



Smart Contract Audit

FOR
Ketaicoin

DATED : 9 august 23'



MANUAL TESTING

Centralization – Excessive fees

Severity: **High**

function: updateTax

Status: Not Resolved

Overview:

Owner is able to put upto 50% tax on buy and sells separately.

```
function updateTax(uint256 _buyTax, uint256 _sellTax) external onlyOwner {  
    buyTax = _buyTax;  
    sellTax = _sellTax;  
    totalTax = _buyTax + _sellTax;  
    require(buyTax <= 49, "buy Fees cannot exceed 49%");  
    require(sellTax <= 49, "buy Fees cannot exceed 49%");  
    emit UpdateTax(buyTax, sellTax);  
}
```

Suggestion

Consider reducing the upper bound of maximum buy/sell tax. Usually 10% is suggested to be a reasonable upperbound limit for buy/sell/transfer tax.

```
function updateTax(uint256 _buyTax, uint256 _sellTax) external onlyOwner {  
    buyTax = _buyTax;  
    sellTax = _sellTax;  
    totalTax = _buyTax + _sellTax;  
    require(buyTax <= 10, "buy Fees cannot exceed 10%");  
    require(sellTax <= 10, "buy Fees cannot exceed 10%");  
    emit UpdateTax(buyTax, sellTax);  
}
```



AUDIT SUMMARY

Project name -Ketaicoin

Date: 9 august, 2023

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

Audit Status: Passed with High Risk

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	1	0	0	0
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 conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3- Slither :

The code has undergone static analysis using Slither.

Testnet version:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/token/0x346616967C2DD603f6f023155182866f90c2c81A>



Token Information

Token Name : Ketaicoin

Token Symbol: Ketaicoin

Decimals: 18

Token Supply: 8,000,000

Token Address:

0xEF676F869b3F79A56D31Af069e3B1e53B4116D02

Checksum:

9e2bd80d31502d9e11717b040953c2164fd5bdbf

Owner:

0x7e4b3b0078bF47B98420E86B6Db97BE6Cff25C0

(at time of writing the audit)

Deployer:

0x7e4b3b0078bF47B98420E86B6Db97BE6Cff25C0



TOKEN OVERVIEW

Fees:

Buy Fees: 0-49%

Sell Fees: 0-49%

Transfer Fees: 0%

Fees Privilege: owner

Ownership: not owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: no

Blacklist: No

Other Privileges: Initial distribution of the tokens
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 is exercised 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



