

# Advance Audit Report **Harvest**

April 8, 2024

Network: BASE





Address: 0x486c3fb721c7faa426d4e68d7769b4427f86a7d9

Audited by ©NeonAI

## Global Overview








### Generated Code Review

In this audit report we will highlight the following issues:

Vulnerability Level	Total	Pending	Acknowledged	Resolved
 Informational	0	0	0	0
 Low-Risk	0	0	0	0
 Medium-Risk	0	0	0	0
 High-Risk	0	0	0	0

### Centralization Risks

NeonAI checked the following privileges:

Contract Privilege	Description
Owner needs to enable trading?	 Owner does not need to enable trading
Owner can mint?	 Owner cannot mint new tokens
Owner can blacklist?	 Owner cannot blacklist addresses
Owner can set fees?	 Owner cannot set the fees
Owner can exclude from fees?	 Owner cannot exclude from fees
Can be honeypotted?	 Token is sellable, no honeypot risk detected.
Owner can set Max TX amount?	 Owner cannot set maximum transaction amount

More owner privileges are listed later in the report.

# Table of Contents

## **1. Audit Summary**

- 1.1 Audit Overview
- 1.2 Risk Classification

## **2. Token Ecosystem Analysis**

- 2.1 Maximum Fee Limit Check
- 2.2 Pool Analysis
- 2.2 Holder Overview

## **3. Smart Contract Vulnerability Assessment**

- 3.1 SWC Attack Analysis

## **4. Summary**

## **5. Disclaimer**

## Audit Summary

Contract Name	Harvest
Symbol	HVR
Created At	2024-02-19
Contract Address	0x486c3fb721c7faa426d4e68d7769b4427f86a7d9
ChainId	8453
Decimals	18
Max Supply Cap	20,000,000
Audit date	April 8, 2024

## Pre-launch Audit Status

Approved

This report has been meticulously crafted by NeonAI's specialized team upon the client's request. Herein, we delineate the outcomes of both static analysis and comprehensive manual code examination. The audit's core objective is to validate the contract's functionality against its intended design and pinpoint any security vulnerabilities inherent within the smart contract's architecture.

This document serves as a critical resource for understanding the potential risks posed by the smart contract. It also offers strategic insights for the development team, guiding them on enhancing the contract's robustness by addressing the identified concerns.

## Audit Overview

NeonAI was commissioned by Harvest to conduct an audit based on the following code:

<https://basescan.org/token/0x486c3fb721c7faa426d4e68d7769b4427f86a7d9#code>

Please note that this audit was performed on the code accessible at the provided URL at the audit time. If the link does not lead to a main net block explorer, the content of the code might have changed. Always verify the contract address in this audit report against the token you're researching.

## NeonAI's Multi-Layered Audit Approach

Our audit process is designed to comprehensively evaluate the smart contract's security posture. Here's an overview of the methodologies employed.

### In-Depth Review

NeonAI's security AI meticulously examines the smart contract code line-by-line. This deep dive allows us to identify potential vulnerabilities, understand coding decisions within the broader context, and consider the developer's intent and the overall business logic. These are factors that automated tools might miss in general.

### AI-Powered Vulnerability Detection





We leverage premium AI tools to scan the code for common smart contract vulnerabilities like integer overflows, underflows, out-of-gas errors, and unvalidated transfers. This helps expedite the identification of potential issues.

### Tools Utilized

- BASE for blockchain analysis
- Remix: The Integrated Development Environment tool
- CWE: Common Weakness Enumeration for standardizing vulnerabilities
- SWC: Smart Contract Weakness Classification and Test Cases for identifying specific smart contract vulnerabilities

## Risk Classification

NeonAI assesses smart contracts through certain risk levels. The risk levels indicate how good or bad certain factors within a smart contract are. A lower risk level indicates a safer investment, while higher risk levels recommend corrections to the factors assessed before using the contract or before investing.

