verichains

SECURITY AUDIT OF

HIMOWORLD STAKING POOL SMART CONTRACTS

Public Report

Feb 07, 2022

Verichains Lab

info@verichains.io

https://www.verichains.io

Driving Technology > Forward

ABBREVIATIONS

Name	Description
Ethereum	An open source platform based on blockchain technology to create and distribute smart contracts and decentralized applications.
Ether (ETH)	A cryptocurrency whose blockchain is generated by the Ethereum platform. Ether is used for payment of transactions and computing services in the Ethereum network.
Smart contract	A computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
Solidity	A contract-oriented, high-level language for implementing smart contracts for the Ethereum platform.
Solc	A compiler for Solidity.
ERC20	ERC20 (BEP20 in Binance Smart Chain or *x*RP20 in other chains) tokens are blockchain-based assets that have value and can be sent and received. The primary difference with the primary coin is that instead of running on their own blockchain, ERC20 tokens are issued on a network that supports smart contracts such as Ethereum or Binance Smart Chain.

EXECUTIVE SUMMARY

This Security Audit Report prepared by Verichains Lab on Feb 07, 2022. We would like to thank the HimoWorld for trusting Verichains Lab in auditing smart contracts. Delivering high-quality audits is always our top priority.

This audit focused on identifying security flaws in code and the design of the HimoWorld Staking Pool Smart Contracts. The scope of the audit is limited to the source code files provided to Verichains. Verichains Lab completed the assessment using manual, static, and dynamic analysis techniques.

During the audit process, the audit team had identified no vulnerable issue in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About HimoWorld Staking Pool Smart Contracts

Himo World is an NFT game with a Play-to-Earn feature, in which players can engage in battles with others, build their team to their favourite to explore the universe, or choose to become observers of the war. This game is also providing a true Free-to-Play experience, which a lot of other NFT games in the market is lacking at the moment. Setting up in a distant realm, the player just awoke his summoning power, and realize they now are in the middle of the war between realms, where they fight against each other in a battle of strengths and wits.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the HimoWorld Staking Pool Smart Contracts. It was conducted on the source code provided by the HimoWorld team.

The latest version of the following files were made available in the course of the review:

SHA256 Sum	File
77a2ca10001c1a9ca50c670c98c73490deedb92ce1bf8aac8eeab5c5d92bb069	staking/StakingPool.sol

1.3. Audit methodology

Our security audit process for smart contract includes two steps:

- Smart contract codes are scanned/tested for commonly known and more specific vulnerabilities using public and RK87, our in-house smart contract security analysis tool.
- Manual audit of the codes for security issues. The contracts are manually analyzed to look for any potential problems.

Following is the list of commonly known vulnerabilities that was considered during the audit of the smart contract:

- Integer Overflow and Underflow
- Timestamp Dependence
- Race Conditions
- Transaction-Ordering Dependence
- DoS with (Unexpected) revert
- DoS with Block Gas Limit
- Gas Usage, Gas Limit and Loops
- Redundant fallback function

- Unsafe type Inference
- Reentrancy
- Explicit visibility of functions state variables (external, internal, private and public)
- Logic Flaws

For vulnerabilities, we categorize the findings into categories as listed in table below, depending on their severity level:

SEVERITY LEVEL	DESCRIPTION
CRITICAL	A vulnerability that can disrupt the contract functioning; creates a critical risk to the contract; required to be fixed immediately.
HIGH	A vulnerability that could affect the desired outcome of executing the contract with high impact; needs to be fixed with high priority.
MEDIUM	A vulnerability that could affect the desired outcome of executing the contract with medium impact in a specific scenario; needs to be fixed.
LOW	An issue that does not have a significant impact, can be considered as less important.

Table 1. Severity levels

1.4. Disclaimer

Please note that security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a 100% secure smart contract. However, auditing allows discovering vulnerabilities that were unobserved, overlooked during development and areas where additional security measures are necessary.

2. AUDIT RESULT

2.1. Overview

The HimoWorld Staking Pool Smart Contracts was written in Solidity language, with the required version to be ^0.8.3.

The Himo World staking pool allows users to stake and earn rewards as time goes by.

The owner can update the rewards per block parameter at any time. He can also withdraw all reward tokens from this contract (in case of an emergency situation).

