**ARBITECH**

**SOLUTIONS**

KNIGHTDOGE

BEP

TOKEN

20

SMART

CONTRACT

CODE REVIEW

AND

SECURITY

ANALYSIS

REPORT

Arbitech

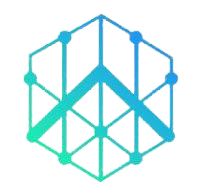
Solutions

1

3

September,

2021



Contents

Commission ................................................................................................................................................ 3

Disclaimer ................................................................................................................................................... 4

KNIGHTDOGE Properties ......................................................................................................................... 5

Token Analytics .......................................................................................................................................... 6

Contract Functions ....................................................................................................................................... 7

Public ........................................................................................................................................................... 7

View ........................................................................................................................................................... 7

Virtual ........................................................................................................................................................ 7

Executables ................................................................................................................................................. 7

Owner Executables ..................................................................................................................................... 7

Checklist ................................................................................................................................................... 9

Owner privileges ....................................................................................................................................... 10

KNIGHTDOGE Contract ........................................................................................................................ 10

DogeDividendTracker Contract ............................................................................................................... 15

Potential Issues ......................................................................................................................................... 17

[Low] Smart Contract presented before DxSale .................................................................................. 17

[Low] Dividend’s logic can change at any time ............................................................................... 18

[Low] Dividends can be disabled at any time .................................................................................. 18

[Mid] Dividends Contract can set the Balance ................................................................................. 19

Conclusions ............................................................................................................................................ 20

# Commission

|  |  |
| --- | --- |
| **Audited Project** | **KNIGHTDOGE Token** |
| **Contract Owner** | **0x59A092d876A2FF4A049eA4cB8aA69A95cA107A3c** |
| **Smart Contract** | **0xb9d55cbc1e10a72f1b4d236c7576c0672b7770bc** |
| **Blockchain** | **Binance Main Smart Chain** |

Arbitech Solutions was commissioned by KNIGHTDOGE Token owners to perform an audit of their main smart contract. 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 identified.

# 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 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 Arbitech Solution and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Arbitech Solution) owe no duty of care towards you or any other person, nor does Arbitech Solution 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 Arbitech Solution 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, Arbitech Solution hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Arbitech Solution, 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.

# KNIGHTDOGE Properties

|  |  |
| --- | --- |
| Contract name | KNIGHTDOGE Token |
| Contract address | 0xb9d55cbc1e10a72f1b4d236c7576c0672b7770bc |
| Total supply | 5 Lac |
| Token ticker | KNIGHTDOGE |
| Decimals | 18 |
| Token holders | 1 |
| Transaction’s count | 1 |
| Top 100 holder’s dominance | 100% |
| Liquidity fee | 2 |
| Tax fee | 0 |
| Total fees | 10 |
| Mintable | Yes |
| Burnable | Yes |
| Uniswap V2 pair | 0x6cc0590457a4dba3f689d6e58d14c2bc9a1f6b57 |
| Contract deployer address | 0x59A092d876A2FF4A049eA4cB8aA69A95cA107A3c |
| Contract’s current owner address | 0x59A092d876A2FF4A049eA4cB8aA69A95cA107A3c |
| Marketing Address | 0xeC70292cf5c5D46DBB37Bc72319de3BCd05394e3 |

# Contract Functions

### View

1. function WbnbDividendTokenBalanceOf(address account)
2. function allowance(address owner, address spender)
3. function balanceOf(address account)
4. function decimals()
5. function getAccountDogeDividendsInfo(address account)
6. function getAccountDogeDividendsInfoAtIndex(uint256 index)
7. function getDogeClaimWait()
8. function getIsExcludedFromFees(address account)
9. function getLastDogeDividendProcessedIndex()
10. function getNumberOfWbnbDividendTokenHolders()
11. function getTotalDogeDividendsDistributed()
12. function name()
13. function owner()
14. function symbol()
15. function totalSupply()
16. function withdrawableDogeDividendOf(address account)

