RD AUDITORS

PokeMoney, Smart Contract, Code Review and Security Analysis Report

Customer: PokeMoney
Prepared on: 18th April 2022
Platform: BSC
Language: Solidity

rdauditors.com

Table of Contents

Disclaimer

This document may contain confidential information about its systems and intellectual property of the customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the customer or it can be disclosed publicly after all vulnerabilities are fixed - upon the decision of the customer.

Document

Name	Smart Contract Code Review and Security Analysis Report of PokeMoney
Platform	BSC / Solidity
File 1	PMY.sol
MD5 hash	96B32937CA91B948CAE9B76965173E3A
SHA256 hash	33A774986CF5B07B964B05A5999DAD425CB8D6186923096F8EA6E8886A6CD47A
Date	18/4/2022

Introduction

RD Auditors (Consultant) were contracted by PokeMoney (Customer) to conduct a Smart Contracts Code Review and Security Analysis. This report represents the findings of the security assessment of the customer`s smart contracts and its code review conducted between 16th - 18th April 2022.

This contract consists of one file.

Project Scope

The scope of the project is a smart contract. We have scanned this smart contract for commonly known and more specific vulnerabilities, below are those considered (the full list includes but is not limited to):

- Reentrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with (Unexpected) Throw
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Byte array vulnerabilities
- Style guide violation
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Unchecked external call - Unchecked math
- Unsafe type inference
- Implicit visibility level

Executive Summary

According to the assessment, the customer's solidity smart contract is **Well-Secured.**

Automated checks are with smartDec, Mythril, Slither and remix IDE. All issues were performed by our team, which included the analysis of code functionality, the manual audit found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the audit overview section. The general overview is presented in the AS-IS section and all issues found are located in the audit overview section.

We found the following;

Total Issues	1
Critical	0
High	0
Medium	0
Low	1
Very Low	0

Code Quality

Please note that within this report IBEP20, Context, Ownable are taken from the popular OpenZeppelin library.

The libraries within this smart contract are part of a logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned to a specific address and its properties/methods can be reused many times by other contracts.

The PokeMoney team has not provided scenario and unit test scripts, which would help to determine the integrity of the code in an automated way.

Documentation

We were given the PokeMoney code as a Github link:

https://github.com/pokemoney001/pokemoney/blob/main/PMY.sol

The hash of that file is mentioned in the table. As mentioned above, It's recommended to write comments in the smart contract code, so anyone can quickly understand the programming flow as well as complex code logic.

Comments are very helpful in understanding the overall architecture of the protocol. It also provides a clear overview of the system components, including helpful details, like the lifetime of the background script.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure. Those were based on well known industry standard open source projects and even core code blocks that are written well and systematically.

