AuditAce

FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

ALT CRYPTO

DATED : 24 August 23'

AUDIT SUMMARY

Project name – ALT CRYPTO

Date: 24 August 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	0	1
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/address/0x30cCd4CeD5bb60e6CA065D17e8A315EEa0e5E574

Token Information

Token Address :
0xb8927b3ee00e9aded1431feea6975795403873ef

Name: ALT CRYPTO

Symbol: ALTC

Decimals: 18

Netowrk: BSC

Token Type: BEP20

Owner: 0xB0F969d7B93Cc11B9a479F094C058889a3B8b94F
(at time of writing the audit)

Deployer:
0xB0F969d7B93Cc11B9a479F094C058889a3B8b94F

Token Supply: 10,000,000,000

Checksum:
fa17c9f5736affaf74cb2b9343cf49e4888f335b

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/address/0x30cCd4CeD5bb60e6C
A065D17e8A315EEa0e5E574

TOKEN OVERVIEW

buy fee: 0%

Sell fee: 2%

transfer fee: 0%

Fee Privilege: Static fees

Ownership: Owned

Minting: None

Max Tx: No

Blacklist: No

Other Privileges:

- Initial distribution of the tokens

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

- ✅ Return values of low-level calls
- ✅ Private modifier
- ✅ Multiple Sends
- ✅ Using Suicide
- ✅ Gas Limitand Loops
- ✅ Address hardcoded
- ✅ Exception Disorder
- ✅ Using inline assembly
- ✅ Divide before multiply
- ✅ Missing Zero Address Validation
- ✅ Compiler version not fixed

- ✅ **Gasless Send**
- ✅ Using block.timestamp
- ✅ Re-entrancy
- ✅ Tautology or contradiction
- ✅ Timestamp Dependence
- ✅ Revert/require functions
- ✅ Use of tx.origin
- ✅ Integer overflow/underflow
- ✅ Dangerous strict equalities
- ✅ Using SHA3
- ✅ 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.
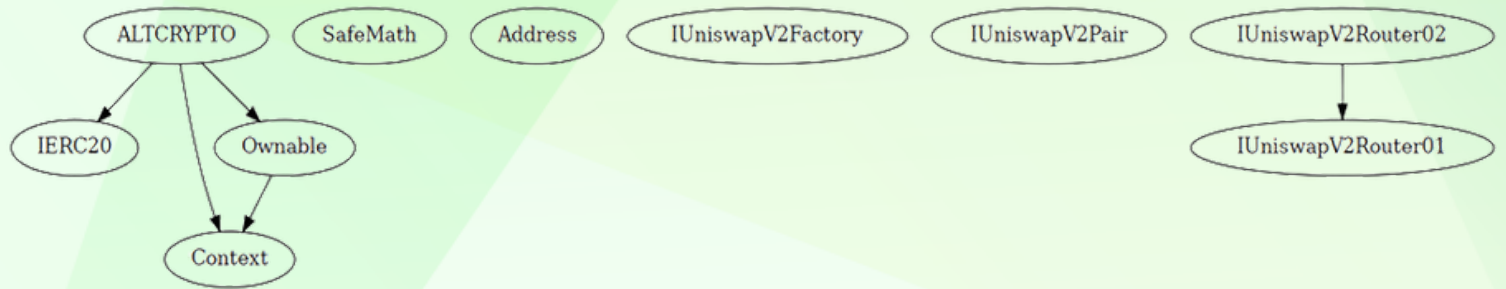
Findings

Severity

Found

◆ **Critical**

0

◆ **High-Risk**

0

◆ **Medium-Risk**

0

◆ **Low-Risk**

0

◆ **Gas Optimization / Suggestions**

1

INHERITANCE TREE

POINTS TO NOTE

- Owner is not able to change currrnt fees (0% buy/

2% sell / 0% transfer)

- Owner is not able to blacklist an arbitrary address.

