verichains

SECURITY AUDIT OF

BINGOFAMILY SMART CONTRACT

Public Report

Apr 04, 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 Apr 04, 2022. We would like to thank the BingoFamily 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 BingoFamily 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 application.

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY 5

1.1. About BingoFamily Smart Contract 5

1.2. Audit scope 5

1.3. Audit methodology 5

1.4. Disclaimer 6

2. AUDIT RESULT 7

2.1. Overview 7

2.2. Contract codes 7

2.2.1. IBEP20 interface 7

2.2.2. IBEP20Metadata interface 7

2.2.3. Context abstract contract 7

2.2.4. Ownable abstract contract 7

2.2.5. BEP20 contract 7

2.2.6. Pausable abstract contract 7

2.2.7. BEP20Burnable abstract contract 8

2.2.8. BGOF contract 8

2.3. Findings 8

3. VERSION HISTORY 10

1. MANAGEMENT SUMMARY

1.1. About BingoFamily Smart Contract

BINGO.FAMILY is the simplest bingo game. In 1:1 mode, users complete 5 horizontal, vertical, and diagonal bingo to score points within 2 minutes, and the user with the highest final score will win. The winner will receive higher Points than the loser.

1.2. Audit scope

This audit focused on identifying security flaws in code and the design of the smart contracts of BingoFamily Smart Contract. It was conducted on the source code provided by the BingoFamily team.

It was conducted on commit ae9136369c7cf355ee23f61d81aca91166161170 from git repository *https://github.com/BingoFamily/Bingo.family/*.

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 BingoFamily Smart Contract is an BEP-20 Token Contract, which implements a standard interface for token as defined in IBEP20. This standard provides basic functionality to transfer tokens, as well as allow tokens to be approved so they can be spent by another on-chain third party.

2.2. Contract codes

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

2.2.1. IBEP20 interface

This is the interface of the BEP-20 token standard. The source code is referenced from OpenZeppelin's implementation.

2.2.2. IBEP20Metadata interface

This is the interface that extends IBEP20 interface to add functions for interacting with some metadata. The source code is referenced from OpenZeppelin's implementation.

2.2.3. Context abstract contract

This abstract contract provides information about the current execution context, including the sender of the transaction and its data. The source code is referenced from OpenZeppelin's implementation.

2.2.4. Ownable abstract contract

This abstract contract makes the BingoFamily Smart Contract ownable. The source code is referenced from OpenZeppelin's implementation.

2.2.5. BEP20 contract

This is the contract implement BEP20 token. The source code is referenced from OpenZeppelin's implementation.

2.2.6. Pausable abstract contract

Contract module allows children to implement an emergency stop mechanism that can be triggered by an authorized account. The source code is referenced from OpenZeppelin's implementation.

2.2.7. BEP20Burnable abstract contract

This abstract contract extends BEP20 abstract contract that allows token holders to destroy their tokens. The source code is referenced from OpenZeppelin's implementation.

2.2.8. BGOF contract

This is the main contract in the BingoFamily Smart Contract, which extends BEP20, BEP20Burnable, Pausable, Ownable abstract contract. Almost functions in the BGOF Smart Contract are inherited, some functions are overridden by composing between the old function and the modifiers.

The contract implements the mint public function which allows the owner of the contract to create unlimited tokens. The totalSupply of the contract may be changed by this function. The contact also implements some functions which lock the amount of the tokens of the users. The owner may lock any users with any amount by the lockAddress function.

This table lists some properties of the audited BingoFamily Smart Contract (as of the report writing time).