AS-IS Overview

PokeMoney

File And Function Level Report

File: PMY.sol

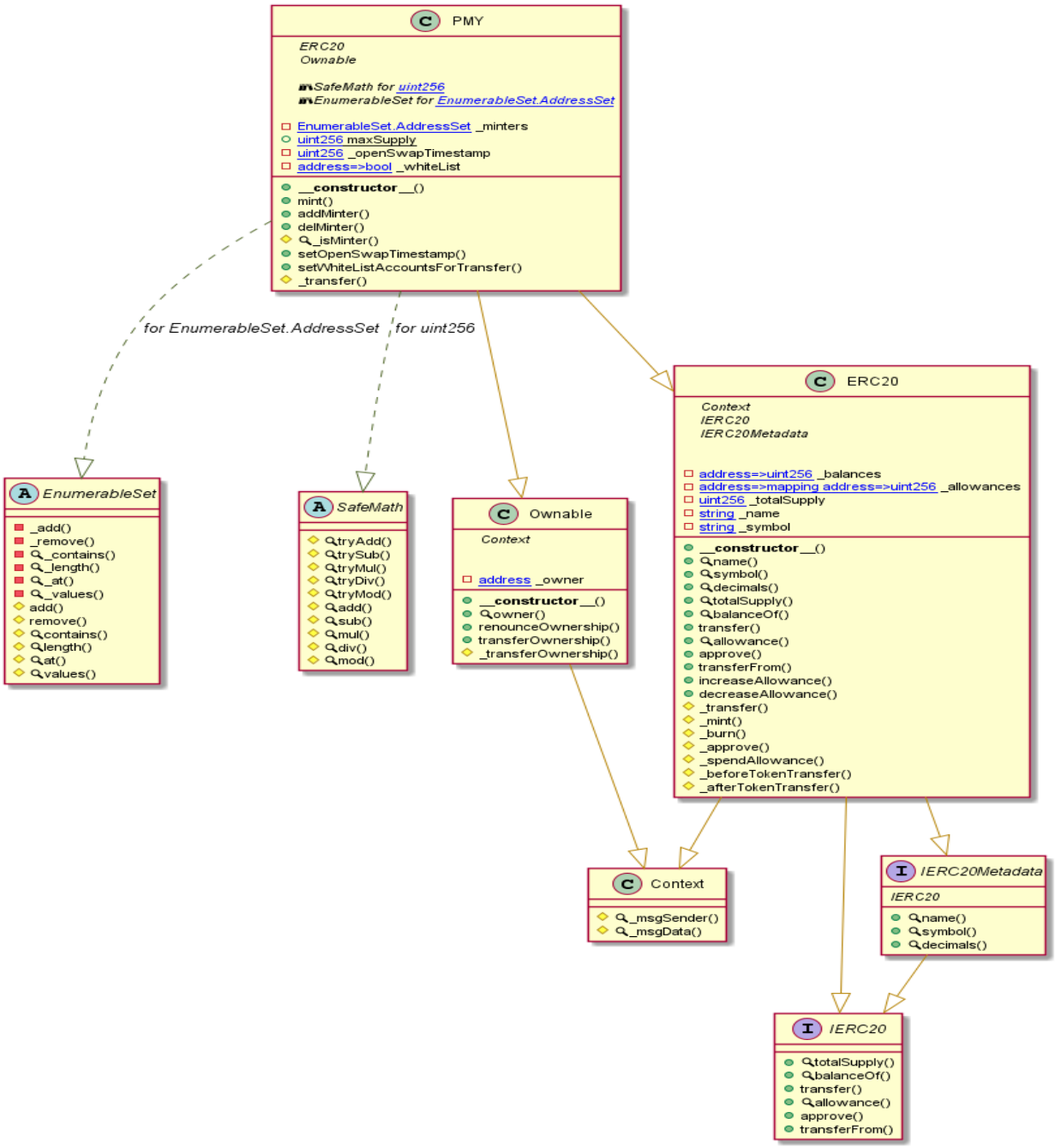
Contract: PMY

Observation: Passed

Test Report: Passed

Sl.	Function	Type	Observation	Test Report	Conclusion	Score
1	mint	write	Passed	All Passed	No Issue	Passed
2	addMinter	write	Passed	All Passed	No Issue	Passed
3	delMinter	write	Passed	All Passed	No Issue	Passed
4	_isMinter	internal	Passed	All Passed	No Issue	Passed
5	setOpenSwapTimestamp	write	Passed	All Passed	No Issue	Passed
6	setWhiteListAccountsForTransfer	external	Passed	All Passed	No Issue	Passed
7	_transfer	internal	Passed	All Passed	No Issue	Passed