- Owner is not able to disable trades

- Owner is not able to limit buy/sell/transfer/wallet

amounts

- Owner is not able to mint new tokens

STATIC ANALYSIS


```
Parameter ALTCRYPTO.calculateRnDFee(uint256)._amount (contracts/Token.sol#1271) is not in mixedCase
Parameter ALTCRYPTO.calculateBurnFee(uint256)._amount (contracts/Token.sol#1275) is not in mixedCase
Parameter ALTCRYPTO.withdrawToken(address,uint256)._tokenContract (contracts/Token.sol#1511) is not in mixedCase
Parameter ALTCRYPTO.withdrawToken(address,uint256)._amount (contracts/Token.sol#1512) is not in mixedCase
Variable ALTCRYPTO._marketingTax (contracts/Token.sol#875-876) is not in mixedCase
Variable ALTCRYPTO._burnTax (contracts/Token.sol#877-878) is not in mixedCase
Variable ALTCRYPTO._RnDTax (contracts/Token.sol#879-880) is not in mixedCase
Variable ALTCRYPTO._RnDFee (contracts/Token.sol#906) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Redundant expression "this (contracts/Token.sol#266)" inContext (contracts/Token.sol#260-269)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#667) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,
uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#668)
Variable ALTCRYPTO._getRValues(uint256,uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1208-1212) is too similar to ALTCRYPTO._transferFromExcluded(address,address,uint256).tTransferAmount (contracts
/Token.sol#1447)
Variable ALTCRYPTO._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1394) is too similar to ALTCRYPTO._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1417)
Variable ALTCRYPTO._getRValues(uint256,uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1208-1212) is too similar to ALTCRYPTO._transferToExcluded(address,address,uint256).tTransferAmount (contracts/T
oken.sol#1417)
Variable ALTCRYPTO._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1423) is too similar to ALTCRYPTO._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1388)
Variable ALTCRYPTO._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1453) is too similar to ALTCRYPTO._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1417)
Variable ALTCRYPTO._getRValues(uint256,uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1208-1212) is too similar to ALTCRYPTO._transferStandard(address,address,uint256).tTransferAmount (contracts/Tok
en.sol#1388)
Variable ALTCRYPTO._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1423) is too similar to ALTCRYPTO._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1417)
Variable ALTCRYPTO._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1483) is too similar to ALTCRYPTO._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1417)
Variable ALTCRYPTO._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1453) is too similar to ALTCRYPTO._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1388)
Variable ALTCRYPTO._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1483) is too similar to ALTCRYPTO._getTValues(uint256).tTransferAmount (contracts/Token.sol#1188)
Variable ALTCRYPTO._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1453) is too similar to ALTCRYPTO._getTValues(uint256).tTransferAmount (contracts/Token.sol#1188)
Variable ALTCRYPTO._getRValues(uint256,uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1208-1212) is too similar to ALTCRYPTO._transferBothExcluded(address,address,uint256).tTransferAmount (contracts
/Token.sol#1477)
Variable ALTCRYPTO._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1483) is too similar to ALTCRYPTO._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1388)
Variable ALTCRYPTO._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1394) is too similar to ALTCRYPTO._getTValues(uint256).tTransferAmount (contracts/Token.sol#1188)
Variable ALTCRYPTO._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1394) is too similar to ALTCRYPTO._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1388)
Variable ALTCRYPTO._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1423) is too similar to ALTCRYPTO._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1477)
Variable ALTCRYPTO._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1483) is too similar to ALTCRYPTO._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1477)
Variable ALTCRYPTO._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1453) is too similar to ALTCRYPTO._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1477)
Variable ALTCRYPTO._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1394) is too similar to ALTCRYPTO._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1477)
Variable ALTCRYPTO._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1423) is too similar to ALTCRYPTO._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1447)
Variable ALTCRYPTO._getRValues(uint256,uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1208-1212) is too similar to ALTCRYPTO._getTValues(uint256).tTransferAmount (contracts/Token.sol#1188)
Variable ALTCRYPTO._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1453) is too similar to ALTCRYPTO._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1447)
Variable ALTCRYPTO._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1483) is too similar to ALTCRYPTO._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1447)
Variable ALTCRYPTO._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1394) is too similar to ALTCRYPTO._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1447)
Variable ALTCRYPTO._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1423) is too similar to ALTCRYPTO._getTValues(uint256).tTransferAmount (contracts/Token.sol#1188)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
Loop condition `i < _excluded.length` (contracts/Token.sol#1224) should use cached array length instead of referencing `length` member of the storage array.
 Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#cache-array-length
INFO:Detectors:
ALTCRYPTO._decimals (contracts/Token.sol#884) should be constant
ALTCRYPTO._name (contracts/Token.sol#882) should be constant
ALTCRYPTO._symbol (contracts/Token.sol#883) should be constant
ALTCRYPTO._tTotal (contracts/Token.sol#871) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Slither:../contracts/Token.sol analyzed (10 contracts with 88 detectors), 73 result(s) found
```