Vulnerability Level	Description
 Informational	Does not compromise the functionality of the contract in any way
 Low-Risk	Won't cause any problems, but can be adjusted for improvement
 Medium-Risk	Will likely cause problems and it is recommended to adjust
 High-Risk	Will definitely cause problems, this needs to be adjusted

NeonAI has three statuses that are used for each risk level. Below you will find brief explanations to each risk level.

Risk Status	Description
<b>Low-Risk</b>	Total amount of issues within this category
<b>Pending</b>	Risks that have yet to be addressed by the team
<b>Resolved</b>	The team has resolved and remedied the risk
<b>Acknowledged</b>	The team is aware of the risks but does not resolve them

## Maximum Fee Limit Check

Exploit	Description
---------	-------------

No exploits have been found.

NeonAI evaluates whether the smart contract's owner can set transfer, purchase, or sell fees exceeding 25%. Fees this high are considered poor practice because they can hinder or even halt trading activity, preventing a fair and active market.

Type of fee	Description
-------------	-------------

Max Tax Simulated Fee	0.00%
-----------------------	-------

Max Buy fee	N/A%
-------------	------

Max Sell fee	N/A%
--------------	------

## Pool Analysis

There are several steps to NeonAI's Liquidity Pool Analysis. In the first step, Pool Identification, the analysis identifies the different liquidity pools associated with the token contract. It looks for pools on various Decentralized Exchanges (DEXs) such as, for example, Uniswap.

Pool Attribute	Description
Initial Liquidity Provided	The initial pool value is Initial liquidity not found .
Liquidity Lock Status	● Liquidity is not found.
Liquidity Lock Date	The liquidity doesn't seem to exist at the moment.
Swap Fee	Swap fee is set at a standard rate of 0.3%
Direct BASE Support	Yes, the pool supports direct BASE swaps
Automated Market Making	Yes, the pool utilizes automated market making
Liquidity Pool Pair	none
Liquidity Provider	none
Pair Address	none

Further details on pool attributes and functionalities are elaborated on in subsequent sections of this report.



## Holder Overview

We incorporate a comprehensive Holder Overview through our Top Holder analysis. This critical assessment identifies the key stakeholders in the token ecosystem by quantifying their token holdings. Utilizing data directly from the BASE blockchain, our methodology encompasses data acquisition from the BASE network, precise wallet identification, and meticulous balance calculation for each wallet.

Wallet Address	Percentage of supply held
1. 0x3bf6468a010467de2c02b96cef2f2cb889779998	<div></div> 95.00%
2. 0xcb8bbb6abaf4e16b6c585ec1051e4cb91b89d04a	<div></div> 4.00%

Following the enumeration of the top 10 holders, it's crucial to acknowledge their pivotal role and influence within the token's ecosystem, highlighting the dynamics that shape the token's distribution and market behavior.

## SWC Attack Analysis

Here is the SWC attack analysis for the provided Harvest ERC20 token contract:

### SWC-102 Outdated Compiler Version

The contract is using a recent version of Solidity (0.8.23). It is not susceptible to outdated compiler issues.

### SWC-103 Floating Pragma

The contract has a fixed pragma version `pragma solidity 0.8.23;`. It is not affected by the floating pragma vulnerability.

### SWC-104 Unchecked Call Return Value

The contract does not make any external calls. Thus, it is not vulnerable to unchecked call return values.

### SWC-105 Unprotected Ether Withdrawal

The contract does not have any functions that allow Ether withdrawal. It is not susceptible to unprotected Ether withdrawal.

### SWC-106 Unprotected SELFDESTRUCT Instruction

The contract does not have any `selfdestruct` instructions. It is not vulnerable to unprotected selfdestruct.

### SWC-107 Reentrancy

The contract does not have any external calls or state changes after transfers. It is not susceptible to reentrancy attacks.

### SWC-108 State Variable Default Visibility

All state variables in the contract have explicit visibility specifiers. There are no state variables with default visibility.

### SWC-113 DoS with Failed Call

The contract does not make any external calls. It is not vulnerable to DoS with failed call.

