SECURITY AUDIT OF

NFT MARBLE TOKEN SMART CONTRACT

Public Report

Jan 21, 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 Jan 21, 2022. We would like to thank the NFT MARBLE 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 NFT MARBLE 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 NFT MARBLE Token Smart Contract

NFT MARBLE is an online Board game based on blockchain technology with simple play, various tactics and different modes.You can ather friends, form a team, play board games with others and earn money with your skills.

Dozen is BEP20 token that NFT MARBLE players can use in the game.

1.2. Audit scope

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

The audited contract is the NFT MARBLE Token Smart Contract that deployed on Binance Smart Chain Mainnet at address 0xc236a71f9633a0be7d97ad68f8c16de6ec46a252. The details of the deployed smart contract are listed in Table 1.

FIELD	VALUE
Contract Name	DOZEN
Contract Address	0xc236a71f9633a0be7d97ad68f8c16de6ec46a252
Compiler Version	v0.8.7+commit.e28d00a7
Optimization Enabled	No with 200 runs
Explorer	*https://bscscan.com/address/0xc236a71f9633a0be7d97ad68f8c16de6ec46a252*

Table 1. The deployed smart contract details

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 2. 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

2.1.1. Contract codes

The NFT MARBLE Token Smart Contract was written in Solidity language, with the required version to be 0.8.0.

2.1.2. Dozen token contract

The DOZEN contract extends Ownable, Pausable, BEP20 and BEP20Burnable contracts. With Ownable, by default, Token Owner is contract deployer but he can transfer ownership to another address at any time. He can pause/unpause contract using Pausable contract, user can only transfer tokens when contract is not paused. The BEP20Burnable allows token holders to destroy both their own tokens and those that they have an allowance for.

In addition, the main contract implements a bunch of lock and unlock amount which allows the owner of contract restricting to transfer tokens.

Table 2 lists some properties of the audited NFT MARBLE Token Smart Contract (as of the report writing time).

PROPERTY	VALUE
Name	NFT MARBLE TOKEN DOZEN
Symbol	DOZEN
Decimals	18
Total Supply	1,000,000,000 (x10^{18}) Note: the number of decimals is 18, so the total representation token will be 1,000,000,000 or 1 billion.

Table 3. The NFT MARBLE Token Smart Contract properties

2.2. Findings

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

APPENDIX

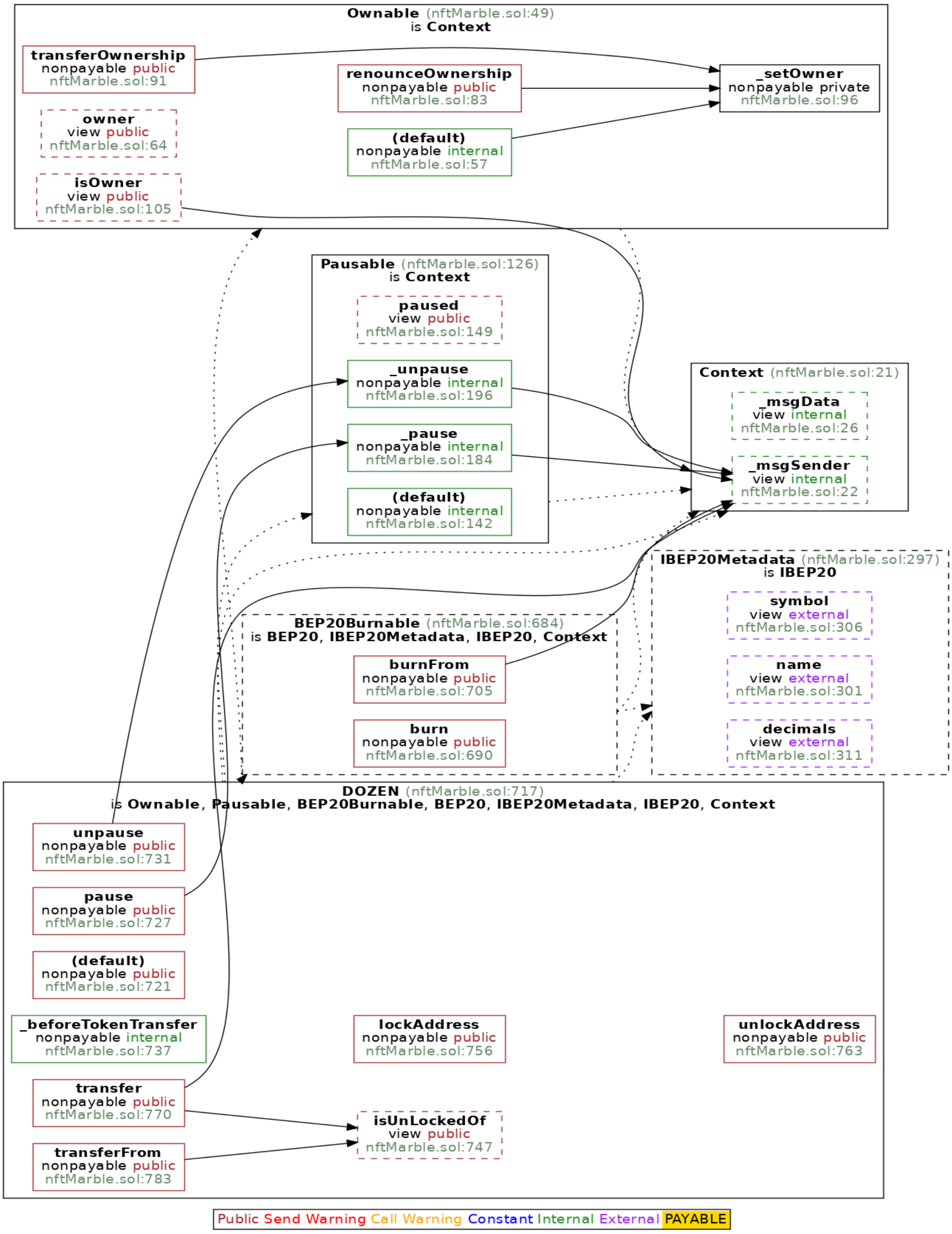

Image 1. NFT MARBLE Token Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Jan 21, 2021*	Public Report	Verichains Lab

Table 4. Report versions history