verichains

SECURITY AUDIT OF

PEACE COIN SMART CONTRACT

Public Report

Feb 23, 2024

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 was prepared by Verichains Lab on Feb 23, 2024. We would like to thank the Peace Network 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 Peace Coin 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 Peace Coin Smart Contract

The core mission of Peace Network is to establish a project platform based on blockchain smart contracts, with the noble aim of providing a safe, secure, and fair environment for all.

Peace Coin is an ERC20 token that is used in the Peace Network ecosystem.

1.2. Audit scope

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

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

SHA256 Sum	File
49a072b5ed5a82d57ec6047eda58a6a2d01734681055535e0731a718600ed5d9	ERC20.sol
900f3bc4d657385fbd602766132ef0cadf5c8c35d906585fa3b8d1660d46a1b7	Ownable.sol
fde229dce39536e9b13a8231bf73ebe616e1e1aae1a95ee296eca5be49314c08	PeaceCoin.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 were 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

Peace Network acknowledges that the security services provided by Verichains, are conducted to the best of their professional abilities but cannot guarantee 100% coverage of all security vulnerabilities. Peace Network understands and accepts that despite rigorous auditing, certain vulnerabilities may remain undetected. Therefore, Peace Network agrees that Verichains shall not be held responsible or liable, and shall not be charged for any hacking incidents that occur due to security vulnerabilities not identified during the audit process.

1.5. Acceptance Minute

This final report served by Verichains to the Peace Network will be considered an Acceptance Minute. Within 7 days, if no any further responses or reports is received from the Peace Network, the final report will be considered fully accepted by the Peace Network without the signature.

2. AUDIT RESULT

2.1. Overview

The Peace Coin Smart Contract was written in `Solidity` language, with the required version to be `0.8.20`.

The contract extends `ERC20` and `Ownable`. With `Ownable` being a minor modification from the `OpenZeppelin` library, the Token Owner is, by default, the contract deployer. However, they can transfer ownership to another address at any time. The contract charges users a fee when they transfer tokens or interact with swap pairs on the Dex. This fee will be sent to the vault address set by the `owner`; only users on the `whitelistFee` are exempted from this fee. The transferFee, buyFee, and sellFee are set by the `owner` and can be changed at any time, with the maximum value being `10%`. The `owner` can also change the lock state to prevent users from selling/buying tokens on the Dex. During this time, only users on the `whitelistAction` can trade the token. All `whitelists` can be added or removed by the `owner` at any time.

Table 2 lists some properties of the audited Peace Coin Smart Contract (as of the report writing time).

PROPERTY	VALUE
Name	Peace Coin
Symbol	PC
Decimals	18
Total Supply	99,000,000 ($x10^{18}$) Note: the number of decimals is 18, so the total representation token will be 99,000,000 or 99 million.

Table 2. The Peace Coin Smart Contract properties

2.2. Findings

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

APPENDIX

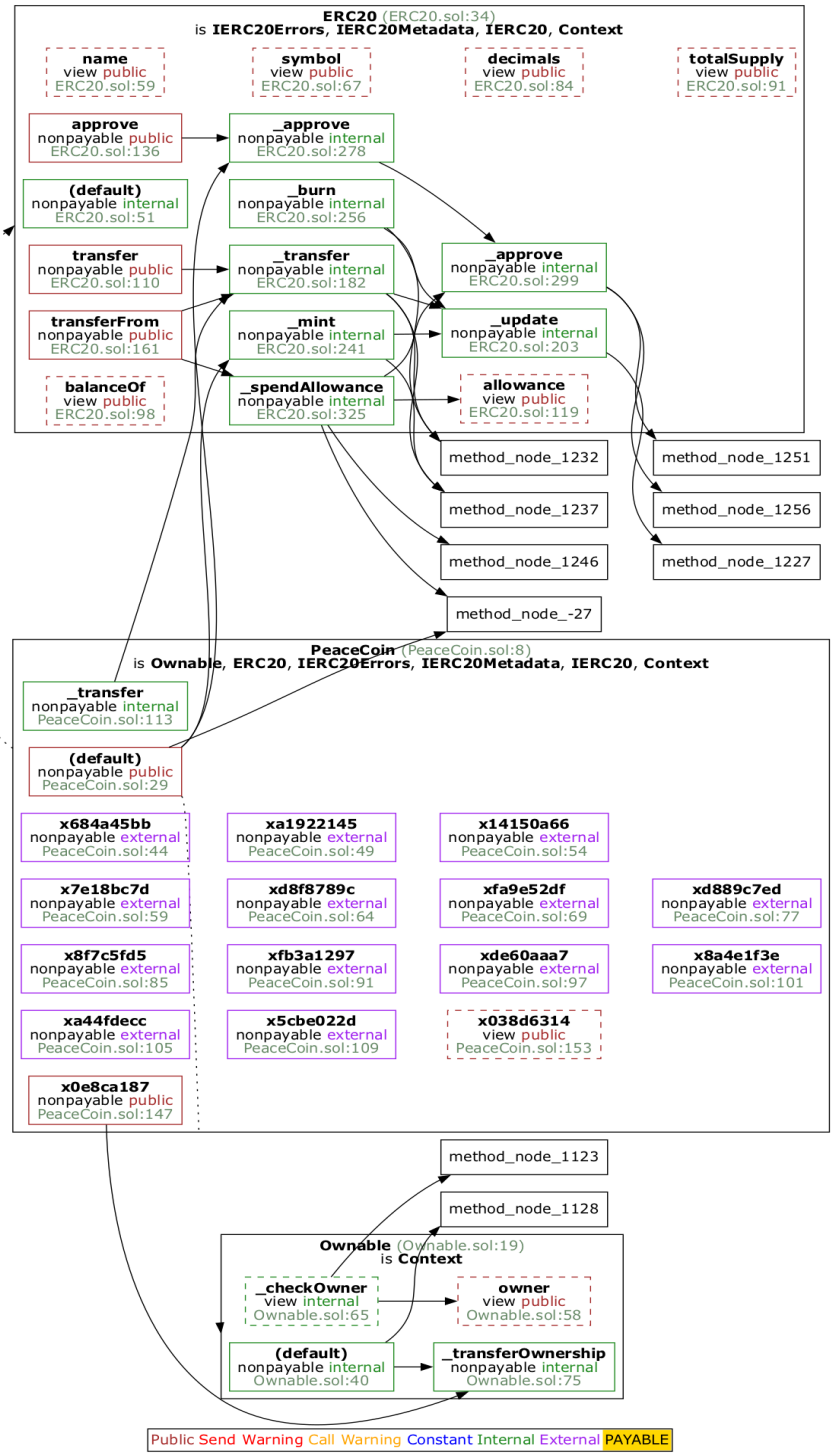

Image 1. Peace Coin Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Feb 23, 2024*	Public Report	Verichains Lab

Table 3. Report versions history