### Virtual

1. increaseAllowance()
2. decreaseAllowance()
3. function renounceOwnership()

### Executables

1. function approve(address spender, uint256 amount)
2. function claim()
3. function decreaseAllowance(address spender, uint256 subtractedValue)
4. function excludeFromDividend(address account)
5. function increaseAllowance(address spender, uint256 addedValue)
6. function transfer(address recipient, uint256 amount)
7. function transferFrom(address sender, address recipient, uint256 amount)

### Owner Executables

1. function afterPreSale()
2. function excludeFromFees(address account, bool excluded)
3. function excludeMultipleAccountsFromFees(address[] calldata accounts, bool excluded)
4. function lock(uint256 time)
5. function prepareForPartherOrExchangeListing(address \_partnerOrExchangeAddress)
6. function processDividendTracker(uint256 gas)
7. unction renounceOwnership()
8. function setAutomatedMarketMakerPair(address pair, bool value)
9. function setBuyBackAndLiquifyEnabled(bool \_enabled)
10. function setDogeDividendEnabled(bool \_enabled)
11. function setMarketingEnabled(bool \_enabled)
12. function setMaxBuyTransaction(uint256 \_maxTxn)
13. function setMaxSellTransaction(uint256 \_maxTxn)
14. function setMaxWalletTokend(uint256 \_maxToken)
15. function setSellTransactionMultiplier(uint256 \_multiplier)
16. function setSwapTokensAtAmount(uint256 \_swapAmount)
17. function setTradingIsEnabled(bool \_enabled)
18. function transferOwnership(address newOwner) xix. function updateBuyBackAndLiquidityFee(uint8 newFee) xx. function updateClaimWait(uint256 claimWait)
19. function updateDogeDividendRewardFee(uint8 newFee
20. function updateDogeDividendTracker(address newAddress)
21. function updateGasForProcessing(uint256 newValue) xxiv. function updateMarketingFee(uint8 newFee)
22. function updateMarketingWallet(address \_newWallet)
23. function updateMinimumBalanceForDividends(uint256 newMinimumBalance
24. function updateUniswapV2Router(address newAddress)
25. function whitelistDxSale(address \_presaleAddress, address \_routerAddres)

# Checklist

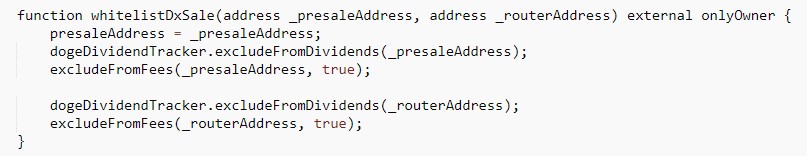
|  |  |  |
| --- | --- | --- |
| Compiler errors. |  | Passed |
| Possible delays in data delivery. |  | Passed |
| Timestamp dependence. |  | Low Severity |
| Integer Overflow and Underflow. |  | Passed |
| DoS with Revert. |  | Passed |
| DoS with block gas limit. |  | Passed |
| Methods execution permissions. |  | Mid Severity |
| Economy model of the contract. |  | Passed |
| Private user data leaks. |  | Passed |
| Malicious Events Log. |  | Passed |
| Scoping and Declarations. |  | Passed |
| Uninitialized storage pointers. |  | Passed |
| Arithmetic accuracy. |  | Passed |
| Design Logic. |  | Passed |
| Cross-function race conditions. |  | Passed |
| Fallback function security. |  | Passed |
| Safe Open Zeppelin contracts and usage. | implementation | Passed |
| Whitepaper-Website-Contract correlation. | | Low Severity |

# Owner privileges

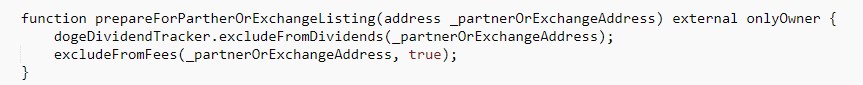
### KNIGHTDOGE Contract

The owner can set when the presale ends by excluding the

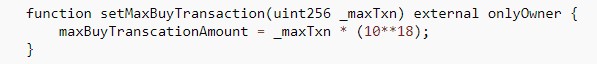
Dividend contract and presale address



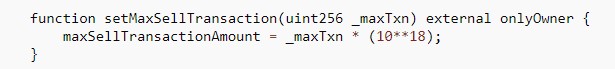
The owner can exclude from fees the Dividend contract and the partnering address.



