Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

TitsV2

Deployer address

0xb5aCc0EC58BF6B7054811981eB064C5f45BAfaA7

Client contacts:

TitsV2 Team

Blockchain

Binance Smart Chain

Project website:

https://titscoin.io/

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by TitsV2 to perform an audit of smart contracts:

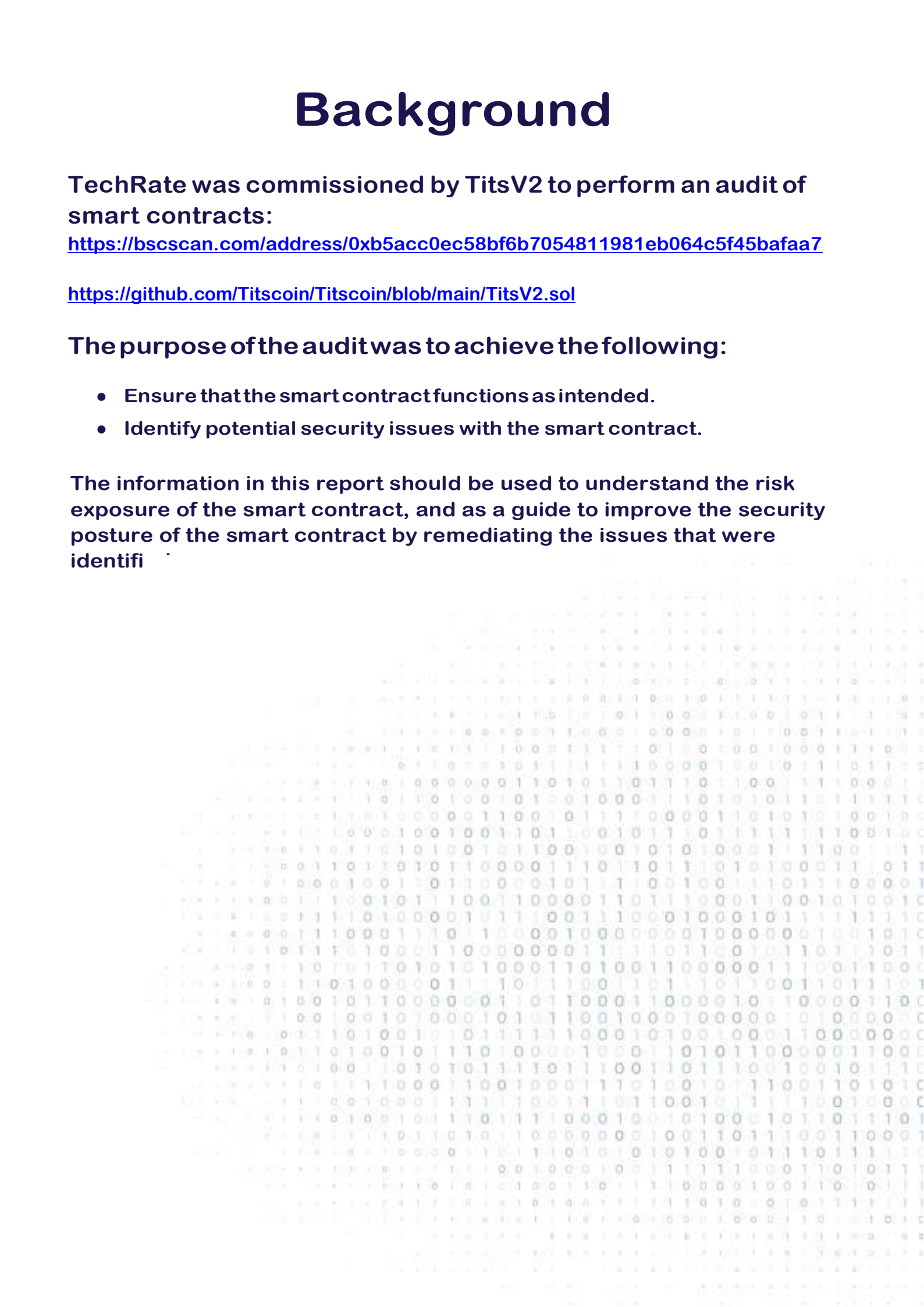
https://bscscan.com/address/0xb5acc0ec58bf6b7054811981eb064c5f45bafaa7