### SWC-115 Authorization through tx.origin

The contract does not use `tx.origin` for authorization. It is not affected by this vulnerability.

Overall, the Harvest ERC20 token contract follows best practices and does not exhibit any known vulnerabilities based on the provided SWC attack vectors. Harvest Haven: [Website](#) | [Twitter](#) | [Discord](#)

## Summary

The Harvest (HVR) project emerges on chainId 8453 as an innovative venture into the cryptocurrency domain, distinguished by its limited treasury of 20,000,000 HVR tokens. The project emphasizes transparency and commitment to authenticity, underscored by its verified contract address, 0x486c3fb721c7faa426d4e68d7769b4427f86a7d9. Enhanced transaction precision, enabled through an 18 decimal allocation, ensures a sophisticated handling of exchanges.

Initiated by a deployer at address 0x562a2b9177dd821caa073f18f669a121fd583508, Harvest has undergone extensive security and reliability testing. These evaluations rigorously explored aspects such as proxy contracts, pausable functions, minting capabilities, and transaction limitations, underscoring the project's comprehensive and robust framework. A key highlight is its fixed supply model, achieved by forgoing a mint function and fee modifiers, thus preserving the token supply from inflation or arbitrary fee changes.

Being in the pre-launch phase, the project's current token allocation, with 95% concentrated in a single wallet (address: 0x3bf6468a010467de2c02b96cef2f2cb889779998), is a preparatory measure rather than a risk indicator. This centralized holding facilitates initial project management and sets the stage for strategic distribution post-launch, aiming for a balanced token spread. The deployer's controlled stake of 200,000 HVR evidences a deliberate approach to prevent overwhelming initial governance influence.

Harvest promises robust liquidity, laying a solid foundation for its market introduction and instilling confidence in its financial mechanics. The project further advances towards decentralization and community-led governance through the renouncement of ownership, paving the way for an inclusive and participatory future.

Notably, the project's choice to exclude adjustable fees, transaction size limits, and blocklist features prioritizes contract simplicity and user experience. This strategic decision, while enhancing usability, necessitates careful navigation to balance simplicity with the flexibility needed for adapting to market dynamics or optimizing the economic model.

In summary, the Harvest project stands out for its transparent and verified operational framework. As it moves from pre-launch to active phases, stakeholders are encouraged to stay informed about the project's token distribution and governance strategies. Such insights are essential for evaluating the project's long-term viability and stability. Potential participants are advised to consider both the innovative aspects of Harvest and the strategic planning around token distribution, as these factors collectively influence the project's price stability, market liquidity, and governance framework moving forward.


## Disclaimer


The information provided in this report does not constitute investment, financial, or trading advice, and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to, or relied upon by any person for any purpose, nor may copies be delivered to any other person without NeonAI's prior written consent. This report should not be considered an "endorsement" or "disapproval" of any particular project or team. It does not provide any indication of the economics or value of any "product" or "asset" created by any team or project that contracts NeonAI to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor does it provide any indication of the technologies proprietors' business, business model, or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intended to help our clients improve the quality of their code while mitigating the high level of risk associated with cryptographic tokens and blockchain technology. However, it is important to note that blockchain technology and cryptographic assets inherently present a significant level of ongoing risk.


NeonAI's stance is that each company and individual is responsible for their own due diligence and continuous security measures. NeonAI's objective is to help reduce attack vectors and the high level of variance associated with utilizing new and constantly evolving technologies. We do not claim any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by NeonAI are subject to dependencies and are under continuous development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry high levels of technical risk and uncertainty. The assessment reports may include false positives, false negatives, and other unpredictable results. The services may access and depend upon multiple layers of third parties.


End of report

# Smart Contract Audit

 [t.me/NeonAlapp](https://t.me/NeonAlapp)

 [@neonaiapp](https://twitter.com/neonaiapp)

 [team@neonai.app](mailto:team@neonai.app)

 [neonai.app](https://neonai.app)