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of the HimoWorld Staking Pool Smart Contracts.

APPENDIX

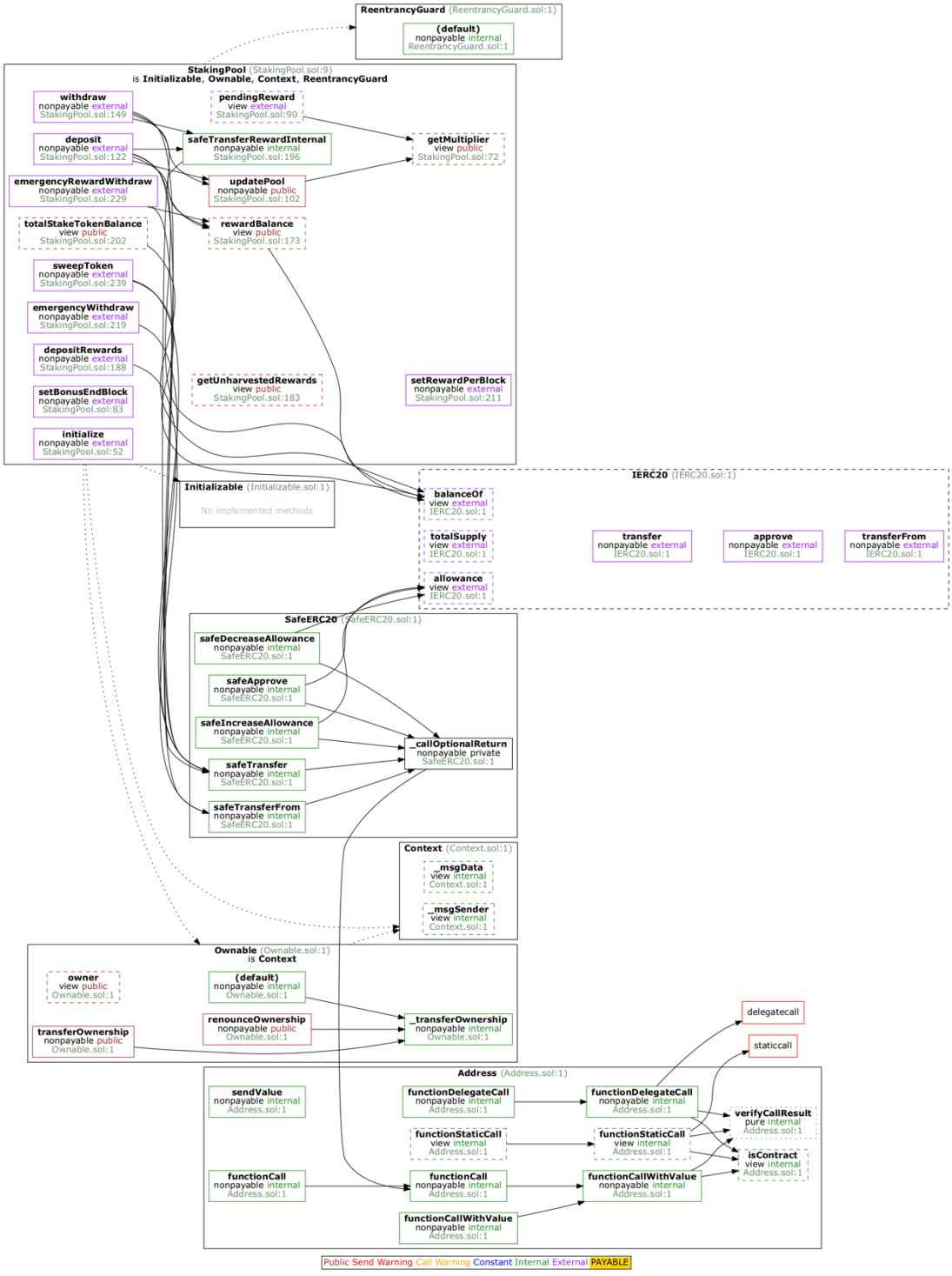

Image 1. HimoWorld Staking Pool Smart Contracts call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Feb 07, 2022*	Public Report	Verichains Lab

Table 2. Report versions history