PROPERTY	VALUE
Name	BINGO FAMILY TOKEN
Symbol	BGOF
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 2. The BingoFamily Smart Contract properties

2.3. Findings

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

APPENDIX

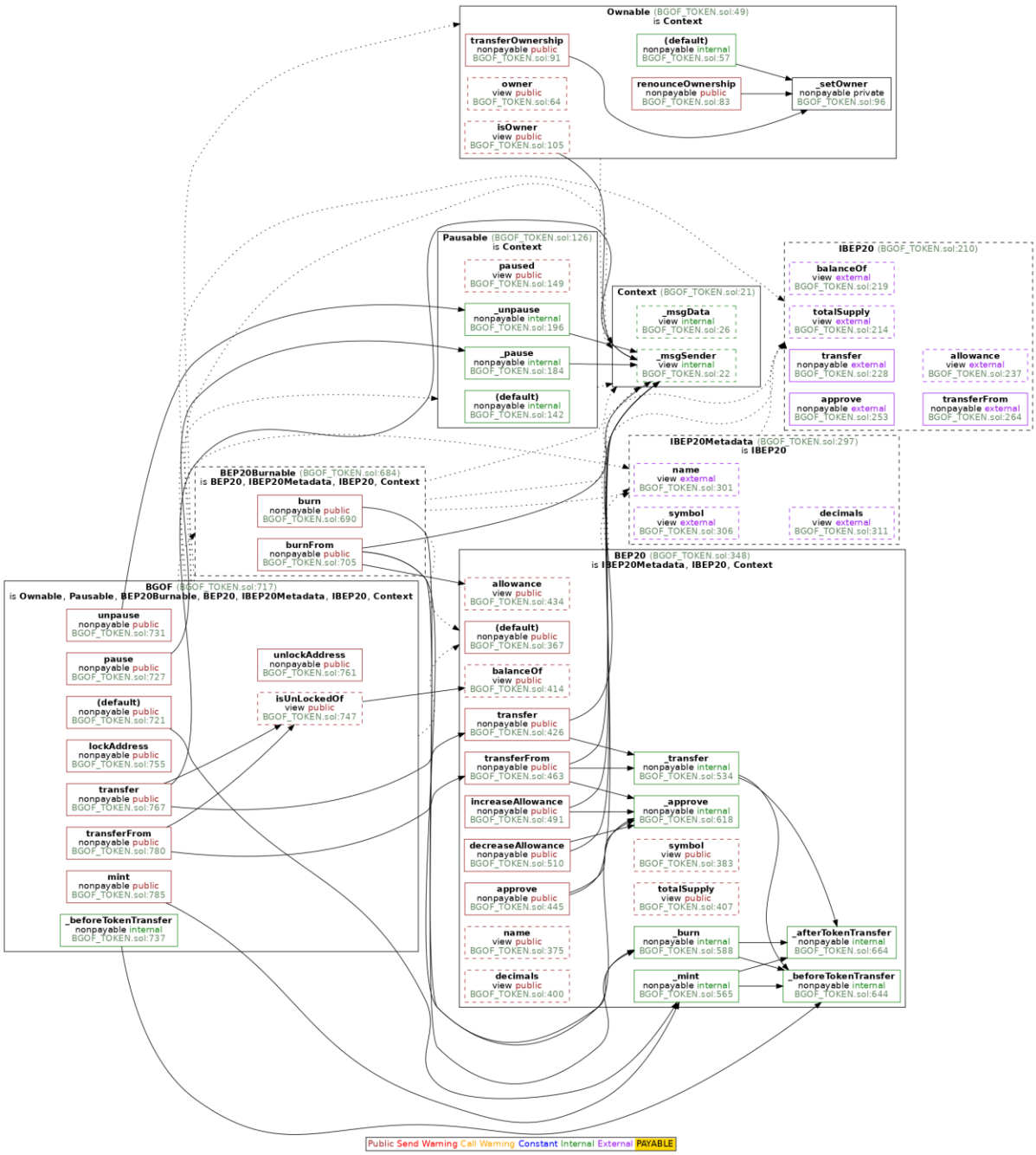

Image 1. BingoFamily Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Apr, 04, 2022*	Public Report	Verichains Lab

Table 3. Report versions history