The Owner can limit the Max Buy amount.



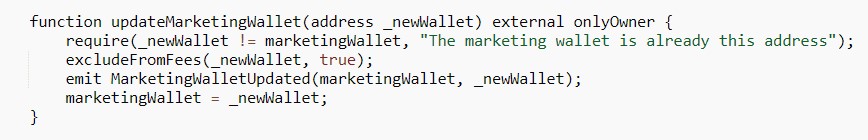
The owner can limit the Max Sell amount



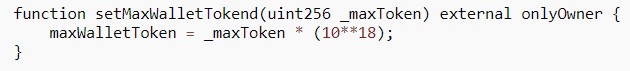
The owner can change the Dividend contract address at anytime



The owner can update the Marketing Wallet at anytime.



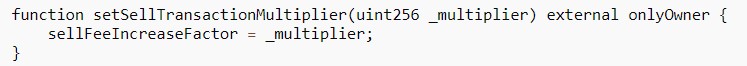
The owner can set the Max amount of tokens per wallet at anytime.



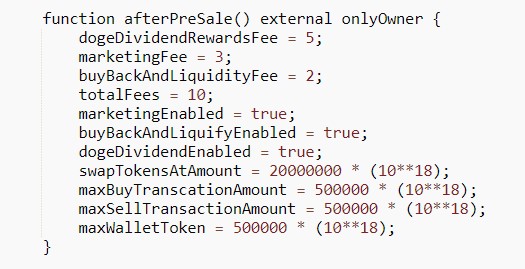
The owner can set the max swap amount at anytime.



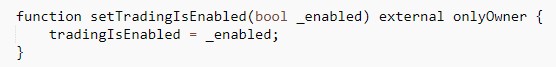
The owner can set the transaction multiplier at anytime



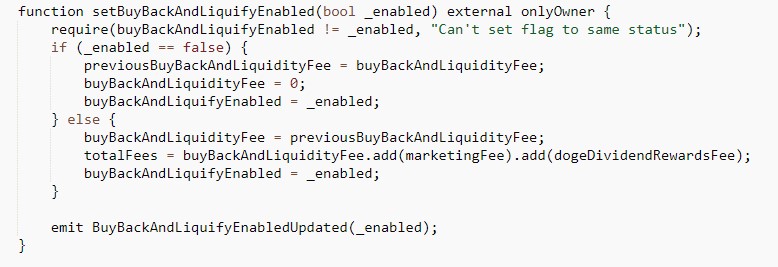
The owner can set the token properties to the following amount at anytime



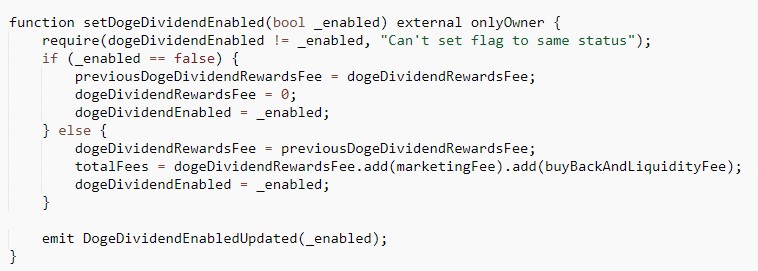
The owner can stop the trading at anytime



