AuditAce
FROM INCEPTION TO SUCCESS

# Smart Contract Audit

FOR

# Crypto PepeMines

DATED : 10 May 23'

# AUDIT SUMMARY

**Project name** – Crypto PepeMines

**Date**: 10 May, 2023

**Scope of Audit-** Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

**Audit Status:** Passed

## Issues Found

| Status | Critical | High | Medium | Low | Suggestion |
|---|---|---|---|---|---|
| Open | 0 | 0 | 0 | 1 | 2 |
| Acknowledged | 0 | 0 | 0 | 0 | 0 |
| Resolved | 0 | 0 | 0 | 0 | 0 |

# USED TOOLS

## Tools:

**1- Manual Review:**
a line by line code review has been performed by audit ace team.

**2- BSC Test Network:**
all tests were done on BSC Test network, each test has its transaction has attached to it.

**3- Slither : Static Analysis**

**Testnet Link:** all tests were done using this contract, tests are done on BSC Testnet

https://testnet.bscscan.com/token/0x4Bbe7693380942c505856e72371c6a3f784dF4ca

# Token Information

**Token Name** : Crypto PepeMines

**Token Symbol**: CPM

**Decimals**: 18

**Token Supply**:5,000,000

**Token Address:** -

**Checksum:**
bf50ef6934cc5b1dc376c49e6e5ffe496eb329da

**Owner:** -

# TOKEN OVERVIEW

**Fees:**

Buy Fees: 3 %

Sell Fees: 3 %

Transfer Fees: 3%

**Fees Privilige:** owner

**Ownership** : none

**Minting:** No mint function

**Max Tx Amount/ Max Wallet Amount:** No

**Blacklist: No**

**Other Priviliges**: modifying fees

# AUDIT METHODOLOGY

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code isexercised when we run the test cases.
- Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

# VULNERABILITY CHECKLIST

- [x] Return values of low-level calls
- [x] Private modifier
- [x] Multiple Sends
- [x] Using Suicide
- [x] Gas Limitand Loops
- [x] Address hardcoded
- [x] Exception Disorder
- [x] Using inline assembly
- [x] Divide before multiply
- [x] Missing Zero Address Validation
- [x] Compiler version not fixed
- [x] **Gasless Send**
- [x] Using block.timestamp
- [x] Re-entrancy
- [x] Tautology or contradiction
- [x] Timestamp Dependence
- [x] Revert/require functions
- [x] Use of tx.origin
- [x] Integer overflow/underflow
- [x] Dangerous strict equalities
- [x] Using SHA3
- [x] Using throw

