



QuillAudits

Audit Report October, 2021

For



Contents

| | |
|---|----|
| Scope of Audit | 01 |
| Check Vulnerabilities | 01 |
| Techniques and Methods | 02 |
| Issue Categories | 03 |
| Number of security issues per severity. | 03 |
| Introduction | 04 |
| A. Contract - Bollycoin.sol | 05 |
| High Severity Issues | 05 |
| Medium Severity Issues | 05 |
| Low Severity Issues | 05 |
| 1. Gas Consumption | 05 |
| Informational Issues | 05 |
| Functional Tests | 06 |
| Automated Tests | 07 |
| Closing Summary | 10 |

Scope of the Audit

The scope of this audit was to analyze and document the Bollycoin Token smart contract codebase for quality, security, and correctness.

Checked Vulnerabilities

We have scanned the smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

Techniques and Methods

Throughout the audit of smart contract, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods and tools were used to review all the smart contracts.

Structural Analysis

In this step, we have analysed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis

Static analysis of smart contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis

Manual analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analysed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption

In this step, we have checked the behaviour of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit

Remix IDE, Solhint, Mythril, Slither.

Issue Categories

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

| Risk-level | Description |
|----------------------|---|
| High | A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment. |
| Medium | The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed. |
| Low | Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future. |
| Informational | These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact. |

Number of issues per severity

| Type | High | Medium | Low | Informational |
|---------------------|------|--------|-----|---------------|
| Open | 0 | 0 | 0 | 0 |
| Acknowledged | 0 | 0 | 1 | 0 |
| Closed | 0 | 0 | 0 | 0 |

Introduction

During the period of **October 19, 2021 to October 25, 2021** - QuillAudits Team performed a security audit for the **Bollycoin** smart contract.

The contract was deployed and tested on Ropsten and you can find it here:
- Bollycoin: [0xF8F3F6efF63C3BCebe95829dA4522383d6Ff1eb2](https://ropsten.etherscan.io/address/0xF8F3F6efF63C3BCebe95829dA4522383d6Ff1eb2)



Issues Found

A. Contract – Bollycoin.sol

High severity issues

No issues were found.

Medium severity issues

No issues were found.

Low severity issues

1. Gas Consumption

Description

The following functions can be made **external** instead of **public**:

- mint()
- burn()
- pause()
- unpause()

Reason

External functions in solidity use lesser gas as compared to public functions. You can read more about it [here](#).

Status: **Acknowledged**

Informational Issues

No issues were found.

Functional test

| Function Names | Testing results |
|-------------------|-----------------|
| transfer | Passed |
| transferFrom | Passed |
| mint | Passed |
| burn | Passed |
| approve | Passed |
| increaseAllowance | Passed |
| decreaseAllowance | Passed |
| grantRole | Passed |
| pause | Passed |
| unpause | Passed |
| renounceRole | Passed |
| revokeRole | Passed |