Return values of low-level calls



Gasless Send



Private modifier



Using block.timestamp



Multiple Sends



Re-entrancy



Using Suicide



Tautology or contradiction



Gas Limit and Loops



Timestamp Dependence



Address hardcoded



Revert/require functions



Exception Disorder



Use of tx.origin



Using inline assembly



Integer overflow/underflow



Divide before multiply



Dangerous strict equalities



Missing Zero Address Validation



Using SHA3



Compiler version not fixed



Using throw



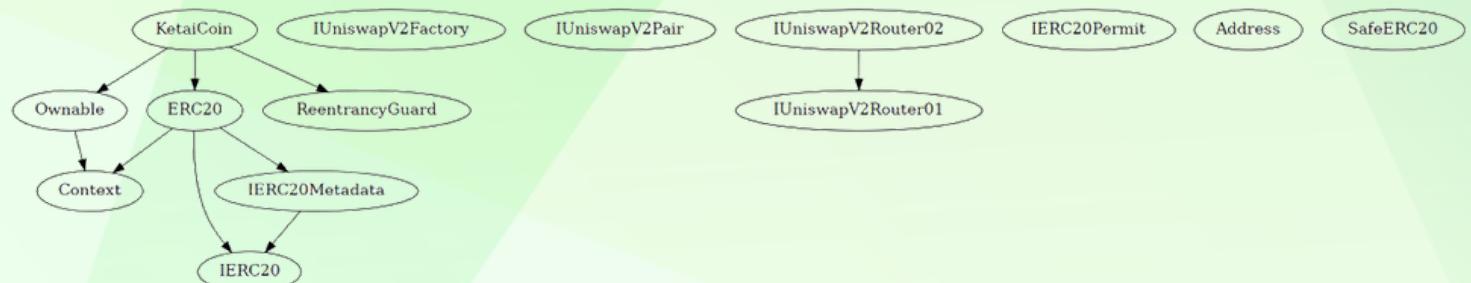
CLASSIFICATION OF RISK

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	1
◆ Medium-Risk	0
◆ Low-Risk	0
◆ Gas Optimization / Suggestions	0

INHERITANCE TREE



POINTS TO NOTE

- Owner is able to update buy and sell fees (0-49%)
- Owner is not able to set fee on transfers
- Owner is not able to blacklist an address
- Owner is not able to set maximum wallet and maximum buy/sell limits
- Owner is not able to mint new tokens
- Owner is not able to disable trades

CONTRACT ASSESSMENT

```

| Contract | Type | Bases |           | |
|---|---|---|---|---|
|   ↳ | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
|           |
|||||||
| **Context** | Implementation | III
| ↳ | _msgSender | Internal 🔒 | II
| ↳ | _msgData | Internal 🔒 | II
|||||||
| **IUniswapV2Factory** | Interface | III
| ↳ | feeTo | External ! | INO ! | | |
| ↳ | feeToSetter | External ! | INO ! |
| ↳ | getPair | External ! | INO ! |
| ↳ | allPairs | External ! | INO ! |
| ↳ | allPairsLength | External ! | INO ! |
| ↳ | createPair | External ! | 🚫 INO ! |
| ↳ | setFeeTo | External ! | 🚫 INO ! |
| ↳ | setFeeToSetter | External ! | 🚫 INO ! |
|||||||
| **IUniswapV2Pair** | Interface | III
| ↳ | name | External ! | INO ! |
| ↳ | symbol | External ! | INO ! |
| ↳ | decimals | External ! | INO ! |
| ↳ | totalSupply | External ! | INO ! |
| ↳ | balanceOf | External ! | INO ! |
| ↳ | allowance | External ! | INO ! |
| ↳ | approve | External ! | 🚫 INO ! |
| ↳ | transfer | External ! | 🚫 INO ! |
| ↳ | transferFrom | External ! | 🚫 INO ! |
| ↳ | DOMAIN_SEPARATOR | External ! | INO ! |

```

CONTRACT ASSESSMENT

```

| └ I PERMIT_TYPEHASH I External ! | INO ! | | | | |
| └ I nonces I External ! | INO ! |
| └ I permit I External ! | ⚡ INO ! |
| └ I MINIMUM_LIQUIDITY I External ! | INO ! |
| └ I factory I External ! | INO ! |
| └ I token0 I External ! | INO ! |
| └ I token1 I External ! | INO ! |
| └ I getReserves I External ! | INO ! |
| └ I price0CumulativeLast I External ! | INO ! |
| └ I price1CumulativeLast I External ! | INO ! |
| └ I kLast I External ! | INO ! |
| └ I mint I External ! | ⚡ INO ! |
| └ I burn I External ! | ⚡ INO ! |
| └ I swap I External ! | ⚡ INO ! |
| └ I skim I External ! | ⚡ INO ! |
| └ I sync I External ! | ⚡ INO ! |
| └ I initialize I External ! | ⚡ INO ! |
|||||||
| **IUniswapV2Router01** I Interface | ||
| └ I factory I External ! | INO ! |
| └ I WETH I External ! | INO ! |
| └ I addLiquidity I External ! | ⚡ INO ! |
| └ I addLiquidityETH I External ! | ⚡ INO ! |
| └ I removeLiquidity I External ! | ⚡ INO ! |
| └ I removeLiquidityETH I External ! | ⚡ INO ! |
| └ I removeLiquidityWithPermit I External ! | ⚡ INO ! |
| └ I removeLiquidityETHWithPermit I External ! | ⚡ INO ! |
| └ I swapExactTokensForTokens I External ! | ⚡ INO ! |
| └ I swapTokensForExactTokens I External ! | ⚡ INO ! |
| └ I swapExactETHForTokens I External ! | ⚡ INO ! |
| └ I swapTokensForExactETH I External ! | ⚡ INO ! |
| └ I swapExactTokensForETH I External ! | ⚡ INO ! |