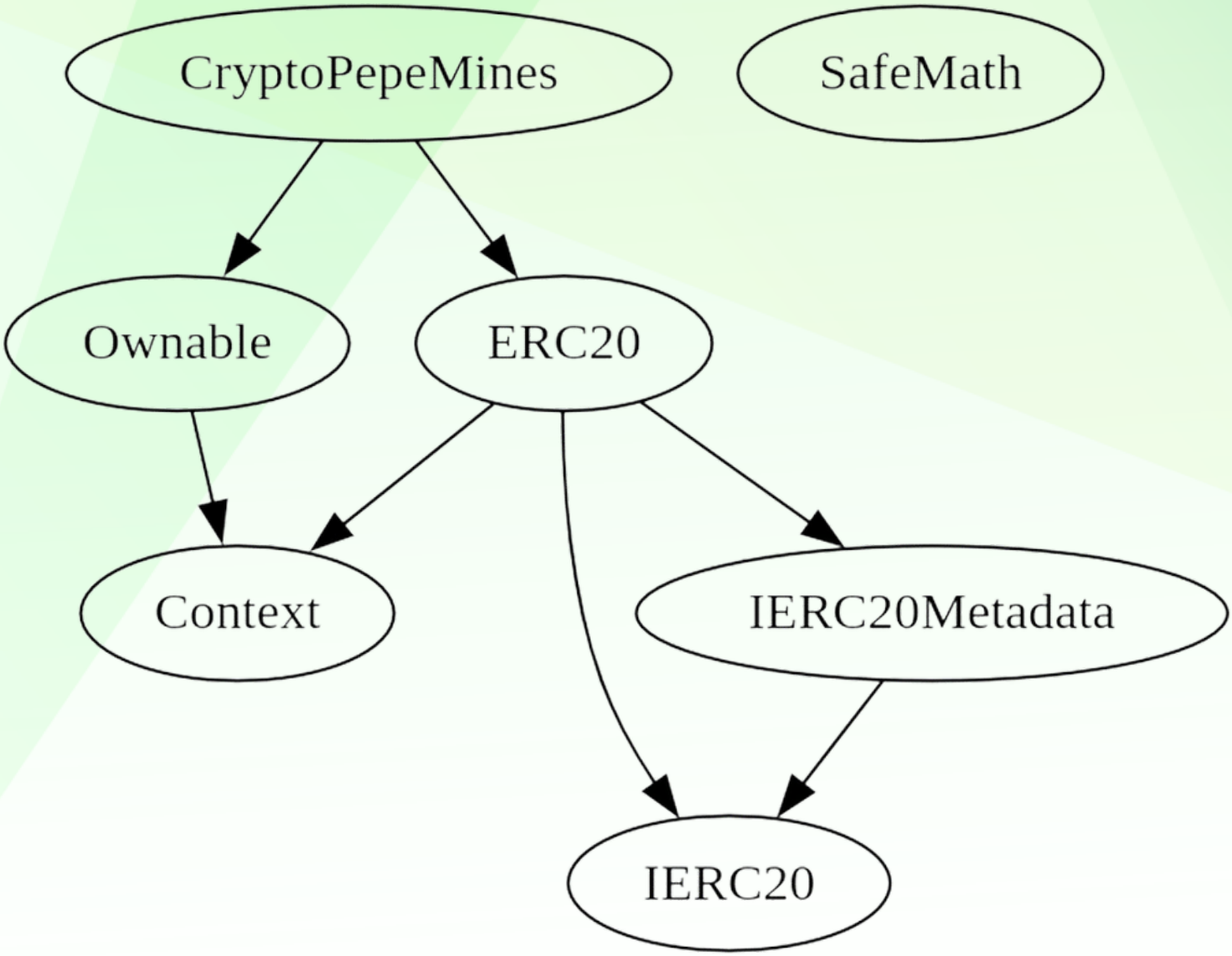
# CLASSIFICATION OF RISK

| Severity | Description |
| --- | --- |
| Critical | These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away. |
| High-Risk | A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way. |
| Medium-Risk | A vulnerability that could affect the desired outcome of executing the contract in a specific scenario. |
| Low-Risk | A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective. |
| Gas Optimization /Suggestion | A vulnerability that has an informational character but is not affecting any of the code. |

# Findings

| Severity | Found |
| --- | --- |
| Critical | 0 |
| High-Risk | 0 |
| Medium-Risk | 0 |
| Low-Risk | 1 |
| Gas Optimization / Suggestions | 2 |

# INHERITANCE TREE



# POINTS TO NOTE

- Owner is not able to set buy/sell/transfer tax over 3% each
- Owner is not able to set a max buy/transfer/wallet/sell amount
- Owner is not able to blacklist an arbitrary wallet
- Owner is not able to disable trades
- Owner is not able to mint new tokens

