



Smart Contract Audit

FOR
DETA
DATED : 23 July 23'



MANUAL TESTING

Centralization – swaps are disabled by default

Severity: **High**

function: enableTrading

Status: Not Resolved

Overview:

The smart contract owner must enable trades for holders. If trading remain disabled, no one would be able to buy/sell/transfer tokens.

```
function enableTrading() external onlyOwner {  
    require(!tradingEnabled, "Trading is already enabled");  
    tradingEnabled = true;  
}
```

Suggestion

To mitigate this centralization issue, we propose the following options:

1. Renounce Ownership: Consider relinquishing control of the smart contract by renouncing ownership. This would remove the ability for a single entity to manipulate the router, reducing centralization risks.
2. Multi-signature Wallet: Transfer ownership to a multi-signature wallet. This would require multiple approvals for any changes to the mainRouter, adding an additional layer of security and reducing the centralization risk.
3. Transfer ownership to a trusted and valid 3rd party in order to guarantee enabling of the trades



AUDIT SUMMARY

Project name -DETA

Date: 23 July, 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/0x4Cd3b2546716731906Ec4b3519b7FFA9d8e27346>



Token Information

Token Name : Deta Finance

Token Symbol: DETA

Decimals: 18

Token Supply: 800,000,000

Token Address:

0xA122253EE92A42Bd7de40aCe38c3248B6f425ce3

Checksum:

4288d966137e156f7e6ec06092b873817bd9da58

Owner:

0x81977cf2e9Ac85b51B289399ADdEB71e73cDc7a6

(at time of writing the audit)

Deployer:

0x81977cf2e9Ac85b51B289399ADdEB71e73cDc7a6



TOKEN OVERVIEW

Fees:

Buy Fees: 3%

Sell Fees: 3%

Transfer Fees: 0%

Fees Privilege: owner

Ownership: owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: no

Blacklist: No

Other Privileges: Initial distribution of the tokens enabling trades



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



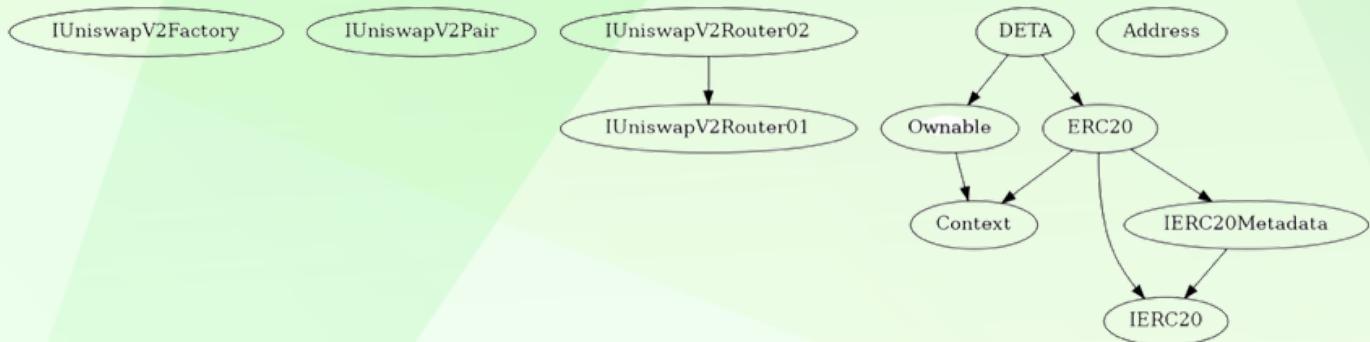
CLASSIFICATION OF RISK

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 not able to change fees (3% for each type of tax)
- Owner is not able to set transfer fees (0% transfer fees)
- Owner is not able to blacklist an arbitrary address.
- Owner is not able to disable trades
- Owner is not able to mint new tokens
- **Owner must enable trades manually**

