# IMO BEP20 Audit

# The BlockChain Auditor

This document expresses all security concerns of the IMO BEP20 smart contract as expressed by Jorge Martinez. I took care to attempt to find as many ways to improve the security, code efficiency, best practices, and overall function of the smart contracts.

## Contract Status: Ready for Deployment

0 Critical Issue(s) found were found.

0 Medium Issue(s) were found.

0 Low Issue(s) were found.

0 Informational Issue(s) were found.

## Solidity Code Coverage

| Jorge's Test Suite | IMO | Industry Standard |
|---|---|---|
| 89.83% | 0% | 95% |

For this audit, I wasn't provided with a testing suite but as part of my audit methodology I developed a test suite to verify the functionality of the IMO contracts, check their security, and to help reveal any underlying issues.

This audit should be seen as one step in the development process with the intent of raising awareness on the meticulous work involved in secure development and making no material statements or guarantees to the operational state of the smart contract(s) once they are deployed. This document is not an endorsement of the reliability or effectiveness of the smart contracts. This is an assessment of the smart contract logic, implementation, and best practices. I cannot take responsibility for any potential consequences of the deployment or use of the smart contract(s) related to the audit.

# Test Suite Results

## Jorge's Test Suite

```
IMO Token Security Suite
  Deployment
    ✓ should have a name (582ms)
  airdrop logic
    ✓ testing claiming after airdrop (434ms)
    ✓ testing burn function claim exploit (155ms)
    -
  transfer functions
    ✓ calling transferFrom() invokes a fee and a burn (77ms)
    transfer
      ✓ can transfer tokens (38ms)
      ✓ transferring using the pair invokes a fee and a burn (87ms)


  6 passing (1s)
  1 pending

---------------|----------|----------|----------|----------|----------------|
File           | % Stmts  | % Branch | % Funcs  | % Lines  |Uncovered Lines |
---------------|----------|----------|----------|----------|----------------|
 contracts/    |    89.83 |    53.85 |    84.09 |    89.17 |                |
  imo-token.sol|    89.83 |    53.85 |    84.09 |    89.17 |... 649,650,651 |
---------------|----------|----------|----------|----------|----------------|
All files      |    89.83 |    53.85 |    84.09 |    89.17 |                |
---------------|----------|----------|----------|----------|----------------|
```

# Table of Contents

# Audit Methodology & Techniques

The BlockChain Auditor has the following auditing process:

1. Our audits include
    a. Review of the specifications, source code, and instructions provided to the TheBlockchainAuditor to clearly identify the desired functionality of the smart contract(s).
    b. Manual line by line review of contract code to spot potential vulnerabilities.
    c. Identification of deviations between desired functionality expressed to the TheBlockchainAuditor and what the smart contract(s) are doing.
2. Automated static and symbolic analysis, as well as verifying testing coverage using the provided test suite.
    a. Automated static and symbolic analysis help determine what inputs cause each part of the smart contract to execute. Analysis of how much of the code base is tested and comparison to industry standard.
3. Examination of smart contracts and development process as a whole, ensuring best practices are followed, allowing improved efficiency and security based on established industry and academic practices.
4. Specific, itemized, and actionable recommendations to assist in securing the smart contract(s) in question.

# Contract Checklist

## imo-token.sol

| Contract Vulnerability | |
| --- | --- |
| Integer Overflow | Pass |
| Race Condition | Pass |
| Denial of Service | Pass |
| Logical Vulnerability | Pass |
| Hardcoded Address | Pass |
| Function Input Parameter Check | Pass |
| Function Access Control Check | Pass |
| Random Number Generation | N/A |
| Random Number Use | N/A |
| **Contract Specification** | |
| Solidity Compiler Version | Pass |
| Event Use | Pass |
| Fallback Function Use | N/A |
| Constructor Use | Pass |
| Function Visibility Declaration | Pass |
| Variable Storage Declaration | Pass |
| Deprecated Keyword Use | Pass |
| BEP20/223 Standard | Pass |
| BEP721 Standard | N/A |
| **Business Risk** | |
| Able to Arbitratrily Create Token | Pass |
| Able to Arbitrarily Destroy Token | Pass |
| Can Suspend Transactions | Pass |
| Short Address Attack | Pass |
| **Gas Optimization** | |
| assert()/require()/revert() misused | Pass |
| Loop Optimization | Pass |
| Storage Optimization | Pass |

## Critical

These issues in the smart contract can have catastrophic implications that could ruin your reputation, disrupt the contract's functionality, or impact the client and your users' sensitive information.

## Informational

This issue relates to style and security best practices but does not pose an immediate risk.

## Medium

An issue classified as medium has relatively small risk and isn't exploitable to circumvent desired functionality and could not have financial consequences but could put user's sensitive information at risk.

## Acknowledged

The issue remains in the code but is a result of an intentional business or design decision.

## Low

An issue classified as informational does not pose an immediate threat to disruption of functionality and could not be exploited on a recurring basis, however, it should be considered for security best practices or code integrity.

## Unresolved

Although the client has been informed of the risk, it was decided to accept it because it was not relevant in the functionality of the smart contract.

## Undetermined

The impact of the issue is uncertain and more investigation is required to understand the repercussions of the issue.

## Mitigated

Actions were taken to minimize the impact or likelihood of the risk.

# Executive Summary

## Overall Thoughts

During this audit, I uncovered 0 issues. I was able to verify the basic functionality of the IMO BEP20 contract. It is able to be traded and provides industry standard protections. The token fee and burn per trade are also working as expected. I was able to verify that the airdrop distribution will in fact be pro rata and users only need to do a transaction in order to receive it. Savings lots of gas by making it unnecessary to repeat duplicate caluclations.

# Appendix A

## File Fingerprints

| | |
|---|---|
| imo-token.sol | b38194e8ddaf94472df6d6c3525ebc17 |

The Blockchain Auditor is honored to have the opportunity to help verify the functionality of IMO's BEP20 smart contract. We look forward to seeing the growth of the IMO ecosystem.

# The BlockChain Auditor

- Jorge Martinez

THEBLOCKCHAINAUDITOR.COM