```

CONTRACT ASSESSMENT

```

| └ I swapETHForExactTokens | External ! | 📈 INO ! | |
| └ I quote | External ! | INO ! |
| └ I getAmountOut | External ! | INO ! |
| └ I getAmountIn | External ! | INO ! |
| └ I getAmountsOut | External ! | INO ! |
| └ I getAmountsIn | External ! | INO ! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 ||
| └ I removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ⚡️
INO ! |
| └ I removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External !
| External ! | ⚡️ INO ! |
| └ I swapExactTokensForTokensSupportingFeeOnTransferTokens | External !
| ⚡️ INO ! |
| └ I swapExactETHForTokensSupportingFeeOnTransferTokens | External !
| 📈 INO ! |
| └ I swapExactTokensForETHSupportingFeeOnTransferTokens | External !
| ⚡️ INO ! |
|||||
| **IERC20Permit** | Interface | ||
| └ I permit | External ! | ⚡️ INO ! |
| └ I nonces | External ! | INO ! |
| └ I DOMAIN_SEPARATOR | External ! | INO ! |
|||||
| **Address** | Library | ||
| └ I isContract | Internal 🔒 | ||
| └ I sendValue | Internal 🔒 | ⚡️ ||
| └ I functionCall | Internal 🔒 | ⚡️ ||
| └ I functionCall | Internal 🔒 | ⚡️ ||
| └ I functionCallWithValue | Internal 🔒 | ⚡️ ||
| └ I functionCallWithValue | Internal 🔒 | ⚡️ ||
| └ I functionStaticCall | Internal 🔒 | ||
| └ I functionStaticCall | Internal 🔒 | ||
| └ I functionDelegateCall | Internal 🔒 | ⚡️ ||

```

CONTRACT ASSESSMENT

```

| └| functionDelegateCall | Internal 🔒 | ⚡ | 
| └| verifyCallResultFromTarget | Internal 🔒 | 
| └| verifyCallResult | Internal 🔒 | 
| └| _revert | Private 🔒 | 
|||||
| **IERC20** | Interface | 
| └| totalSupply | External ! | NO ! | 
| └| balanceOf | External ! | NO ! | 
| └| transfer | External ! | ⚡ NO ! | 
| └| allowance | External ! | NO ! | 
| └| approve | External ! | ⚡ NO ! | 
| └| transferFrom | External ! | ⚡ NO ! | 
|||||
| **SafeERC20** | Library | 
| └| safeTransfer | Internal 🔒 | ⚡ | 
| └| safeTransferFrom | Internal 🔒 | ⚡ | 
| └| safeApprove | Internal 🔒 | ⚡ | 
| └| safeIncreaseAllowance | Internal 🔒 | ⚡ | 
| └| safeDecreaseAllowance | Internal 🔒 | ⚡ | 
| └| safePermit | Internal 🔒 | ⚡ | 
| └| _callOptionalReturn | Private 🔒 | ⚡ | 
|||||
| **IERC20Metadata** | Interface | IERC20 | 
| └| name | External ! | NO ! | 
| └| symbol | External ! | NO ! | 
| └| decimals | External ! | NO ! | 
|||||
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata | 
| └| <Constructor> | Public ! | ⚡ NO ! | 
| └| name | Public ! | NO ! | 
| └| symbol | Public ! | NO ! | 
| └| decimals | Public ! | NO ! | 
| └| totalSupply | Public ! | NO ! | 