Code Flow Diagram - PokeMoney



Code Flow Diagram - Slither Results Log

```
INFO:Detectors:
PMY._transfer(address,address,uint256) (PMY.sol#1111-1124) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp >= _openSwapTimestamp && _openSwapTimestamp > 0,invalid) (PMY.sol#1117-1121)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
EnumerableSet.values(EnumerableSet.AddressSet) (PMY.sol#248-257) uses assembly
        - INLINE ASM (PMY.sol#252-254)
EnumerableSet.values(EnumerableSet.UintSet) (PMY.sol#321-330) uses assembly
        - INLINE ASM (PMY.sol#325-327)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Context._msgData() (PMY.sol#639-641) is never used and should be removed
ERC20._burn(address,uint256) (PMY.sol#946-961) is never used and should be removed
EnumerableSet._at(EnumerableSet.Set,uint256) (PMY.sol#104-106) is never used and should be removed
EnumerableSet._length(EnumerableSet.Set) (PMY.sol#90-92) is never used and should be removed
EnumerableSet._values(EnumerableSet.Set) (PMY.sol#116-118) is never used and should be removed
EnumerableSet.add(EnumerableSet.Bytes32Set,bytes32) (PMY.sol#132-134) is never used and should be removed
EnumerableSet.add(EnumerableSet.UintSet,uint256) (PMY.sol#271-273) is never used and should be removed
EnumerableSet.at(EnumerableSet.AddressSet,uint256) (PMY.sol#236-238) is never used and should be removed
EnumerableSet.at(EnumerableSet.Bytes32Set,uint256) (PMY.sol#170-172) is never used and should be removed
EnumerableSet.at(EnumerableSet.UintSet,uint256) (PMY.sol#309-311) is never used and should be removed
EnumerableSet.contains(EnumerableSet.Bytes32Set,bytes32) (PMY.sol#149-151) is never used and should be removed
EnumerableSet.contains(EnumerableSet.UintSet,uint256) (PMY.sol#288-290) is never used and should be removed
EnumerableSet.length(EnumerableSet.AddressSet) (PMY.sol#222-224) is never used and should be removed
EnumerableSet.length(EnumerableSet.Bytes32Set) (PMY.sol#156-158) is never used and should be removed
EnumerableSet.length(EnumerableSet.UintSet) (PMY.sol#295-297) is never used and should be removed
EnumerableSet.remove(EnumerableSet.Bytes32Set,bytes32) (PMY.sol#142-144) is never used and should be removed
EnumerableSet.remove(EnumerableSet.UintSet,uint256) (PMY.sol#281-283) is never used and should be removed
EnumerableSet.values(EnumerableSet.AddressSet) (PMY.sol#248-257) is never used and should be removed
EnumerableSet.values(EnumerableSet.Bytes32Set) (PMY.sol#182-184) is never used and should be removed
EnumerableSet.values(EnumerableSet.UintSet) (PMY.sol#321-330) is never used and should be removed
SafeMath.div(uint256,uint256) (PMY.sol#451-453) is never used and should be removed
SafeMath.div(uint256,uint256,string) (PMY.sol#507-516) is never used and should be removed
SafeMath.mod(uint256,uint256) (PMY.sol#467-469) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (PMY.sol#533-542) is never used and should be removed
SafeMath.mul(uint256,uint256) (PMY.sol#437-439) is never used and should be removed
```

```
SafeMath.sub(uint256,uint256,string) (PMY.sol#484-493) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (PMY.sol#338-344) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (PMY.sol#380-385) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (PMY.sol#392-397) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (PMY.sol#363-373) is never used and should be removed
SafeMath.trySub(uint256,uint256) (PMY.sol#351-356) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Parameter PMY.mint(address,uint256)._to (PMY.sol#1068) is not in mixedCase
Parameter PMY.mint(address,uint256)._amount (PMY.sol#1068) is not in mixedCase
Parameter PMY.addMinter(address)._addMinter (PMY.sol#1080) is not in mixedCase
Parameter PMY.delMinter(address)._delMinter (PMY.sol#1085) is not in mixedCase
Constant PMY.maxSupply (PMY.sol#1057) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
PMY.slitherConstructorConstantVariables() (PMY.sol#1051-1131) uses literals with too many digits:
        - maxSupply = 210000000 * 1e18 (PMY.sol#1057)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
```

```
INFO:Detectors:
PMY.slitherConstructorConstantVariables() (PMY.sol#1051-1131) uses literals with too many digits:
        - maxSupply = 210000000 * 1e18 (PMY.sol#1057)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (PMY.sol#677-679)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (PMY.sol#685-688)
name() should be declared external:
        - ERC20.name() (PMY.sol#728-730)
symbol() should be declared external:
        - ERC20.symbol() (PMY.sol#736-738)
decimals() should be declared external:
        - ERC20.decimals() (PMY.sol#753-755)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (PMY.sol#767-769)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (PMY.sol#779-783)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (PMY.sol#802-806)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (PMY.sol#824-833)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (PMY.sol#847-851)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (PMY.sol#867-876)
mint(address,uint256) should be declared external:
