HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: NepNomad
Date: June 13th, 2022

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Document

Name	Token tokenomics audit for NeoNomad.
Approved By	Evgeniy Bezuglyi | SC Department Head at Hacken OU
Type	Solana SPL token; Staking
Platform	Solana
Language	Rust
Methods	Manual Review, General Morphological Analysis (GMA)
Website	https://www.neonomad.finance/
Timeline	02.06.2022 - 13.06.2022
Changelog	13.06.2022 - Initial Review

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Table of contents

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Introduction

Hacken OÜ (Consultant) was contracted by NeoNomad to conduct a Token Tokenomics Audit and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contracts.

Scope

The scope of the project is token tokenomics audit in the documentation:

Initial review scope
NNI token address:
https://explorer.solana.com/address/buMnhMd5xSyXBssTQo15jouu8VhuEZJCfbtBUZgRcuW
Documentation: Yes
https://docs.neonomad.finance/neonomad-documentation/defi-tutorials/staking-step-by-step-guide
Technical Documentation: Yes
https://hacken.atlassian.net/jira/software/projects/SA/boards/3?label=rust%2Cwasm&selectedIssue=SA-181
JS tests: Yes
Contracts: neonomad/src/*

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets 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 cannot lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that cannot have a significant impact on execution

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Executive Summary

The score measurement details can be found in the corresponding section of the methodology.

Documentation quality

The Customer provided functional documentation without staking smart contracts. Documentation is not complete. The total Documentation Quality score is **7** out of **10**.

Security score

As a result of the audit, the code contains **1** medium, and **1** low severity issues. The security score is **9** out of **10**.

All found issues are displayed in the “Findings” section.

Summary

According to the assessment, the Customer's smart contract has the following score: **9.3**

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Checked Items

We have audited provided tokenomics for commonly known and more specific categories. Here are some of the items that are considered:

Item	Description	Status
Incentive Theory in Token Economics	The model of operations in the token economy should be configured for enabling participants to earn more tokens by contributing positively. In this case, tokenomics ensures that token incentives are financial, owing to their financial value and contribution to an overall market capitalization of a project.	Passed
Significance of Tokens	The structure of tokens could be classified into three types: Layer 1 and Layer 2 tokens or Layer 0.	Passed
Token distribution	Projects should have the ability to distribute coins to potential users.	Failed
Unlock token schedule	The project should have a transparent lock-up schedule for Team/ Advisors/ Private/ Seed members.	Passed
Business Scope	The basic utility of a token depends on its utility in return for the products and services it serves.	Passed
Price stability	Token economics could support an increase in token prices through growth in demands.	Passed
Token economics Use Cases	Use cases define the direction of tokenomics price evaluation.	Passed
Token market capitalization	The market cap is a strong predictor of the token's worth. As a result, small-cap cryptocurrencies are riskier.	Passed
Inflationary/deflationary pressure	Inflationary tokens have no limit supply, and may be mined endlessly. Deflationary tokens have a token supply that is limited to the maximum supply. As a result, deflationary tokens are excellent for token price. Inflationary tokens do an excellent job of motivating network validators, miners.	Passed
Max/total/initial / circulation supply	How many tokens will be in the system, and how many tokens are in the system right now?	Passed
Emission and burn rate	There is no clear documentation for analyzing this metric.	Failed

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Tokenomics Overview

NNI tokenomics describes coin distribution allocation proportion. Neonomad tokenomics provides general information about emission and burn rate and provides a detailed token distribution model with lock-ups and vesting schedule for all pools such as Private, Public, Team, Marketing/Dev Advisors pools. Tokenomics contains useful information about NNI Funds distribution to Payment Service, AgDefi, MinDefi and platform/ development/ marketing purposes .

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Findings

Critical

No critical severity issues were found.

High

No critical severity issues were found.

Medium

1. **Token Distribution Address.**

   Currently, NNI tokens are in an individual wallet address.

   Recommendation: Each token allocation can have its own wallet.

   Status: New

Low

1. **Emission and burn rate.**
   There is no clear documentation for analyzing emission and burn rate

   Recommendation: Provide more details and examples of how emission and burn rate are calculated.

   Status: New

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed by the best industry practices at the date of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on the security of the code. It also cannot be considered a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

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 cannot guarantee the explicit security of the audited smart contracts.