# CONTRACT ASSESMENT

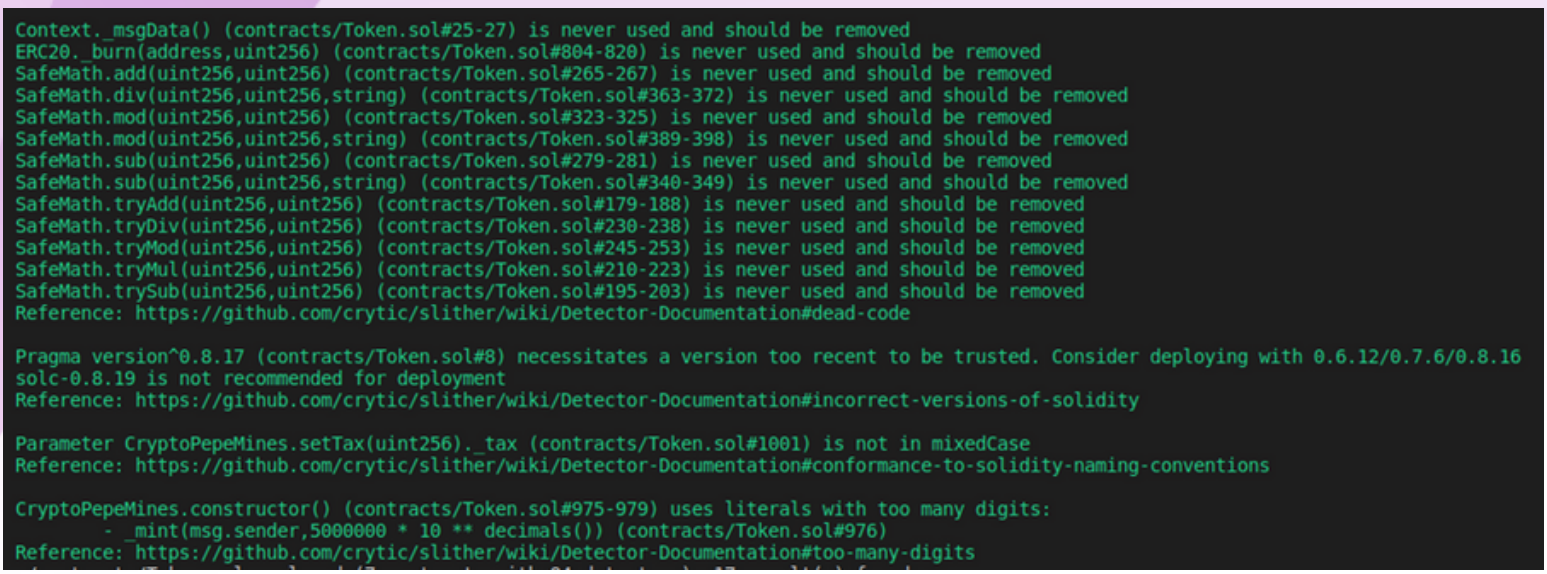
| Contract | Type | Bases | | |
|:---|:---|:---|:---|:---|
| └ | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
| **CryptoPepeMines** | Implementation | ERC20, Ownable | | |
| └ | <Constructor> | Public ❗ | 🛑 | ERC20 |
| └ | setLiquidityContract | External ❗ | 🛑 | onlyOwner |
| └ | setWalletsExcludedFromFee | External ❗ | 🛑 | onlyOwner |
| └ | setTax | External ❗ | 🛑 | onlyOwner |
| └ | _transfer | Internal 🔒 | 🛑 | |
| | | | | |
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata | | |
| └ | <Constructor> | Public ❗ | 🛑 | NO❗ |
| └ | name | Public ❗ | | NO❗ |
| └ | symbol | Public ❗ | | NO❗ |
| └ | decimals | Public ❗ | | NO❗ |
| └ | totalSupply | Public ❗ | | NO❗ |
| └ | balanceOf | Public ❗ | | NO❗ |
| └ | transfer | Public ❗ | 🛑 | NO❗ |
| └ | allowance | Public ❗ | | NO❗ |
| └ | approve | Public ❗ | 🛑 | NO❗ |
| └ | transferFrom | Public ❗ | 🛑 | NO❗ |
| └ | increaseAllowance | Public ❗ | 🛑 | NO❗ |
| └ | decreaseAllowance | Public ❗ | 🛑 | NO❗ |
| └ | _transfer | Internal 🔒 | 🛑 | |
| └ | _mint | Internal 🔒 | 🛑 | |
| └ | _burn | Internal 🔒 | 🛑 | |
| └ | _approve | Internal 🔒 | 🛑 | |
| └ | _spendAllowance | Internal 🔒 | 🛑 | |
| └ | _beforeTokenTransfer | Internal 🔒 | 🛑 | |
| └ | _afterTokenTransfer | Internal 🔒 | 🛑 | |
| | | | | |
| **IERC20** | Interface | | | |
| └ | totalSupply | External ❗ | | NO❗ |
| └ | balanceOf | External ❗ | | NO❗ |
| └ | transfer | External ❗ | 🛑 | NO❗ |
| └ | allowance | External ❗ | | NO❗ |
| └ | approve | External ❗ | 🛑 | NO❗ |
| └ | transferFrom | External ❗ | 🛑 | NO❗ |
| | | | | |
| **IERC20Metadata** | Interface | IERC20 | | |
| └ | name | External ❗ | | NO❗ |
| └ | symbol | External ❗ | | NO❗ |

# CONTRACT ASSESMENT

| └ | decimals | External ❗ | | |NO❗ |
|||||||
| **Context** | Implementation | |||
| └ | _msgSender | Internal 🔒 | | |
| └ | _msgData | Internal 🔒 | | |
|||||||
| **Ownable** | Implementation | Context |||
| └ | <Constructor> | Public ❗ | 🛑 | |NO❗ |
| └ | owner | Public ❗ | | |NO❗ |
| └ | _checkOwner | Internal 🔒 | | |
| └ | renounceOwnership | Public ❗ | 🛑 | onlyOwner |
| └ | transferOwnership | Public ❗ | 🛑 | onlyOwner |
| └ | _transferOwnership | Internal 🔒 | 🛑 | |
|||||||
| **SafeMath** | Library | |||
| └ | tryAdd | Internal 🔒 | | |
| └ | trySub | Internal 🔒 | | |
| └ | tryMul | Internal 🔒 | | |
| └ | tryDiv | Internal 🔒 | | |
| └ | tryMod | Internal 🔒 | | |
| └ | add | Internal 🔒 | | |
| └ | sub | Internal 🔒 | | |
| └ | mul | Internal 🔒 | | |
| └ | div | Internal 🔒 | | |
| └ | mod | Internal 🔒 | | |
| └ | sub | Internal 🔒 | | |
| └ | div | Internal 🔒 | | |
| └ | mod | Internal 🔒 | | |

| Symbol | Meaning |
|:--------:|-----------|
| 🛑 | Function can modify state |
| 💵 | Function is payable |