        - PMY.mint(address,uint256) (PMY.sol#1068-1078)
addMinter(address) should be declared external:
        - PMY.addMinter(address) (PMY.sol#1080-1083)
delMinter(address) should be declared external:
        - PMY.delMinter(address) (PMY.sol#1085-1088)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:PMY.sol analyzed (8 contracts with 75 detectors), 55 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Solidity Static Analysis

Security

Inline assembly:

The Contract uses inline assembly, this is only advised in rare cases. Additionally static analysis modules do not parse inline Assembly, this can lead to wrong analysis results.
more
Pos: 252:8:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 1118:16:

Gas & Economy

Gas costs:

Gas requirement of function PMY.transferOwnership is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 685:4:

Gas costs:

Gas requirement of function PMY.mint is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 1068:4:

Gas costs:

Gas requirement of function PMY.setWhiteListAccountsForTransfer is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 1102:4:

For loop over dynamic array:

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs. Carefully test how many items at maximum you can pass to such functions to make it successful.
more
Pos: 1106:8:

Miscellaneous

Constant/View/Pure functions:

EnumerableSet.contains(struct EnumerableSet.Bytes32Set,bytes32) : Is constant but potentially should not be. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 149:4:

Constant/View/Pure functions:

PMY._isMinter(address) : Is constant but potentially should not be. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 1090:4:

Constant/View/Pure functions:

PMY._transfer(address,address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 1111:4:

Similar variable names:

ERC20._burn(address,uint256) : Variables have very similar names "account" and "amount". Note: Modifiers are currently not considered by this static analysis.
Pos: 960:49:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1098:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1117:12:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1127:8:

Delete from dynamic array:

Using "delete" on an array leaves a gap. The length of the array remains the same. If you want to remove the empty position you need to shift items manually and update the "length" property.
more
Pos: 72:12:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 452:15:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 514:19:

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to lost tokens etc.
High	High level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g. public access to crucial functions.
Medium	Medium level vulnerabilities are important to fix; however, they cannot lead to lost tokens.
Low	Low level vulnerabilities are most related to outdated, unused etc. These code snippets cannot have a significant impact on execution.
Lowest Code Style/ Best Practice	Lowest level vulnerabilities, code style violations and information statements cannot affect smart contract execution and can be ignored.

Audit Findings

Critical

No critical severity vulnerabilities were found.

High:

No high severity vulnerabilities were found.

Medium:

No medium severity vulnerabilities were found.

Low:

```
function setOpenSwapTimestamp(uint256 openSwapTimestamp)
external
onlyOwner
{
    require(_openSwapTimestamp != 0, "timestamp invalid");
    _openSwapTimestamp = openSwapTimestamp;
}
```

Require should check the function parameter “openSwapTimestamp” instead of “ _openSwapTimestamp”.

Very Low:

No very low severity vulnerabilities were found.

Conclusion

We were given a contract file and have used all possible tests based on the given object. The contract is written systematically, so it is ready to go for production.

We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

The security state of the reviewed contract is now “ well-secured”.

Note For Contract Users

There are several owner only functions. Those can be called by the owner's wallet only. So, if the owner's wallet is compromised, then it carries the risk of the contract becoming vulnerable.

Owner has full control over the smart contract. Thus, technical auditing does not guarantee the project's ethical side.

Please do your due diligence before investing. Our audit report is never an investment advice.

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyse the feasibility of an attack in a live system.

Suggested Solutions

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinised by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

RD Auditors Disclaimer

The smart contracts given for audit have been analysed in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

Because the total number of test cases are unlimited, the audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only - we recommend proceeding with several independent audits and a public bug bounty program to ensure security of smart contracts.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.

Email: info@rdauditors.com

Website: www.rdauditors.com