SECURITY AUDIT OF

LGBT TOKEN SMART CONTRACT

Public Report

Apr 08, 2021

Verichains Lab

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 xRP20 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 08, 2021. We would like to thank the LGBT 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 LGBT 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 LGBT Token Smart Contract

The $LGBT Token is the lifeblood of LGBT Finance, whether in the metaverse or other projects. The Token comes to life and real usability when needed in the first Gay Friendly city, basically for you to do any kind of trading, you will need to be a holder of $LGBT. The official currency of the city in the metaverse will be $LGBT , making the token more and more in demand, and thus, having more and more appreciation.

1.2. Audit scope

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

The audited contract is the LGBT Token Smart Contract that deployed on Binance Smart Chain Mainnet at address 0x774dda160206347d065c68d2e92fefb90ad0d6bb. The details of the deployed smart contract are listed in Table 1.

FIELD	VALUE
Contract Name	LGBTToken
Contract Address	0x774dda160206347d065c68d2e92fefb90ad0d6bb
Compiler Version	v0.8.2+commit.661d1103
Optimization Enabled	No with 200 runs
Explorer	*https://bscscan.com/token/0x774dda160206347d065c68d2e92fefb90ad0d6bb*

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

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

PROPERTY	VALUE
Name	LGBT Token
Symbol	LGBT
Decimals	10
Total Supply	50,000,000,000 (x10^{10}) Note: the number of decimals is 10, so the total representation token will be 50,000,000,000 or 50 billion.

Table 3. The LGBT Token Smart Contract properties

2.2. Contract codes

The LGBT Token Smart Contract was written in Solidity language, with the required version to be 0.8.2.

The contract imported a lot of contracts that were implemented by OpenZeppelin.

LGBTToken contract extends ERC20, ERC20Burnable, ERC20Snapshot, Ownable, Pausable, ERC20Snapshot, ERC20Votes and ERC20FlashMint contracts. With Ownable, by default, Token Owner is contract deployer but he can transfer ownership to another address at any time. ERC20Burnable allows token holders to destroy both their own tokens and those that they have an allowance for. ERC20Snapshot help Token Owner take a snapshot of the balances and total supply at a time for later access.

2.3. Findings

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

APPENDIX
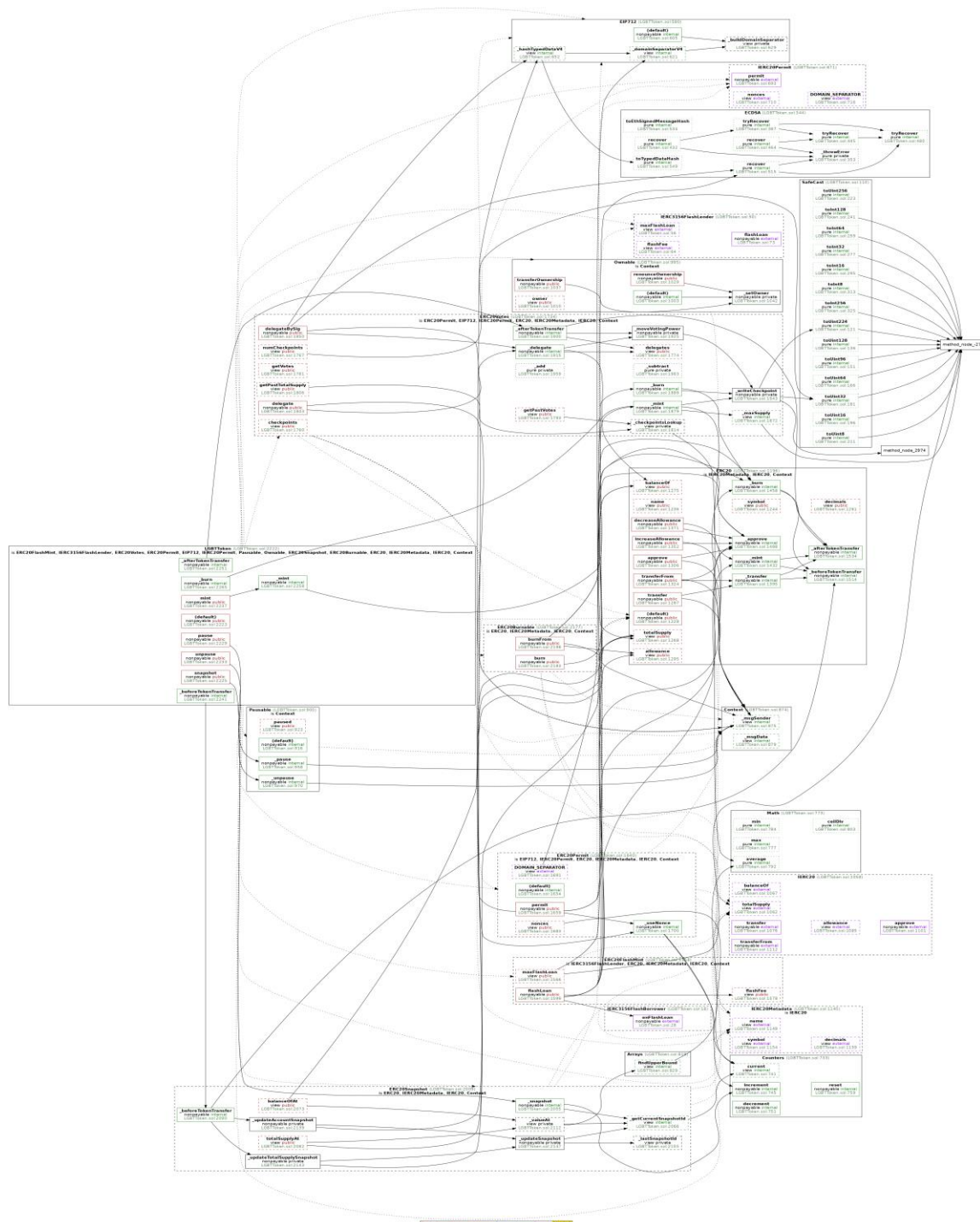
Image 1. LGBT Token Smart Contract call graph

3. VERSION HISTORY

Version	Date	Status/Change	Created by
1.0	*Apr 08, 2022*	Public Report	Verichains Lab

Table 3. Report versions history