# STATIC ANALYSIS



```
Context._msgData() (contracts/Token.sol#25-27) is never used and should be removed
ERC20._burn(address,uint256) (contracts/Token.sol#804-820) is never used and should be removed
SafeMath.add(uint256,uint256) (contracts/Token.sol#265-267) is never used and should be removed
SafeMath.div(uint256,uint256,string) (contracts/Token.sol#363-372) is never used and should be removed
SafeMath.mod(uint256,uint256) (contracts/Token.sol#323-325) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (contracts/Token.sol#389-398) is never used and should be removed
SafeMath.sub(uint256,uint256) (contracts/Token.sol#279-281) is never used and should be removed
SafeMath.sub(uint256,uint256,string) (contracts/Token.sol#340-349) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/Token.sol#179-188) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/Token.sol#230-238) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (contracts/Token.sol#245-253) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (contracts/Token.sol#210-223) is never used and should be removed
SafeMath.trySub(uint256,uint256) (contracts/Token.sol#195-203) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.17 (contracts/Token.sol#8) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Parameter CryptoPepeMines.setTax(uint256)._tax (contracts/Token.sol#1001) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

CryptoPepeMines.constructor() (contracts/Token.sol#975-979) uses literals with too many digits:
        - _mint(msg.sender,5000000 * 10 ** decimals()) (contracts/Token.sol#976)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
```

**Result => A static analysis of contract's source code has been performed using slither,**

**No major issues were found in the output**

# FUNCTIONAL TESTING

**Router (PCS V2):**
0xD99D1c33F9fC3444f8101754aBC46c52416550D1

All the functionalities have been tested, no issues were found

**1- Adding liquidity (passed):**
https://testnet.bscscan.com/tx/0x971b9dbfdda14a38a5f2ee9009c5c8bc82858b49dcc245a9a41d7be0c9723381

**2- Buying when excluded (0% tax) (passed):**
https://testnet.bscscan.com/tx/0xed6f8a8ab913c9636143e99da63a9f39f4a0a9c1cbdf51377b11976f6ff1ede8

**3- Selling when excluded (0% tax) (passed):**
https://testnet.bscscan.com/tx/0x66a40fa8cbeb864175168e40263f23569405a47b77911b3e8c2ffd46c876e951

**4- Transferring when excluded (0% tax) (passed):**
https://testnet.bscscan.com/tx/0x19ee4889846f047d74c5c6343a6cf34ccacbd2aec42f4d12900c6d77f786a1bb

**5- Buying when not excluded (3% tax) (passed):**
https://testnet.bscscan.com/tx/0x6bbe8a2d92f6be8fb8ed858f8454519727c83903ef28c6aad68b087bcd568a19

**6- Selling when not excluded (3% tax) (passed):**
https://testnet.bscscan.com/tx/0xe41fb967be70440fcbdb414d765fde6634836b3b419b62e03843647 1ffdc0798

# FUNCTIONAL TESTING

**7- Transferring when not excluded (3% tax) (passed):**
https://testnet.bscscan.com/tx/0x01bc353e07640965bb52d6bce7dd520d25ec9910782e7c59e51b81aa31ee1ea4

# MANUAL TESTING

## Logical – Fee whitlist

**Severity**: Low

**function:** setExcludedFromFee

**Status:** Not Resolved

**Overview:**

if a wallet is excluded from fees, it can not be unexcluded again.

```
function setWalletsExcludedFromFee(address wallet) external onlyOwner {
    require(
        wallet != address(0),
        "address variable can not be zero address"
    );
    require(!isExcludedFromFee[wallet], "This wallet is excluded");
    isExcludedFromFee[wallet] = true;
    emit WalletsExcludedFromFee(wallet);
}
```

**Suggestion**

To mitigate this issue, implement a way to unexclude a wallet from fees

# MANUAL TESTING

## Informational – Stuck ETH

**Status:** Not Resolved

**Overview:**

Currently there is no way to withdraw ETH from the contract

**Suggestion:**

implement a function to be able to withraw ETH from the contract

## Informational – Stuck ERC20 tokens

**Status:** Not Resolved

**Overview:**

ERC20 tokens sent to contract can not be rescued.

**Suggestion:**

implement a function to be able to withraw ERC20 tokens from the contract

# DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.

# ABOUT AUDITACE

We specializes in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.


**https://auditace.tech/**

**https://t.me/Audit_Ace**

**https://twitter.com/auditace_**

**https://github.com/Audit-Ace**