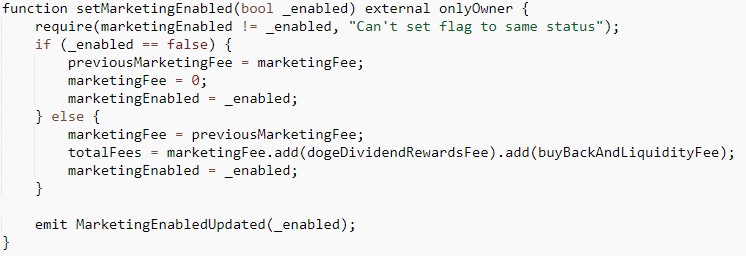
The owner can disable or enable Buy Back for Liquidity at anytime



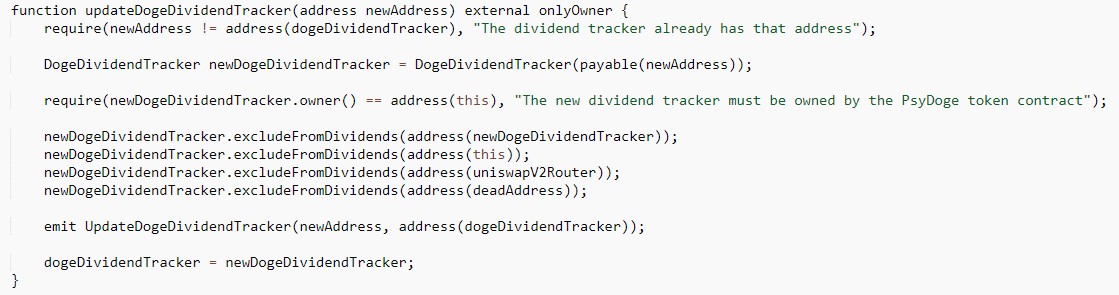
The owner can disable the Dividends at anytime



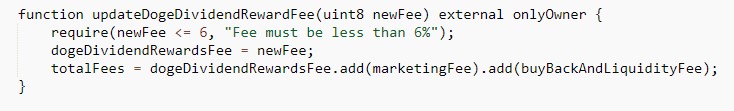
The owner can enable or disable the marketing fees at anytime



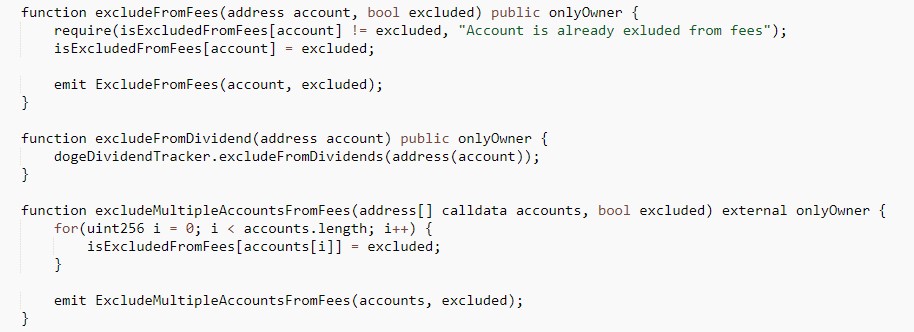
The owner can update the dividend tracker contract at anytime.



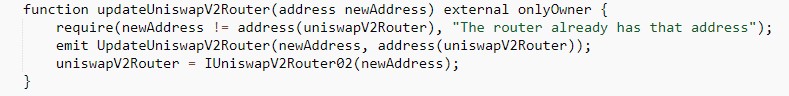
The owner can change fees at anytime.



