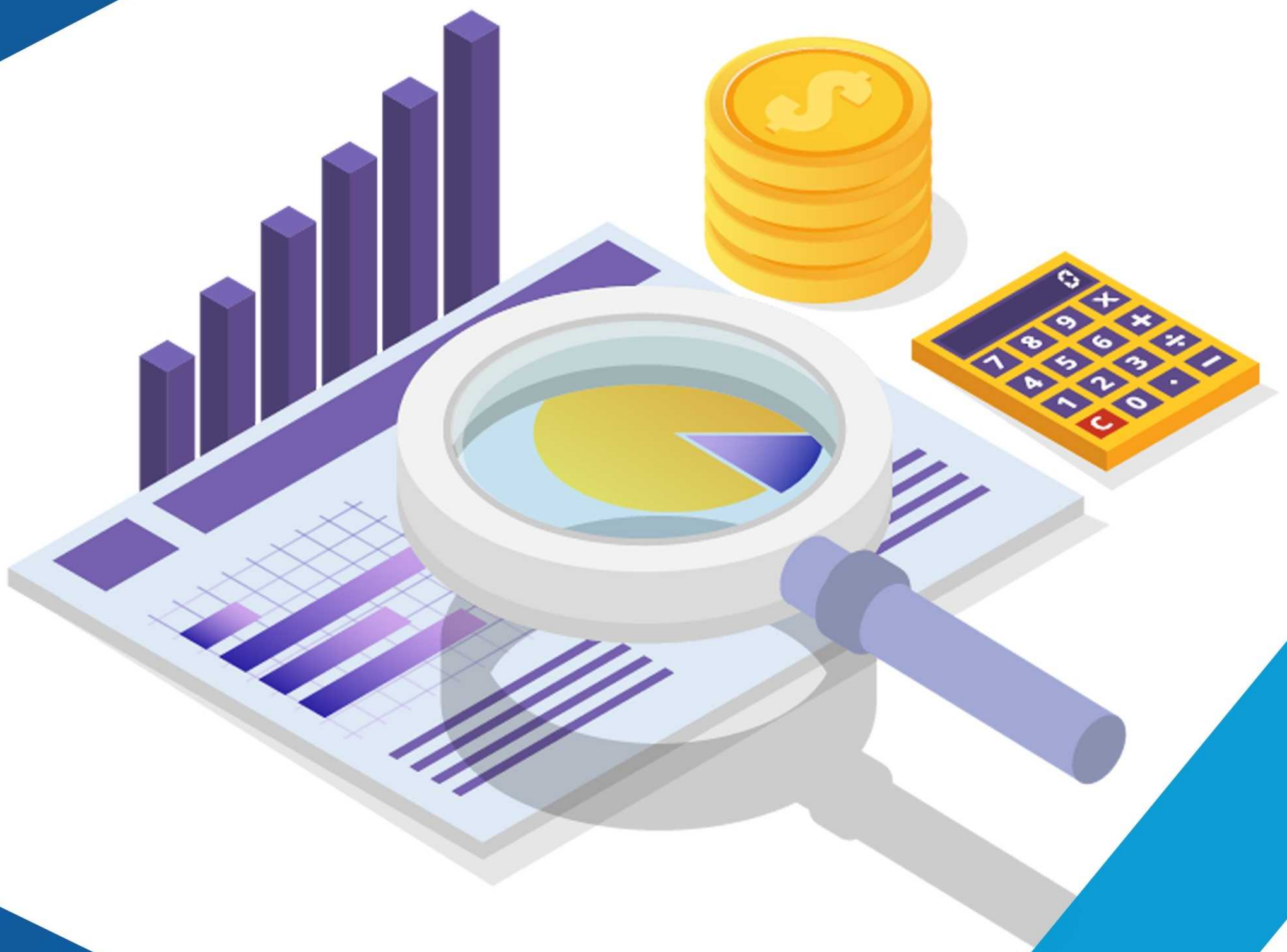
QuillAudits



Audit Report
June, 2021

BINAMON

Contents

Scope of Audit

The scope of this audit was to analyse BMON and BMONSeedAndPreSale smart contract's codebase for quality, security, and correctness.

