [SCA] Zenqira / Zenqira-Contracts / Feb2025

Zenqira

Audit name:
[SCA] Zenqira / Zenqira-Contracts / Feb2025

Date:
Feb 25, 2025

Table of Content

View Report

Introduction

We express our gratitude to the Zenqira team for the collaborative engagement that enabled the execution of this Smart Contract Security Assessment.

Zenqira democratizes AI by connecting global computing power with innovators, enabling efficient resource sharing and rewarding participants through its native ZENQ token.

Document

Name

Smart Contract Code Review and Security Analysis Report for Zenqira

Audited By

Adam Idarrha

Approved By

Oleksii Haponiuk

Website

https://zenqira.com/

Changelog

26/02/2025 – Preliminary Report

26/02/2025 – Final Report

Platform

Binance Smart Chain

Language

Solidity

Tags

ERC20, Fungible Token

Methodology

https://hackenio.cc/sc_methodology

Review Scope

Repository

No repository. Contracts deployed on BSC (0x6c067f39cd81067d63718a5186ad4b3866318adc)

Commit

N/A

View Full Scope →

Audit Summary

0
Total Findings

0
Resolved

0
Accepted

0
Mitigated

The system users should acknowledge all the risks summed up in the risks section of the report

Documentation quality

- Functional requirements are missed.
- Technical description is provided.

Code quality

- The code follows the Solidity Style Guide.

Test coverage

- Tests are not required for projects below 250 LoC.

System Overview

ZENQ — simple ERC-20 token that mints all initial supply to a deployer. Additional minting is not allowed.

It has the following attributes:

- Name: ZENQIRA
- Symbol: ZENQ
- Decimals: 18
- Total supply: 500m tokens.

Privileged roles

- The contract has no privileged roles.

Potential Risks

ⓘ **Centralization risk:** The project concentrates minting tokens in a single address of the deployer, raising the risk of fund mismanagement or theft, especially if key storage security is compromised.

Findings

No vulnerabilities were found

Appendix 1. Definitions

Severities

When auditing smart contracts, Hacken is using a risk-based approach that considers **Likelihood**, **Impact**, **Exploitability** and **Complexity** metrics to evaluate findings and score severities.

Reference on how risk scoring is done is available through the repository in our Github organization:

hknio/severity-formula

Severity

Critical

Description

Critical vulnerabilities are usually straightforward to exploit and can lead to the loss of user funds or contract state manipulation.

Severity

High

Description

High vulnerabilities are usually harder to exploit, requiring specific conditions, or have a more limited scope, but can still lead to the loss of user funds or contract state manipulation.

Severity

Medium

Description

Medium vulnerabilities are usually limited to state manipulations and, in most cases, cannot lead to asset loss. Contradictions and requirements violations. Major deviations from best practices are also in this category.

Severity

Low

Description

Major deviations from best practices or major Gas inefficiency. These issues will not have a significant impact on code execution.

Potential Risks

The "Potential Risks" section identifies issues that are not direct security vulnerabilities but could still affect the project’s performance, reliability, or user trust. These risks arise from design choices, architectural decisions, or operational practices that, while not immediately exploitable, may lead to problems under certain conditions. Additionally, potential risks can impact the quality of the audit itself, as they may involve external factors or components beyond the scope of the audit, leading to incomplete assessments or oversight of key areas. This section aims to provide a broader perspective on factors that could affect the project's long-term security, functionality, and the comprehensiveness of the audit findings.

Appendix 2. Scope

The scope of the project includes the following smart contracts from the provided repository:

Scope Details

Repository

No repository. Contracts deployed on BSC (0x6c067f39cd81067d63718a5186ad4b3866318adc)

Commit

N/A

Whitepaper

https://zenqira.com/

Requirements

N/A

Technical Requirements

N/A

Assets in Scope

zenqira.sol - `zenqira.sol`

Disclaimer

Hacken Disclaimer

Technical Disclaimer

CERTIFIED

TRUST ARMY

EXTRACTOR

HackenProof