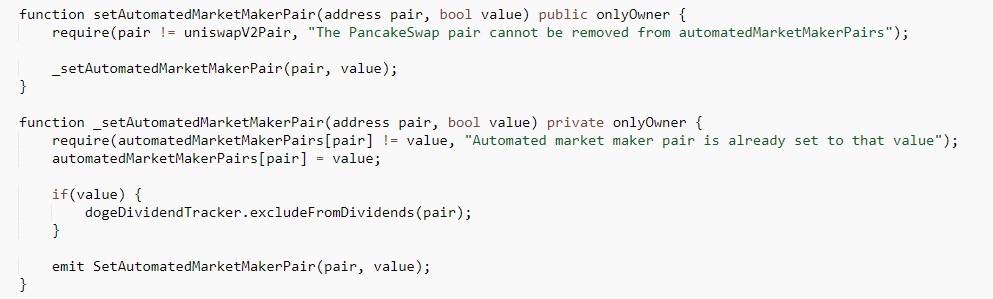
The owner can exclude accounts from fees at anytime



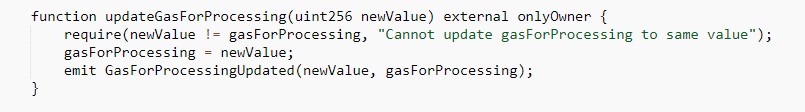
The owner can update the UniSwap Router at anytime.



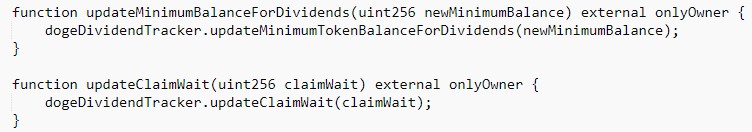
The owner can prepare the token for new AMM pair.



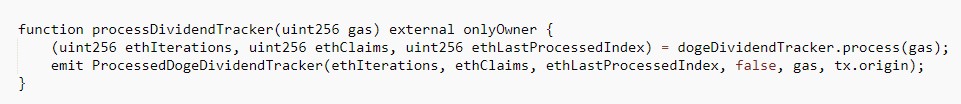
The owner can set gas for processing at anytime.



The owner can update the minimum balance to be allowed to claim dividends as well as the time to wait between claims.



The owner can process the dividends at anytime.

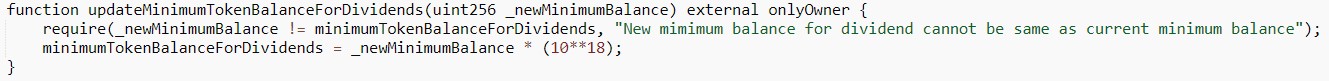


### DogeDividendTracker Contract

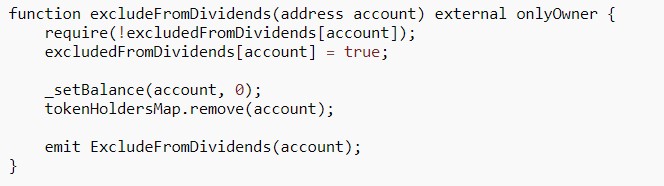
The owner can update the Dividend Tracker contract at anytime



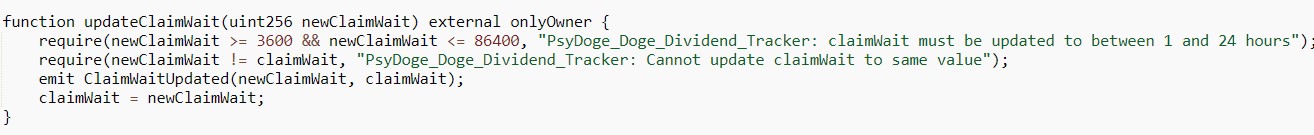
The owner can update the minimum balance needed to claim balance at anytime.



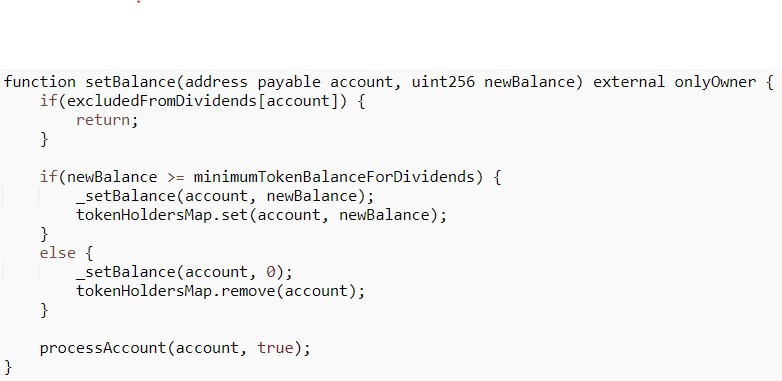
The owner can exclude addresses for Dividends at anytime.