Automated Tests

Slither

Slither, an open-source static analysis framework. This tool provides rich information about Ethereum smart contracts and has critical properties. While Slither is built as a security-oriented static analysis framework, it is also used to enhance the user's understanding of smart contracts, assist in code reviews, and detect missing optimizations. Slither detected the following issues:

```
INFO:Detectors:
Bollycoin.constructor(string,string,uint256,address)._name (dist/BollyCoin.sol#1247) shadows:
- ERC20._name (dist/BollyCoin.sol#874) (state variable)
Bollycoin.constructor(string,string,uint256,address)._symbol (dist/BollyCoin.sol#1248) shadows:
- ERC20._symbol (dist/BollyCoin.sol#875) (state variable)
Bollycoin.constructor(string,string,uint256,address)._totalSupply (dist/BollyCoin.sol#1249) shadows:
- ERC20._totalSupply (dist/BollyCoin.sol#872) (state variable)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
Address.isContract(address) (dist/BollyCoin.sol#642-652) uses assembly
- INLINE ASM (dist/BollyCoin.sol#648-658)
Address.verifyCallResult(bool,bytes,string) (dist/BollyCoin.sol#811-831) uses assembly
- INLINE ASM (dist/BollyCoin.sol#823-828)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Pragma version0.6.12 (dist/BollyCoin.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.6.11
solc-0.6.12 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (dist/BollyCoin.sol#670-675):
- (success) = recipient.call(value: amount)() (dist/BollyCoin.sol#673)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (dist/BollyCoin.sol#738-749):
- (success,returndata) = target.call(value: value)(data) (dist/BollyCoin.sol#747)
Low level call in Address.functionStaticCall(address,bytes,string) (dist/BollyCoin.sol#767-776):
- (success,returndata) = target.staticcall(data) (dist/BollyCoin.sol#774)
Low level call in Address.functionDelegateCall(address,bytes,string) (dist/BollyCoin.sol#794-803):
- (success,returndata) = target.delegatecall(data) (dist/BollyCoin.sol#801)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
```

```

INFO:Detectors:
grantRole(bytes32,address) should be declared external:
  - AccessControl.grantRole(bytes32,address) (dist/BollyCoin.sol#448-448)
revokeRole(bytes32,address) should be declared external:
  - AccessControl.revokeRole(bytes32,address) (dist/BollyCoin.sol#459-461)
renounceRole(bytes32,address) should be declared external:
  - AccessControl.renounceRole(bytes32,address) (dist/BollyCoin.sol#477-481)
name() should be declared external:
  - ERC20.name() (dist/BollyCoin.sol#896-898)
symbol() should be declared external:
  - ERC20.symbol() (dist/BollyCoin.sol#904-906)
decimals() should be declared external:
  - ERC20.decimals() (dist/BollyCoin.sol#921-923)
totalSupply() should be declared external:
  - ERC20.totalSupply() (dist/BollyCoin.sol#928-930)
balanceOf(address) should be declared external:
  - ERC20.balanceOf(address) (dist/BollyCoin.sol#935-937)
transfer(address,uint256) should be declared external:
  - ERC20.transfer(address,uint256) (dist/BollyCoin.sol#947-955)
allowance(address,address) should be declared external:
  - ERC20.allowance(address,address) (dist/BollyCoin.sol#968-968)
approve(address,uint256) should be declared external:
  - ERC20.approve(address,uint256) (dist/BollyCoin.sol#977-985)
transferFrom(address,address,uint256) should be declared external:
  - ERC20.transferFrom(address,address,uint256) (dist/BollyCoin.sol#999-1014)
increaseAllowance(address,uint256) should be declared external:
  - ERC20.increaseAllowance(address,uint256) (dist/BollyCoin.sol#1028-1039)
decreaseAllowance(address,uint256) should be declared external:
  - ERC20.decreaseAllowance(address,uint256) (dist/BollyCoin.sol#1053-1069)
mint(address,uint256) should be declared external:
  - Bollycoin.mint(address,uint256) (dist/BollyCoin.sol#1256-1261)
burn(uint256) should be declared external:
  - Bollycoin.burn(uint256) (dist/BollyCoin.sol#1263-1265)
pause() should be declared external:
  - Bollycoin.pause() (dist/BollyCoin.sol#1267-1271)
unpause() should be declared external:
  - Bollycoin.unpause() (dist/BollyCoin.sol#1274-1279)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:dist/BollyCoin.sol analyzed (12 contracts with 46 detectors), 29 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration

```


Mythril

Mythril is a security analysis tool for EVM bytecode. It detects security vulnerabilities in smart contracts built for Ethereum, Hedera, Quorum, VeChain, Roostock, Tron and other EVM-compatible blockchains. It uses symbolic execution, SMT solving and taint analysis to detect a variety of security vulnerabilities. Mythril raised the following concerns:

The analysis was completed successfully. No issues were detected.

Contract Library

Contract-library contains the most complete, high-level decompiled representation of all Ethereum smart contracts, with security analysis applied to these in real-time.

We performed analysis using the contract Library on the Ropsten address of the Bollycoin contract used during manual testing:

- Bollycoin: F8F3F6EFF63C3BCEBE95829DA4522383D6FF1EB2

Results

No major issues were found. Some false positive errors were reported by the tool. All the other issues have been categorized above according to their level of severity.

Closing Summary

In this report, we have considered the security of Bollycoin. We performed our audit according to the procedure described above.

The audit showed one low level severity issue.

Disclaimer

Quillhash audit is not a security warranty, investment advice, or an endorsement of the **Bollycoin** platform. This audit does not provide a security or correctness guarantee of the audited smart contracts. The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the Bollycoin Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.



Audit Report October, 2021

For



QuillAudits

📍 Canada, India, Singapore, United Kingdom

🌐 audits.quillhash.com

✉️ audits@quillhash.com