verichains

SECURITY AUDIT OF

DEPPMOVE TOKEN SMART CONTRACT

Public Report

Jun 20, 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 Jun 20, 2022. We would like to thank the DEPPMOVE 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 DEPPMOVE Token Smart Contract. 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 issues in the smart contracts code.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

1.1. About DEPPMOVE Token Smart Contract

DEPP MOVE creates a Gamified and Socialfied Metaverse with the Pirate concept where users can walk, jog and run to earn $DEPP Token

Inspired by The Captain Jack Sparrow in the Pirates of the Caribbean, we created a Move-to-Earn Web 3 lifestyle app with the pirate concept

In DEPP MOVE, users equip themselves with NFTs in the form of Pirate-Concept Sneakers. By walking, jogging, running daily, users can earn rewards, which can either be used in-game, or cashed out for profit.

With Game-Fi, Social-Fi and an inspiring Pirate concept, DEPP MOVE aims to nudge not only the runner community, but also millions of people out there toward a modern, healthy and positive lifestyle. DEPP MOVE is the first app in the DEPP ecosystem. In the middle term, we aims to effectively bring the combination between different forms of moving including riding, driving and traveling.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the DEPPMOVE Token Smart Contract.

It was conducted on commit 9fd53c3752c69f006623c13a53ecd9aa8cebcc26 from git repository *https://github.com/deppmove/smartcontract/*.

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

SHA256 Sum	File
c9113c936073d36f2e9064e0b8a68ad2202cc1b0bc3839fa3de7829538323e72	**TokenDEPP.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 DEPPMOVE Token Smart Contract was written in Solidity language, with the required version to be ^0.8.0. The source code was written based on OpenZeppelin's library.

2.1.1. TokenDEPP contract

TokenDEPP is an upgradable ERC20 token contract which extends OwnableUpgradeable and ERC20Upgradeable contracts. With OwnableUpgradeable, by default, Token Owner is contract deployer, but he can transfer ownership to another address at any time. Please note that with ERC20Upgradeable, the whole contract can be upgraded anytime to change any logic (mint, transfer, lock, ...).

The contract pre-mints 350,000,000 tokens for the owner when initializing. The Token Owner can set any addresses to be operator. Operators can update unlockPercent and transfer locked amount of tokens to users. Users can only transfer unlockPercent of their lockBalances. If users approve for operators to use their tokens, operators can transfer and unlock tokens for users.

Table below lists some properties of the audited DEPPMOVE Token Smart Contract (as of the report writing time).

PROPERTY	VALUE
Name	DEPP
Symbol	DEPP
Decimals	18
Total Supply	350,000,000 ($x10^{18}$) Note: the number of decimals is 18, so the total representation token will be 350,000,000 or 350 million.

Table 2. The DEPPMOVE Token Smart Contract properties

2.2. Findings

During the audit process, the audit team found no vulnerability in the given version of DEPPMOVE Token Smart Contract.

APPENDIX

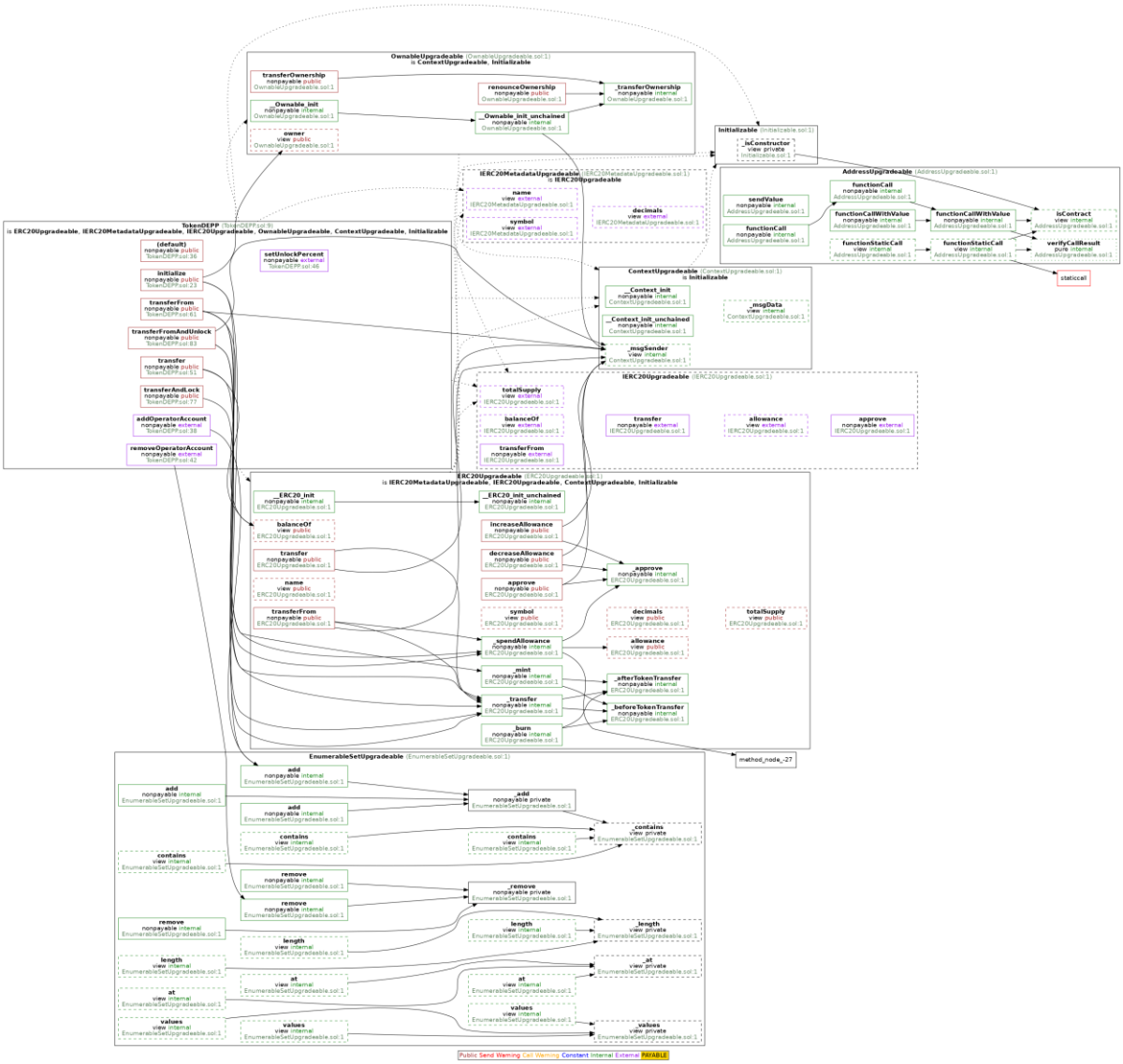

Image 1. DEPPMOVE Token Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Jun 20, 2022*	Public Report	Verichains Lab

Table 3. Report versions history