CONTRACT ASSESSMENT

Contract	Type	Bases		
└ **Function Name** **Visibility** **Mutability** **Modifiers**				
IUniswapV2Factory Interface				
L feeTo External ! NO !				
L feeToSetter External ! NO !				
L getPair External ! NO !				
L allPairs External ! NO !				
L allPairsLength External ! NO !				
L createPair External !  NO !				
L setFeeTo External !  NO !				
L setFeeToSetter External !  NO !				
IUniswapV2Pair Interface				
L name External ! NO !				
L symbol External ! NO !				
L decimals External ! NO !				
L totalSupply External ! NO !				
L balanceOf External ! NO !				
L allowance External ! NO !				
L approve External !  NO !				
L transfer External !  NO !				
L transferFrom External !  NO !				
L DOMAIN_SEPARATOR External ! NO !				
L PERMIT_TYPEHASH External ! NO !				
L nonces External ! NO !				
L permit External !  NO !				
L MINIMUM_LIQUIDITY External ! NO !				
L factory External ! NO !				
L token0 External ! NO !				

CONTRACT ASSESSMENT

```

| L | token1 | External ! | NO ! | |
| L | getReserves | External ! | NO ! |
| L | price0CumulativeLast | External ! | NO ! |
| L | price1CumulativeLast | External ! | NO ! |
| L | kLast | External ! | NO ! |
| L | mint | External ! | ⚡ | NO ! |
| L | burn | External ! | ⚡ | NO ! |
| L | swap | External ! | ⚡ | NO ! |
| L | skim | External ! | ⚡ | NO ! |
| L | sync | External ! | ⚡ | NO ! |
| L | initialize | External ! | ⚡ | NO ! |
|||||
| **IUniswapV2Router01** | Interface | ||
| L | factory | External ! | NO ! |
| L | WETH | External ! | NO ! |
| L | addLiquidity | External ! | ⚡ | NO ! |
| L | addLiquidityETH | External ! | 💸 | NO ! |
| L | removeLiquidity | External ! | ⚡ | NO ! |
| L | removeLiquidityETH | External ! | ⚡ | NO ! |
| L | removeLiquidityWithPermit | External ! | ⚡ | NO ! |
| L | removeLiquidityETHWithPermit | External ! | ⚡ | NO ! |
| L | swapExactTokensForTokens | External ! | ⚡ | NO ! |
| L | swapTokensForExactTokens | External ! | ⚡ | NO ! |
| L | swapExactETHForTokens | External ! | 💸 | NO ! |
| L | swapTokensForExactETH | External ! | ⚡ | NO ! |
| L | swapExactTokensForETH | External ! | ⚡ | NO ! |
| L | swapETHForExactTokens | External ! | 💸 | NO ! |
| L | quote | External ! | NO ! |
| L | getAmountOut | External ! | NO ! |
| L | getAmountIn | External ! | NO ! |
| L | getAmountsOut | External ! | NO !

```

CONTRACT ASSESSMENT

```

| L | getAmountsIn | External ! | NO ! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 ||
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | 🔴 |
NO ! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External !
| 🔴 | NO ! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External !
| 🔴 | NO ! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External !
| 🔴 | NO ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External !
| 🔴 | NO ! |
NO ! |
||||| |
| **IERC20** | Interface | ||
| L | totalSupply | External ! | NO ! |
| L | balanceOf | External ! | NO ! |
| L | transfer | External ! | 🔴 | NO ! |
| L | allowance | External ! | NO ! |
| L | approve | External ! | 🔴 | NO ! |
| L | transferFrom | External ! | 🔴 | NO ! |
|||||
| **IERC20Metadata** | Interface | IERC20 ||
| L | name | External ! | NO ! |
| L | symbol | External ! | NO ! |
| L | decimals | External ! | NO ! |
|||||
| **Address** | Library | ||
| L | isContract | Internal 🔒 | ||
| L | sendValue | Internal 🔒 | 🔴 ||
| L | functionCall | Internal 🔒 | 🔴 ||
| L | functionCall | Internal 🔒 | 🔴 ||
| L | functionCallWithValue | Internal 🔒 | 🔴 ||