```

CONTRACT ASSESSMENT

```

| └ I balanceOf I Public ! | INO ! | | |
| └ I transfer I Public ! | 🔒 INO ! |
| └ I allowance I Public ! | INO ! |
| └ I approve I Public ! | 🔒 INO ! |
| └ I transferFrom I Public ! | 🔒 INO ! |
| └ I increaseAllowance I Public ! | 🔒 INO ! |
| └ I decreaseAllowance I Public ! | 🔒 INO ! |
| └ I _transfer I Internal 🔒 | 🔒 ||
| └ I _mint I Internal 🔒 | 🔒 ||
| └ I _burn I Internal 🔒 | 🔒 ||
| └ I _approve I Internal 🔒 | 🔒 ||
| └ I _spendAllowance I Internal 🔒 | 🔒 ||
| └ I _beforeTokenTransfer I Internal 🔒 | 🔒 ||
| └ I _afterTokenTransfer I Internal 🔒 | 🔒 ||
|||||
| **Ownable** I Implementation I Context III
| └ I <Constructor> I Public ! | 🔒 INO ! | | |
| └ I owner I Public ! | INO ! |
| └ I _checkOwner I Internal 🔒 | ||
| └ I renounceOwnership I Public ! | 🔒 I onlyOwner |
| └ I transferOwnership I Public ! | 🔒 I onlyOwner |
| └ I _transferOwnership I Internal 🔒 | 🔒 ||
|||||
| **ReentrancyGuard** I Implementation I III
| └ I <Constructor> I Public ! | 🔒 INO ! | | |
| └ I _nonReentrantBefore I Private 🔒 | 🔒 ||
| └ I _nonReentrantAfter I Private 🔒 | 🔒 ||
| └ I _reentrancyGuardEntered I Internal 🔒 | ||
|||||
| **KetaiCoin** I Implementation I ERC20, Ownable, ReentrancyGuard III
| └ I <Constructor> I Public ! | 🔒 I ERC20 |
| └ I <Receive Ether> I External ! | 💸 INO ! |
| └ I <Fallback> I External ! | 💸 INO ! |

```

CONTRACT ASSESSMENT

```

| └ I getRouterAddress | Public ! | INO ! | | |
| └ I claimStuckTokens | External ! | ⚡ | onlyOwner |
| └ I excludeFromFees | External ! | ⚡ | onlyOwner |
| └ I isExcludedFromFees | Public ! | INO ! |
| └ I setAutomatedMarketMakerPair | Public ! | ⚡ | onlyOwner |
| └ I isAutomatedMarketMakerPair | Public ! | INO ! |
| └ I updateTax | External ! | ⚡ | onlyOwner |
| └ I toggleSwapBack | External ! | ⚡ | onlyOwner |
| └ I setSwapTokensAtAmount | External ! | ⚡ | onlyOwner |
| └ I _transfer | Internal 🔒 | ⚡ |||
| └ I ForceSwapBack | External ! | ⚡ | INO ! |
| └ I _autoswapBack | Internal 🔒 | ⚡ |||
| └ I outBNB | Internal 🔒 | ⚡ | nonReentrant |

```

Legend

I Symbol	I Meaning
:-----: -----	
⚡	Function can modify state
💸	Function is payable