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

CONTRACT ASSESMENT

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
└	totalSupply	External ❗		NO ❗
└	balanceOf	External ❗		NO ❗
└	transfer	External ❗	🔴	NO ❗
└	allowance	External ❗		NO ❗
└	approve	External ❗	🔴	NO ❗
└	transferFrom	External ❗	🔴	NO ❗
SafeMath	Library			
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	mod	Internal 🔒		
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Address	Library			
└	isContract	Internal 🔒		
└	sendValue	Internal 🔒	🔴	
└	functionCall	Internal 🔒	🔴	
└	functionCall	Internal 🔒	🔴	
└	functionCallWithValue	Internal 🔒	🔴	

CONTRACT ASSESMENT

└	functionCallWithValue	Internal 🔒	🔴		
└	_functionCallWithValue	Private 🔑	🔴		
Ownable	Implementation	Context			
└	<Constructor>	Public ❗	🔴	NO❗
└	owner	Public ❗		NO❗
└	renounceOwnership	Public ❗	🔴	onlyOwner
└	transferOwnership	Public ❗	🔴	onlyOwner
IUniswapV2Factory	Interface			
└	feeTo	External ❗		NO❗
└	feeToSetter	External ❗		NO❗
└	getPair	External ❗		NO❗
└	allPairs	External ❗		NO❗
└	allPairsLength	External ❗		NO❗
└	createPair	External ❗	🔴	NO❗
└	setFeeTo	External ❗	🔴	NO❗
└	setFeeToSetter	External ❗	🔴	NO❗
IUniswapV2Pair	Interface			
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🔴	NO❗
└	transfer	External ❗	🔴	NO❗
└	transferFrom	External ❗	🔴	NO❗
└	DOMAIN_SEPARATOR	External ❗		NO❗
└	PERMIT_TYPEHASH	External ❗		NO❗
└	nonces	External ❗		NO❗
└	permit	External ❗	🔴	NO❗
└	MINIMUM_LIQUIDITY	External ❗		NO❗

CONTRACT ASSESMENT

└	factory	External ❗			NO❗
└	token0	External ❗			NO❗
└	token1	External ❗			NO❗
└	getReserves	External ❗			NO❗
└	price0CumulativeLast	External ❗			NO❗
└	price1CumulativeLast	External ❗			NO❗
└	kLast	External ❗			NO❗
└	burn	External ❗	🔴	NO❗
└	swap	External ❗	🔴	NO❗
└	skim	External ❗	🔴	NO❗
└	sync	External ❗	🔴	NO❗
└	initialize	External ❗	🔴	NO❗
IUniswapV2Router01	Interface			
└	factory	External ❗			NO❗
└	WETH	External ❗			NO❗
└	addLiquidity	External ❗	🔴	NO❗
└	addLiquidityETH	External ❗	💵	NO❗
└	removeLiquidity	External ❗	🔴	NO❗
└	removeLiquidityETH	External ❗	🔴	NO❗
└	removeLiquidityWithPermit	External ❗	🔴	NO❗
└	removeLiquidityETHWithPermit	External ❗	🔴	NO❗
└	swapExactTokensForTokens	External ❗	🔴	NO❗
└	swapTokensForExactTokens	External ❗	🔴	NO❗
└	swapExactETHForTokens	External ❗	💵	NO❗
└	swapTokensForExactETH	External ❗	🔴	NO❗
└	swapExactTokensForETH	External ❗	🔴	NO❗
└	swapETHForExactTokens	External ❗	💵	NO❗
└	quote	External ❗			NO❗
└	getAmountOut	External ❗			NO❗
└	getAmountIn	External ❗			NO❗
└	getAmountsOut	External ❗			NO❗
└	getAmountsIn	External ❗			NO❗