```

CONTRACT ASSESSMENT

```

| L | functionCallWithValue | Internal 🔒 | ⚡ ||

| L | functionStaticCall | Internal 🔒 | ||

| L | functionStaticCall | Internal 🔒 | ||

| L | functionDelegateCall | Internal 🔒 | ⚡ ||

| L | functionDelegateCall | Internal 🔒 | ⚡ ||

| L | verifyCallResultFromTarget | Internal 🔒 | ||

| L | verifyCallResult | Internal 🔒 | ||

| L | _revert | Private 🔒 | ||

|||||  

| **Context** | Implementation | |||  

| L | _msgSender | Internal 🔒 | |||  

| L | _msgData | Internal 🔒 | |||  

|||||  

| **Ownable** | Implementation | Context |||  

| L | <Constructor> | Public ! | ⚡ | NO ! |  

| L | owner | Public ! | | NO ! |  

| L | renounceOwnership | Public ! | ⚡ | onlyOwner |  

| L | transferOwnership | Public ! | ⚡ | onlyOwner |  

|||||  

| **ERC20** | Implementation | Context, IERC20, IERC20Metadata |||  

| L | <Constructor> | Public ! | ⚡ | NO ! |  

| L | name | Public ! | | NO ! |  

| L | symbol | Public ! | | NO ! |  

| L | decimals | Public ! | | NO ! |  

| L | totalSupply | Public ! | | NO ! |  

| L | balanceOf | Public ! | | NO ! |  

| L | transfer | Public ! | ⚡ | NO ! |  

| L | allowance | Public ! | | NO ! |  

| L | approve | Public ! | ⚡ | NO ! |  

| L | transferFrom | Public ! | ⚡ | NO ! |  

| L | increaseAllowance | Public ! | ⚡ | NO ! |  

| L | decreaseAllowance | Public ! | ⚡ | NO ! |

```

CONTRACT ASSESSMENT

```

| L | _transfer | Internal 🔒 | 🚫 ||

| L | _mint | Internal 🔒 | 🚫 ||

| L | _burn | Internal 🔒 | 🚫 ||

| L | _approve | Internal 🔒 | 🚫 ||

| L | _beforeTokenTransfer | Internal 🔒 | 🚫 ||

| L | _afterTokenTransfer | Internal 🔒 | 🚫 ||

||||||

| **DETA** | Implementation | ERC20, Ownable |||


| L | <Constructor> | Public ! | 🚫 | ERC20 |

| L | <Receive Ether> | External ! | 💸 | NO ! |

| L | claimStuckTokens | External ! | 🚫 | onlyOwner |

| L | excludeFromFees | External ! | 🚫 | onlyOwner |

| L | isExcludedFromFees | Public ! | | NO ! |

| L | changeMarketingWallet | External ! | 🚫 | onlyOwner |

| L | enableTrading | External ! | 🚫 | onlyOwner |

| L | _transfer | Internal 🔒 | 🚫 ||

| L | setSwapTokensAtAmount | External ! | 🚫 | onlyOwner |

| L | swapAndLiquify | Private 💰 | 🚫 ||

| L | swapAndSendMarketing | Private 💰 | 🚫 ||


```

Legend

Symbol	Meaning
-----	-----
🚫	Function can modify state
💸	Function is payable



STATIC ANALYSIS

Pragma version^0.8.17 (contracts/Token.sol#19) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.20 is not recommended for deployment
Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity>

Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#319-324):
- (success) = recipient.call{value: amount}() (contracts/Token.sol#322)

Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (contracts/Token.sol#382-389):
- (success,returnData) = target.call{value: value}(data) (contracts/Token.sol#387)

Low level call in Address.functionStaticCall(address,bytes,string) (contracts/Token.sol#407-414):
- (success,returnData) = target.staticcall(data) (contracts/Token.sol#412)

Low level call in Address.functionDelegateCall(address,bytes,string) (contracts/Token.sol#432-438):
- (success,returnData) = target.delegatecall(data) (contracts/Token.sol#436)