STATIC ANALYSIS

```
INFO:Detectors:
Pragma version0.8.17 (contracts/Token.sol#7) allows old versions
solc-0.8.17 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) (contracts/Token.sol#372-383):
- (success) = recipient.call(value: amount)() (contracts/Token.sol#378)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#420-440):
- (success,returnData) = target.call{value: value}(data) (contracts/Token.sol#430-432)
Low level call in Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#454-467):
- (success,returnData) = target.staticcall(data) (contracts/Token.sol#459)
Low level call in Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#481-494):
- (success,returnData) = target.delegatecall(data) (contracts/Token.sol#486)
Low level call in KetaiCoin.outBNB(address,uint256) (contracts/Token.sol#198-1207):
- (success) = address(_to).call{value: amount}() (contracts/Token.sol#1204)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#83) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#85) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#116) is not in mixedCase
Function IERC20Permit.DOMAIN_SEPARATOR() (contracts/Token.sol#158) is not in mixedCase
Parameter KetaiCoin.updateTax(uint256,uint256)_buyTax (contracts/Token.sol#1082) is not in mixedCase
Parameter KetaiCoin.updateTax(uint256,uint256)_sellTax (contracts/Token.sol#1082) is not in mixedCase
Function KetaiCoin.ForceSwapBack() (contracts/Token.sol#1162-1168) is not in mixedCase
Parameter KetaiCoin.outBNB(address,uint256)._to (contracts/Token.sol#1198) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#163) is too similar to IUniswapV2Router01.ad
dLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#164)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
KetaiCoin.marketingWallet (contracts/Token.sol#965) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
KetaiCoin.marketingWalletShares (contracts/Token.sol#967) should be immutable
KetaiCoin.setSwapTokensLimit (contracts/Token.sol#970) should be immutable
KetaiCoin.taxDenominator (contracts/Token.sol#960) should be immutable
KetaiCoin.uniswapV2Pair (contracts/Token.sol#975) should be immutable
KetaiCoin.uniswapV2Router (contracts/Token.sol#974) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```

**Result => A static analysis of contract's source code has been performed using slither,
No major issues were found in the output**



FUNCTIONAL TESTING

1- Adding liquidity (**passed**):

<https://testnet.bscscan.com/tx/0xf7241f4d2db9d9b4b36f936bfd75bc99172dab83eeda1da7c6d800f2030be92>

2- Buying when excluded from fees (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xd8d7059e671b86b2fd6f53168af1554d1d5353b457490b1f291fe4db2c0683ca>

3- Selling when excluded from fees (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x512fbb3f30f370597ae0b74dc1889cba28449df04ede3f0ca5f177c0c5a4f32>

4- Transferring when excluded from fees (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x5cca435a21bd976afc5792f082cf5ff1824ac5bf7465903f744dd994706d22a5>

5- Buying when not excluded from fees (0-49% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x1a0384d775093abeeca9b219335af0d4794a394a92f5071b314a2a6858925215>

6- Selling when not excluded from fees (0-49% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x4a7fc91a6848f894cacda471387240f563545a6a4c7d011e08d0e41f8842621b>



FUNCTIONAL TESTING

7- Transferring (0% tax) (passed):

<https://testnet.bscscan.com/tx/0xca4ad4aa0f81f26e58506bf61e651a32c837cf973614014a028104896d09116>

8- Internal swap(ETH sent to marketing wallet) (passed):

<https://testnet.bscscan.com/tx/0x4a7fc91a6848f894cacda471387240f563545a6a4c7d011e08d0e41f8842621b>



MANUAL TESTING

Centralization – Excessive fees

Severity: **High**

function: updateTax

Status: Not Resolved

Overview:

Owner is able to put upto 50% tax on buy and sells separately.

```
function updateTax(uint256 _buyTax, uint256 _sellTax) external onlyOwner {  
    buyTax = _buyTax;  
    sellTax = _sellTax;  
    totalTax = _buyTax + _sellTax;  
    require(buyTax <= 49, "buy Fees cannot exceed 49%");  
    require(sellTax <= 49, "buy Fees cannot exceed 49%");  
    emit UpdateTax(buyTax, sellTax);  
}
```

Suggestion

Consider reducing the upper bound of maximum buy/sell tax. Usually 10% is suggested to be a reasonable upperbound limit for buy/sell/transfer tax.

```
function updateTax(uint256 _buyTax, uint256 _sellTax) external onlyOwner {  
    buyTax = _buyTax;  
    sellTax = _sellTax;  
    totalTax = _buyTax + _sellTax;  
    require(buyTax <= 10, "buy Fees cannot exceed 10%");  
    require(sellTax <= 10, "buy Fees cannot exceed 10%");  
    emit UpdateTax(buyTax, sellTax);  
}
```



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 specialize 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>