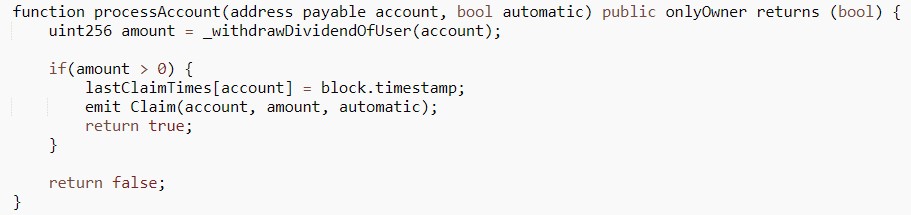
The owner can update the claim time at anytime.



The owner can set the dividend balance of an address at anytime.



The owner can process any address at anytime.



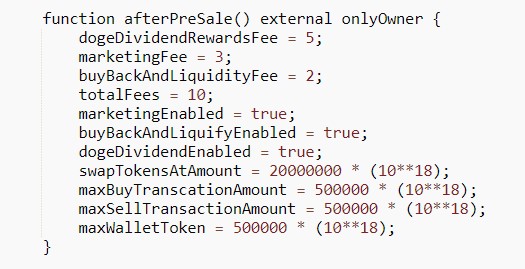
# Potential Issues

## [Low] Smart Contract presented before DxSale

As of 13/09/2021 when the Audit took place the contract has all fees set at 0% as well as the allowed amounts are still set to zero.

The reason behind this is that the DxSale hasn’t go live yet and during the presales the fees have to be set at 0%.

After that the owner will be able to run the afterPresaSale() function in order to set them to the following amounts. Note that this function can be ran at any time rendering this a way to make the contract return to the initial values.

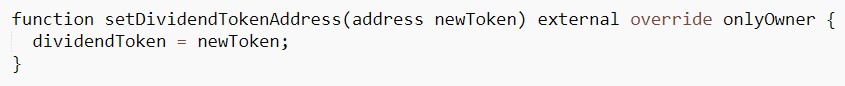
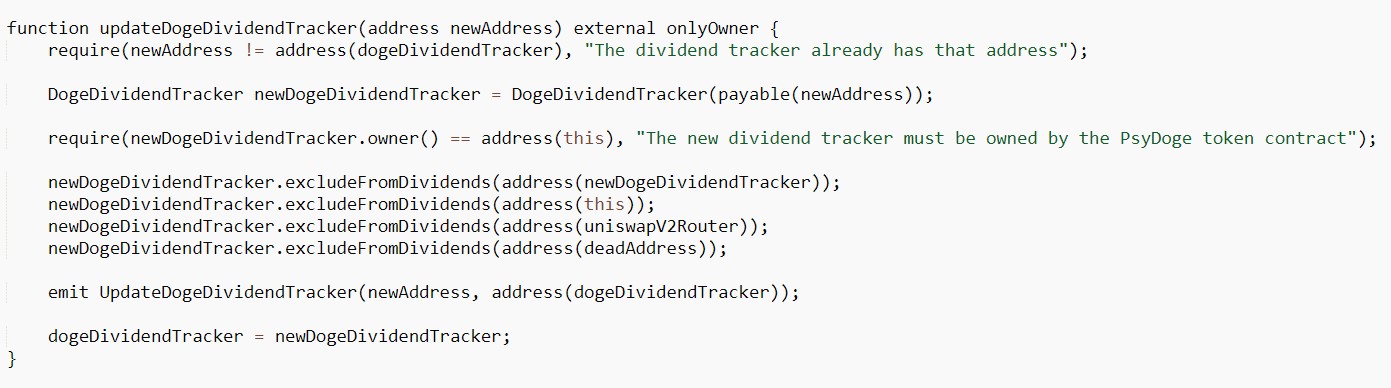


## [Low] Dividend’s logic can change at any time

Even though at this time the Dividends contract is written in the same file as the Token contract giving a clear visibility of the Dividend’s logic, this can change at any time.