Code link - https://drive.google.com/file/d/1lB5WyaTa9jDQcBcfCWOndxA-H9StqImD/view

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
- Exception Disorder
- Gasless Send
- Use of tx.origin
- Malicious libraries
- Compiler version not fixed
- Address hardcoded
- Divide before multiply
- Integer overflow/underflow
- ERC20 transfer() does not return boolean
- ERC20 approve() race
- Dangerous strict equalities
- Tautology or contradiction
- Return values of low-level
- calls Missing Zero Address
- Validation Private modifier
- Revert/require functions
- Using block.timestamp
- Multiple Sends Using SHA3
- Using suicide
- Using throw
- Using inline assembly

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 analyzed 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.
SmartCheck.

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 security of smart contracts.

Code Review / Manual Analysis
Manual Analysis or review of code was done to identify new vulnerability or verify the vulnerabilities found during the static analysis. Contracts were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of 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 possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit
Remix IDE, Truffle, Truffle Team, Ganache, Solhint, Mythril, Slither, SmartCheck.

Issue Categories

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

High severity issues

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 to be fixed before moving to a live environment.

Medium level severity issues

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 level severity issues

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 four issues which 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	3	2
Closed	1	0	0	0

Issues Found – Code Review / Manual Testing

High severity issues

1. **[283-312]Losing tokenAmount due to Multiply After Divide**
   TestCase
   User A want to buy some tokens with implementation
   as [Consider **msg.value = 1ether**]

   tokenAmount = (msg.value / SEED_PRICE) * 10**18;
   The resulting tokenAmount will be **353350000000000000000000**

   Consider, the implementation as
   tokenAmount = (msg.value * 1018) / SEED_PRICE;**
   and the resulting tokenAmount will be **353356890459363957597 17**

   So a user is losing 6890459363957597 17 tokenAmount while calculation

   Status: Fixed

Medium severity issues

No issues were found.

Low level severity issues

1. **Multiple pragma directives have been found**
   Use a single solidity compiler

   Status: Open

2. Missing Zero Address Validation

[#L104-111] function **transfer()**: Missing zero address check for address **receiver**
[#L104-111] function **approve()**: Missing zero address check for address **delegate**
[#L148-151] function **allowBuyingBoosters()**: Missing zero address check for address **bmonc**
[#L153-155] function **setSeedAndPresale()**: Missing zero address check for address **seedAndPresale_**
[#L246-249] function **constructor()**: Missing zero address check for address **token_ and beneficiary_**

Status: Open

3. approve() race

The standard ERC20 implementation contains a widely-known racing condition in its approve function, wherein a spender is able to witness the token owner broadcast a transaction altering their approval and quickly sign and broadcast a transaction using transferFrom to move the current approved amount from the owner's balance to the spender. If the spender's transaction is validated before the owner's, the spender is able to spend their entire approval amount twice.

Reference:

- https://docs.google.com/document/d/1YLPtQxZu1UAvO9cZ1O2RPXBbT0mooh4DYKjA_jp-RLM/edit

- https://medium.com/mycrypto/bad-actors-abusing-erc20-approval-to-steal-your-tokens-c0407b7f7c7c

- https://eips.ethereum.org/EIPS/eip-20

Status: Open

Informational

1. Missing Error Messages

[124, 125] Error Messages can be added to the **require** checks so as to track down the errors

Status: Open

2. [291, 292, 293, 302, 303, 304] Use **add** function from SafeMath library instead of + operator

Status: Open

Gas Optimization

Public functions that are never called by the contract should be declared external to save gas.

Disclaimer

The audit does not give any warranties on the security of the code. One audit cannot be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of the code. Besides a security audit, please don’t consider this report as investment advice.

Closing Summary

Some issues of low severity have been reported during the audit. A high issue has been reported and is now fixed by the developers.

BINAMON

QuillAudits

Canada, India, Singapore and United Kingdom

audits.quillhash.com

audits@quillhash.com