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls>

Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#49) is not in mixedCase

Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#50) is not in mixedCase

Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#68) is not in mixedCase

Function IUniswapV2Router01.WETH() (contracts/Token.sol#88) is not in mixedCase

Parameter DETA.changeMarketingWallet(address).marketingWallet (contracts/Token.sol#779) is not in mixedCase

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions>

Redundant expression "this (contracts/Token.sol#503)" inContext (contracts/Token.sol#497-506)

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements>

Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#93) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#94)

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar>

DETA.constructor() (contracts/Token.sol#710-752) uses literals with too many digits:

- _mint(newOwner,800000000 * (10 ** decimals())) (contracts/Token.sol#750)

DETA.setSwapTokensAtAmount(uint256) (contracts/Token.sol#847-851) uses literals with too many digits:

- require(bool,string)(newAmount > totalSupply() / 1000000,SwapTokensAtAmount must be greater than 0.0001% of total supply) (contracts/Token.sol#848)

)

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits>

DETA._totalFeesOnBuy (contracts/Token.sol#692) should be immutable

DETA._totalFeesOnSell (contracts/Token.sol#693) should be immutable

DETA.liquidityFeeOnBuy (contracts/Token.sol#686) should be immutable

DETA.liquidityFeeOnSell (contracts/Token.sol#687) should be immutable

DETA.marketingFeeOnBuy (contracts/Token.sol#689) should be immutable

DETA.marketingFeeOnSell (contracts/Token.sol#690) should be immutable

DETA.uniswapV2Pair (contracts/Token.sol#682) should be immutable

DETA.uniswapV2Router (contracts/Token.sol#681) should be immutable

DETA.walletToWalletTransferFee (contracts/Token.sol#695) 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/0x9fc66686b2ba6b58924471279150db33cc2ee099494dc4dbeb88c45d95c7a89f>

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

<https://testnet.bscscan.com/tx/0xf034aa7705eaea153931ad7166b9cc74b8435ea52231be528e5e8b23f981586d>

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

<https://testnet.bscscan.com/tx/0x6f4d1775ebff936f11117de815a5f4e82e041cabb47f5b5296e38ea13d86a48c>

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

<https://testnet.bscscan.com/tx/0x9def79eedfe4163f9e78537bf2ed405358baab76becf93be5870bdf2b557f534>

5- Buying when not excluded from fees (3% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x79d5b4b3ba9c0a550f3281db959a17b55b06c76f06c9c52f27eb6bdf435f054e>

6- Selling when not excluded from fees (3% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x8e3814d6b7ca113a06e02dc2b65b128bffcaf8e8986be77d16b5ef2b3add3164>



FUNCTIONAL TESTING

7- Transferring when not excluded from fees (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x711053021013f25fe8661ba7281cd889b94ae9a067a1fd80a1dee5f1747ff7ff>

8- Internal swap (passed):

<https://testnet.bscscan.com/address/0x81977cf2e9ac85b51b289399addeb71e73cdc7a6#internaltx>



MANUAL TESTING

Centralization – swaps are disabled by default

Severity: High

function: enableTrading

Status: Not Resolved

Overview:

The smart contract owner must enable trades for holders. If trading remain disabled, no one would be able to buy/sell/transfer tokens.

```
function enableTrading() external onlyOwner {  
    require(!tradingEnabled, "Trading is already enabled");  
    tradingEnabled = true;  
}
```

Suggestion

To mitigate this centralization issue, we propose the following options:

1. Renounce Ownership: Consider relinquishing control of the smart contract by renouncing ownership. This would remove the ability for a single entity to manipulate the router, reducing centralization risks.
2. Multi-signature Wallet: Transfer ownership to a multi-signature wallet. This would require multiple approvals for any changes to the mainRouter, adding an additional layer of security and reducing the centralization risk.
3. Transfer ownership to a trusted and valid 3rd party in order to guarantee enabling of the trades



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>