https://github.com/Titscoin/Titscoin/blob/main/TitsV2.sol

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identifi

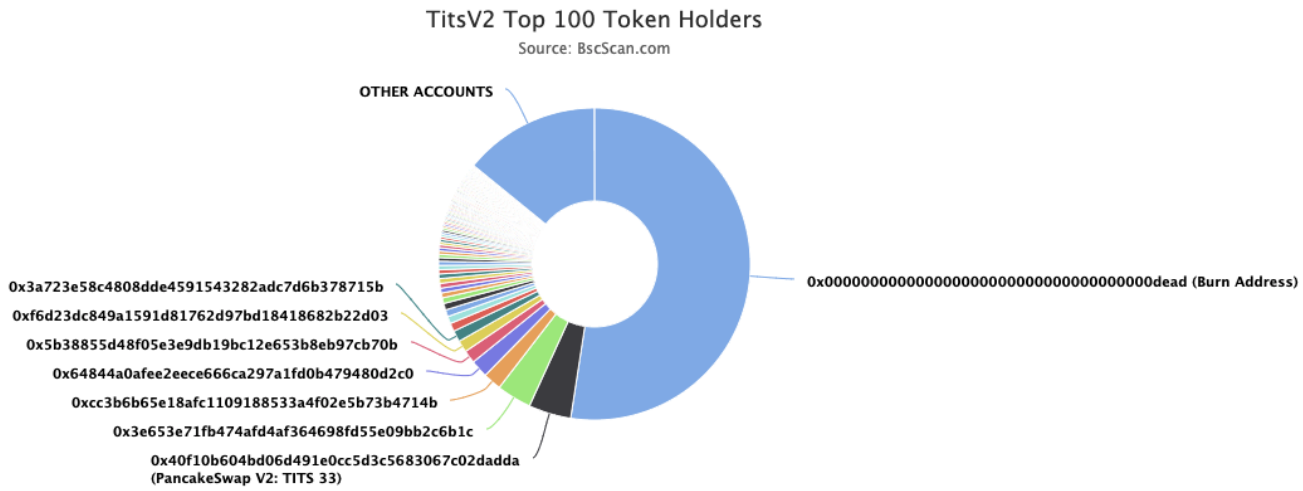


Contracts Details

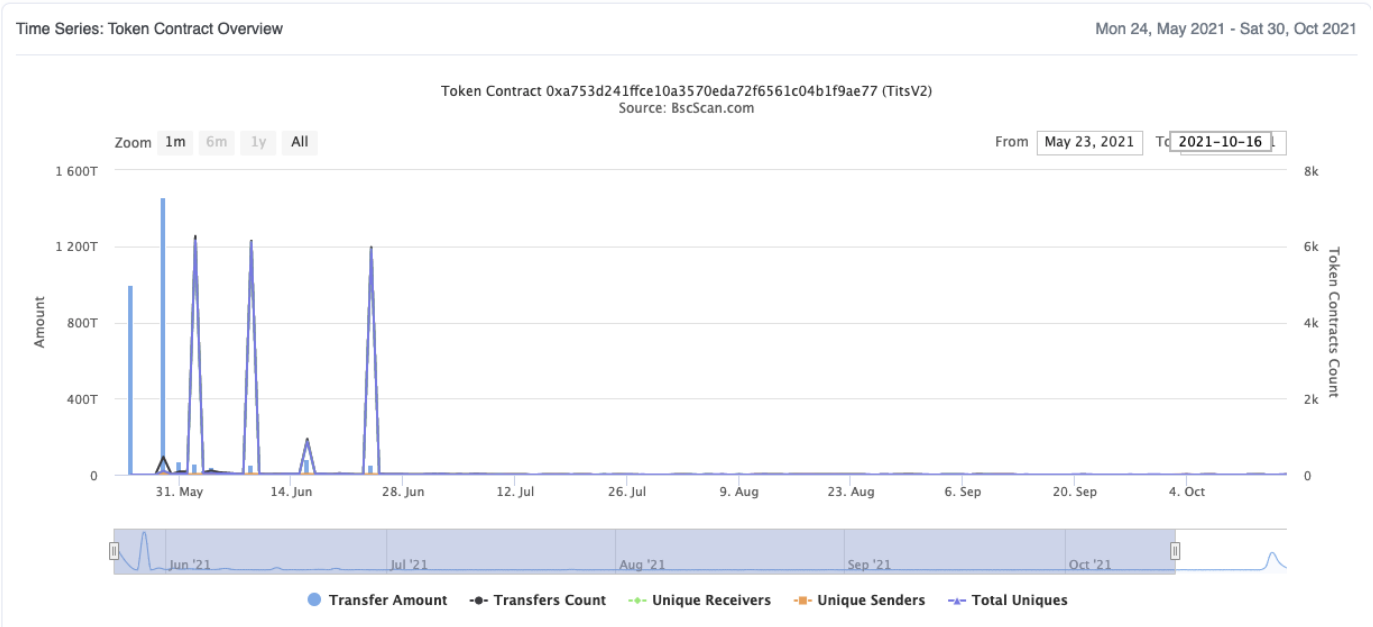
Token contract details for 10.15.2021

Contract name	TitsV2
Contract address	0xA753D241fFcE10A3570eDa72f6561C04b1f9Ae77
Total supply	1,000,000,000,000,000
Token ticker	TITS
Decimals	9
Token holders	12783
Transactions count	33719
Top 100 holders dominance	86.73 %
Total Fees	10

TitsV2 Token Distribution



TitsV2 Contract Interaction Details



TitsV2 Top 20 Token Holders

Rank	Address	Quantity	Percentage	Analytics
1	Burn Address	524,580,479,325,396.854963237	52.4580%	
2	PancakeSwap V2: TITS 33	44,064,770,427,719.190454477	4.4065%	
3	0x3e653e71fb474afd4af364698fd55e09bb2c6b1c	36,040,157,143,015.924504151	3.6040%	
4	0xcc3b6b65e18afc1109188533a4f02e5b73b4714b	18,994,253,939,155.303934363	1.8994%	
5	0x64844a0afee2eece666ca297a1fd0b479480d2c0	18,319,035,719,470.910433462	1.8319%	
6	0x5b38855d48f05e3e9db19bc12e653b8eb97cb70b	13,234,739,193,162.429154172	1.3235%	
7	0xf6d23dc849a1591d81762d97bd18418682b22d03	12,367,503,396,995.483299334	1.2368%	
8	0x3a723e58c4808dde4591543282adc7d6b378715b	11,627,919,141,999.864063994	1.1628%	
9	0x3e03d65c43b3cfaadb72b1d920ad4bc3cd6cd9db	8,483,893,713,448.399804522	0.8484%	
10	0x9784a1be8b21146a0cc65aa18a4914b33b0c9bcb	7,576,703,309,847.478703513	0.7577%	
11	0x8ff07866ae44dd66d8e91f8aeae159aa2ecb1c84	7,121,934,314,906.372965464	0.7122%	