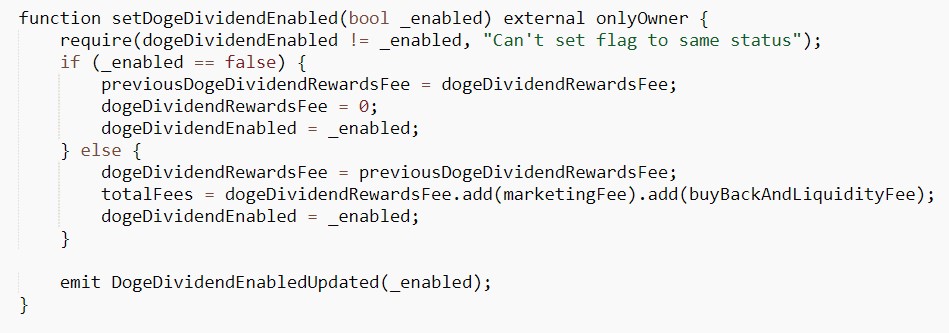
By updating the Dividends tracker address the logic inside the current address would be rendered useless.

This wouldn’t present much of an issue as the new address will be public under the owner’s address but it must be taken into consideration to prevent future issues.



## [Low] Dividends can be disabled at any time

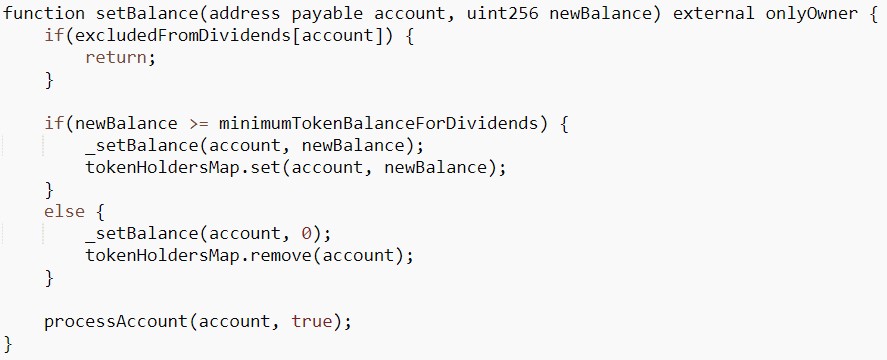
It must be noted that Dividends can be disabled at any time rendering a big part of the Tokenomics/Properties of the Token useless.



## [Mid] Dividends Contract can set the Balance

Inside the DogeDividendTracker contract, the owner, is able to set the balance of any account to over the minimum value in order to take part of the dividends.

This can pose an issue as the token is not mintable but the dividends can effectively be set by hand. While this is only set to external, this cannot be called from the BSCScan site but it could be interacted with from other sources.



# Conclusions

The Smart Contract code passed the audit successfully on the Binance Mainnet with some considerations to take.There were three low severity warnings raised meaning that they should be taken into consideration but if the confidence in the owner is good, they can be dismissed.

* Smart contract current Fees and amount states (pre DxSale), will change after the presale. This is not part of the audit.
* Dividends Tracker logic can change at any time by pointing to another contract.
* Dividends can be disabled at any time with no time limit.

One mid severity warning was raised:

* There’s a function inside the DogeDividendTracker which could be interacted with to set the Dividends balance of an account to any value over the minimum limit.

* This can be fixed by setting the function to internal instead of external, meaning that it can be called only from inside the contract.

The last change is advisable in order to provide more security to new holders. Nonetheless this is not necessary if the holders and/or investors feel confident with the contract owners.