CONTRACT ASSESMENT

IUniswapV2Router02	Interface	IUniswapV2Router01		
└	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🔴	NO❗
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🔴	NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🔴	NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🔴	NO❗
ALTCRYPTO	Implementation	Context, IERC20, Ownable		
└	<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❗
└	isExcludedFromReward	Public ❗		NO❗
└	totalFees	Public ❗		NO❗
└	tokenFromReflection	Public ❗		NO❗
└	updateMarketingWallet	External ❗	🔴	onlyOwner
└	updateburnAddress	External ❗	🔴	onlyOwner
└	updateRnDAddress	External ❗	🔴	onlyOwner
└	excludeFromReward	Public ❗	🔴	onlyOwner
└	includeInReward	External ❗	🔴	onlyOwner
└	excludeFromFee	Public ❗	🔴	onlyOwner
└	includeInFee	Public ❗	🔴	onlyOwner
└	setSellFee	External ❗	🔴	onlyOwner
└	setBuyFee	External ❗	🔴	onlyOwner
└	<Receive Ether>	External ❗	💵	NO❗

CONTRACT ASSESMENT

└	_reflectFee	Private 🔐	🔴	
└	_getTValues	Private 🔐		
└	_getRValues	Private 🔐		
└	_getRate	Private 🔐		
└	_getCurrentSupply	Private 🔐		
└	_takeMarketing	Private 🔐	🔴	
└	_takeBurnFee	Private 🔐	🔴	
└	_takeRnDFee	Private 🔐	🔴	
└	calculatetaxReflectionFee	Private 🔐		
└	calculateMarketingFee	Private 🔐		
└	calculateRnDFee	Private 🔐		
└	calculateBurnFee	Private 🔐		
└	removeAllFee	Private 🔐	🔴	
└	setBuy	Private 🔐	🔴	
└	setSell	Private 🔐	🔴	
└	isExcludedFromFee	Public ❗		|NO❗
└	_approve	Private 🔐	🔴	
└	_transfer	Private 🔐	🔴	
└	swapTokensForEth	Private 🔐	🔴	
└	_tokenTransfer	Private 🔐	🔴	
└	_transferStandard	Private 🔐	🔴	
└	_transferToExcluded	Private 🔐	🔴	
└	_transferFromExcluded	Private 🔐	🔴	
└	_transferBothExcluded	Private 🔐	🔴	
└	withdrawETH	Public ❗	🔴	onlyOwner
└	withdrawToken	Public ❗	🔴	onlyOwner

Legend

Symbol	Meaning
🔴	Function can modify state
💵	Function is payable

FUNCTIONAL TESTING

1- Adding liquidity (passed):

https://testnet.bscscan.com/tx/0xd94a8ddb596b8046ec0f1b87e0e4c1c35 a3e744bb75979244ed84df70ba6eb72

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

https://testnet.bscscan.com/tx/0xdf05bb62adfdc89defd4f1745af83e52c5 9ee28cffa3a5e8fdc8b739f3fdc061

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

https://testnet.bscscan.com/tx/0xf0468501fdb9d0b7349a7016e6ec7ad22 acb3e95fa0d35b0b093fbe028bed810

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

https://testnet.bscscan.com/tx/0xf636cf59f4dc1fc11fee0813983398a3db 60d878baa7861a28aa6bc95742b14e

5- Buying from a regular wallet (0-100% tax) (passed):

https://testnet.bscscan.com/tx/0xaa5ca72580c8ef03ef501528bbf9bdb8e 1869b8e95ba0384c929ae45aaf2af5a

6- Selling from a regular wallet (0-100% tax) (passed):

https://testnet.bscscan.com/tx/0xb1f189b66cbbbbdf9e61bf497c83566fed cdef224c6ad737b1125b4d349f48f8

7- Transferring from a regular wallet (0-100% tax) (passed):

https://testnet.bscscan.com/tx/0x16594a350bee67b71a595560ab8fcb60c ea3897385fa05cb98e7b21f8ae87148

MANUAL TESTING

Missing logic – **Lack of event emission**

Severity: Informational

function: _takeMarketing - _takeBurnFee - _takeRnDFee

Status: Open

Overview:
Blockchain explorers may not show holders correctly because contract is not emitting "Transfer" events when taking fee (marketing, burn, RnD).

Suggestion
Emit events from this function after taking fees:
Sample code:
```
function _takeRnDFee(address from, uint256 tRnD) private {
uint256 currentRate = _getRate();
uint256 rRnD = tRnD.mul(currentRate);
_rOwned[_RnDTax] = _rOwned[_RnDTax].add(rRnD);
if (_isExcluded[_RnDTax]) _tOwned[_RnDTax] = _tOwned[_RnDTax].add(tRnD);
    emit Transfer(from, _RnDTax, tRnD);
  }
```

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