12	0xf14f0836f7d6ef65799d325cc787646f8ad2fa0d	6,866,447,963,371.111706464	0.6866%	
13	0xec9d7e6935cdf1079cd1349155283437841422e7	5,808,500,888,357.190870979	0.5809%	
14	0x0270faa74e3bfedb426e3d145ae4a3a12b61ce5e	5,141,440,097,639.624648053	0.5141%	
15	0x309d3522f7c3a4fe6ac6bb8a2f3916d24c643df7	5,000,000,000,000	0.5000%	
16	0xdcae0a93a8d74e418dbb69c21ecb9fcc886445ac	4,898,424,910,640.459220027	0.4898%	
17	0x08987ed55413fa2fa3c2a413edf0f0be1fe23643	4,891,799,764,822.211032921	0.4892%	
18	0xd53740126ab55eaac65e4cd4f3e020bc09610ee3	4,791,850,016,279.316266146	0.4792%	
19	0xd6ea41017241c326feb660aa7e93e85915429d75	4,373,174,316,988.162730132	0.4373%	
20	0x3fa5edaeb55d8ec7406c32283f49553383d41d27	4,372,119,816,541.643756116	0.4372%	

TitsV2 Top LP Holders

Rank	Address	Quantity	Percentage	Analytics
1	0xeb3a9c56d963b971d320f889be2fb8b59853e449	2,833.7062085449577	64.3949%	
2	Titscoin: Deployer	1,558.547965120841880767	35.4174%	
3	0xb1b9b4bbe8a92d535f5df2368e7fd2ecfb3a1950	5.723583686882962654	0.1301%	
4	0xabb45207b198e77db74cfbc55976893d84dc3ca3	1.259367013530513354	0.0286%	
5	0xda5d539df52f2b13c69920a21d2fea6e008a4c50	1.185166128117605398	0.0269%	
6	0x1da910ea9cb3f6315124b5bc16b373f4f3706a49	0.054942545980093824	0.0012%	
7	0xef14eb068d1ed8e8d44b7af13ca9eb5a1252a281	0.027056863334611088	0.0006%	
8	0xee0b3e616f1ecd38d97447e40c7caf96c3390528	0.009488575137740473	0.0002%	
9	0xc137b46019317dfc4afa95218d6acf02da000431	0.002111903259388474	0.0000%	
10	0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%	

Contract functions details

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ [Lib] IterableMapping
  - [Pub] get
  - [Pub] getIndexOfKey
  - [Pub] getKeyAtIndex
  - [Pub] size
  - [Pub] set #
  - [Pub] remove #

+ [Lib] SafeMathUint
- [Int] toInt256Safe

+ [Lib] SafeMathInt
  - [Int] mul

- [Int] div
- [Int] sub
- [Int] add
- [Int] abs
- [Int] toUint256Safe

+ [Int] DividendPayingTokenInterface
- [Ext] dividendOf
- [Ext] distributeDividends ($)
- [Ext] withdrawDividend #

+ [Int] DividendPayingTokenOptionalInterface
- [Ext] withdrawableDividendOf
- [Ext] withdrawnDividendOf
- [Ext] accumulativeDividendOf

+ [Int] IUniswapV2Pair
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] allowance
- [Ext] approve #
- [Ext] transfer #
- [Ext] transferFrom #
- [Ext] DOMAIN_SEPARATOR
- [Ext] PERMIT_TYPEHASH
- [Ext] nonces
- [Ext] permit #
- [Ext] MINIMUM_LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] mint #
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+ [Int] IUniswapV2Factory
- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #

- [Ext] setFeeToSetter #

+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ ERC20 (Context, IERC20, IERC20Metadata)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _beforeTokenTransfer #

+ TitsV2 (ERC20, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20

- [Ext] <Fallback> ($)
- [Pub] updateDividendTracker #
  - modifiers: onlyOwner
- [Pub] updateUniswapV2Router #
  - modifiers: onlyOwner
- [Pub] transfer #
- [Pub] blacklistAddress #
  - modifiers: onlyOwner
- [Pub] removeBlacklist #
  - modifiers: onlyOwner
- [Pub] excludeFromFees #
- modifiers: onlyOwner
- [Pub] excludeMultipleAccountsFromFees #
- modifiers: onlyOwner
- [Ext] setSwapTokensAtAmount #
- modifiers: onlyOwner
- [Pub] updateOSMWallet #
- modifiers: onlyOwner
- [Pub] updateMarketingWallet #
- modifiers: onlyOwner
- [Pub] updateLiquiWallet #
- modifiers: onlyOwner
- [Pub] updateNFTWallet #
- modifiers: onlyOwner
- [Pub] updateGasForProcessing #
- modifiers: onlyOwner
- [Ext] updateClaimWait #
- modifiers: onlyOwner
- [Ext] getClaimWait
- [Ext] getTotalDividendsDistributed
- [Pub] isExcludedFromFees
- [Pub] withdrawableDividendOf
- [Pub] dividendTokenBalanceOf
- [Ext] getAccountDividendsInfo
- [Ext] getAccountDividendsInfoAtIndex
- [Ext] processDividendTracker #
- [Ext] claim #
- [Ext] getLastProcessedIndex
- [Ext] getNumberOfDividendTokenHolders
- [Int] _transfer #
- [Prv] _getFeeAmount
- [Prv] _accountAllFee #
- [Prv] _distributeBNBBalance #
- [Prv] sendToWallet #
- [Prv] buybackOSM #
- [Ext] getBalance

- [Prv] swapTokensForBNB #
- [Prv] sendDividends #
- [Ext] withdrawTokens #
  - modifiers: onlyOwner
- [Ext] launchNow #
  - modifiers: onlyOwner
- [Ext] bulksendToken #
- [Ext] enableBurnFeeMode #
  - modifiers: onlyOwner
- [Ext] disableBurnFeeMode #
  - modifiers: onlyOwner
- [Ext] reduceSellFee #
  - modifiers: onlyOwner
- [Ext] increaseSellFee #
  - modifiers: onlyOwner

($) = payable function
= non-constant function

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Low issues
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issues found.

Notes:

- Fees can be changed by owner. Ensure that deployer address is held by a non-centralized source
- Token contract is similar to other deflationary tokens with taxing structure

Conclusion

Smart contracts contain no severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details NOT provided by the team.

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner