

# SKELETON ECOSYSTEM

SMART CONTRACT AUDIT



**Dogacoin**  
**DOGA**  
**BEP20**

0xCe6f3c09E602660EB8085273c37D9db11caFC



## Table of Contents

Table of Contents	1
Disclaimer	2
Overview	3
Creation/Audit Date	3
Verified Socials	3
Contract Functions Analysis	4
Contract Safety and Weakness	9
Detected Vulnerability Description	13
Contract Flow Graph	14
Contract Interaction Graph	15
Inheritance Graph	16
Contract Descriptions	17
Audit Scope	29

## Global Disclaimer

This document serves as a disclaimer for the crypto smart contract audit conducted by Skeleton Ecosystem. The purpose of the audit was to review the codebase of the smart contracts for potential vulnerabilities and issues. It is important to note the following:

**Limited Scope:** The audit is based on the code and information available up to the audit completion date. It does not cover external factors, system interactions, or changes made after the audit. The audit itself can not guarantee 100% safety and can not detect common scam methods like farming and developer sell-out.

**No Guarantee of Security:** While we have taken reasonable steps to identify vulnerabilities, it is impossible to guarantee the complete absence of security risks or issues. The audit report provides an assessment of the contract's security as of the audit date.

**Continued Development:** Smart contracts and blockchain technology are evolving fields. Updates, forks, or changes to the contract post-audit may introduce new risks that were not present during the audit.

**Third-party Code:** If the smart contract relies on third-party libraries or code, those components were not thoroughly audited unless explicitly stated. Security of these dependencies is the responsibility of their respective developers.

**Non-Exhaustive Testing:** The audit involved automated analysis, manual review, and testing under controlled conditions. It is possible that certain vulnerabilities or issues may not have been identified.

**Risk Evaluation:** The audit report includes a risk assessment for identified vulnerabilities. It is recommended that the development team carefully reviews and addresses these risks to mitigate potential exploits.

**Not Financial Advice:** This audit report is not intended as financial or investment advice. Decisions regarding the use, deployment, or investment in the smart contract should be made based on a comprehensive assessment of the associated risks.

By accessing and using this audit report, you acknowledge and agree to the limitations outlined above. Skeleton Ecosystem and its auditors shall not be held liable for any direct or indirect damages resulting from the use of the audit report or the smart contract itself.

Please consult with legal, technical, and financial professionals before making any decisions related to the smart contract.

## Overview

Contract Name	Dogacoin
Ticker/Symbol	DOGA
Blockchain	Binance Smart Chain BEP20
Contract Address	0xCe6f3c09E602660EB8085273c37D9db11caFCBeE
Creator Address	0x4c709170DeF702D0Ec4604bbba954e471327DAce
Current Owner Address	0x00
Contract Explorer	<a href="https://bscscan.com/token/0xCe6f3c09E602660EB8085273c37D9db11caFCBeE#code">https://bscscan.com/token/0xCe6f3c09E602660EB8085273c37D9db11caFCBeE#code</a>
Compiler Version	v0.8.19+commit.7dd6d404
License	None
Optimisation	Yes with 200 Runs
Total Supply	1,000,000 <b>DOGA</b>
Decimals	18



## Creation/Audit

Contract Deployed	16.03.2024
Audit Created	17.03.2024
Audit Update	V 1.0

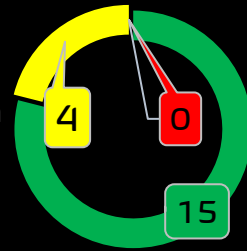
## Verified Socials








Website	<a href="https://dogaofficial.net">https://dogaofficial.net</a>
Telegram	<a href="https://t.me/doga_coin">https://t.me/doga_coin</a>
Twitter (X)	<a href="https://x.com/dogacoin_">https://x.com/dogacoin_</a>











## Contract Function Analysis

 Pass
  Attention Item
  Risky Item

■ Pass  
 ■ Attention  
 ■ Risk



Contract Verified		The contract source code is uploaded to blockchain explorer and is open source, so everybody can read it.
Contract Ownership		0x00 Sometimes referred to as the "zero address" or "dead address" and is not owned by anyone.
Buy Tax	5 %	Shows the taxes for purchase transactions. Above 10% may be considered a high tax rate. More than 50% tax rate means may not be tradable. Fee can be set!
Sell Tax	5 %	Shows the taxes for sell transactions. Above 10% may be considered a high tax rate. More than 50% tax rate means may not be tradable. Fee can be set!
Honeypot Analyse		Holder is able to buy and sell. If honeypot: The contract blocks sell transfer from holder wallet. Multiple events may cause honeypot. Trading disabled, extremely high tax
Liquidity Status		Liquidity status on 17.03.2024 Lp Lock 1: 67.98% Pinklock for 84 days. Lp Lock 2: 22.38% Pinklock for 84 days. Lp Burned: 8.95%
Trading Disable Functions		No Trading suspendable function found. If a suspendable code is included, the token maybe neither be bought or sold (honeypot risk). If contract is renounced this function can't be used
Set Fees function	 max 25%	Fee Setting function found. <b>Contract renounced, function can not be triggered by owner.</b> The contract owner may contain the authority to modify the transaction tax. If the transaction tax is increased to more than 49%, the tokens may not be able to be traded (honeypot risk).
Proxy Contract		Not a Proxy contract.
Mint Function		No Mint Function detected Mint function is transparent or non-existent. Hidden mint functions may increase the amount of tokens in circulation and effect the price of the token. Owner can mint new tokens and sell.

Balance Modifier Function		<p>No Balance Modifier function found.</p> <p>If there is a function for this, the contract owner can have the authority to modify the balance of tokens at other addresses. For example revoke the bought tokens from the holders wallet. Common form of scam: You buy the token, but it's disappearing from your wallet.</p>
Blacklist Function		<p>Blacklist Setting function found.</p> <p>Case: Set Wallets exclude from dividends. Not Blacklist from trading.</p>
Whitelist Function		<p>Whitelist Setting function found. <b>Contract renounced, function can not be triggered by owner.</b></p> <p>If there is a function for this Developer can set zero fee or no max wallet size for addresses (for example team wallets can trade without fee. Can cause farming)</p>
Hidden Owner Analysis		<p>No Hidden or multi owner with authorisation</p> <p>For contract with a hidden owner, developer can still manipulate the contract even if the ownership has been abandoned.</p>
Retrieve Ownership Function		<p>No Functions found which can retrieve ownership of the contract.</p> <p>If this function exists, it is possible for the project owner to regain ownership even after relinquishing it. Also known as fake renounce.</p>
Self Destruct Function		<p>No Self Destruct function found.</p> <p>If this function exists and is triggered, the contract will be destroyed, all functions will be unavailable, and all related assets will be erased.</p>
Specific Tax Changing Function		<p>No Specific Tax Changing Functions found.</p> <p>If it exists, the contract owner may set a very outrageous tax rate for assigned address to block it from trading. Can assign all wallets at once!</p>
Trading Cooldown Function		<p>No Trading Cooldown Function found. If there is a trading cooldown function, the user will not be able to sell the token within a certain time or block after buying. Like a temporary honeypot.</p>
Max Transaction and Holding Modify Function	 min 0.5%	<p>Max Transaction and Holding Modify function found. <b>Contract renounced, function can not be triggered by owner.</b></p> <p>If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot</p>
Transaction Limiting Function		<p>No Transaction Limiter Function Found.</p> <p>The number of overall token transactions may be limited (honeypot risk)</p>

## Details of Risk - Attention Items



### Removing Risk of contract function based on renounced ownership

#### Transaction Receipt Event Logs

307

Address

0xce6f3c09e602660eb8085273c37d9db11cafcbee

Name

OwnershipTransferred (index\_topic\_1 address previousOwner, index\_topic\_2 address newOwner) [View Source](#)

Topics

0

0x8be0079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0

1: previousOwner

Dec ▾

⇒ 0x4c709170DeF702D0Ec4604bbba954e471327DAce

2: newOwner

Dec ▾

⇒ 0x00

Data

0x

Following detected contract functions serve as informational purposes about the contract. The owner has no more authorisation to trigger the following functions.

## ⚠ Set Fee (25% Max)

Contract renounced, function can not be triggered by owner.

The contract owner may contain the authority to modify the transaction tax. If the transaction tax is increased to more than 49%, the tokens may not be able to be traded (honeypot risk).

```

216
    ftrace | funcSig
217     function liquidityFeesSetup(uint16 _buyFee!, uint16 _sellFee!, uint16 _transferFee!) public onlyOwner {
218         totalFees[0] = totalFees[0] - liquidityFees[0] + _buyFee!;
219         totalFees[1] = totalFees[1] - liquidityFees[1] + _sellFee!;
220         totalFees[2] = totalFees[2] - liquidityFees[2] + _transferFee!;
221         require(totalFees[0] <= 2500 && totalFees[1] <= 2500 && totalFees[2] <= 2500, "TaxesDefaultRouter: Cannot exceed max total fee of 25%");
222
223         liquidityFees = [_buyFee!, _sellFee!, _transferFee!];
224
  
```

```

261
    ftrace | funcSig
262     function rewardsFeesSetup(uint16 _buyFee!, uint16 _sellFee!, uint16 _transferFee!) public onlyOwner {
263         totalFees[0] = totalFees[0] - rewardsFees[0] + _buyFee!;
264         totalFees[1] = totalFees[1] - rewardsFees[1] + _sellFee!;
265         totalFees[2] = totalFees[2] - rewardsFees[2] + _transferFee!;
266         require(totalFees[0] <= 2500 && totalFees[1] <= 2500 && totalFees[2] <= 2500, "TaxesDefaultRouter: Cannot exceed max total fee of 25%");
267
268         rewardsFees = [_buyFee!, _sellFee!, _transferFee!];
269
  
```

## ⚠ Whitelist ( Set exclud wallets )

Contract renounced, function can not be triggered by owner.

If there is a function for this Developer can set zero fee or no max wallet size for addresses (for example team wallets can trade without fee. Can cause farming)

```

284
    ftrace | funcSig
285     function excludeFromFees(address account!, bool isExcluded!) public onlyOwner {
286         isExcludedFromFees[account!] = isExcluded!;
287
288         emit ExcludeFromFees(account!, isExcluded!);
289     }
290
  
```

```

404
    ftrace | funcSig
405     function excludeFromLimits(address account!, bool isExcluded!) external onlyOwner {
406         _excludeFromLimits(account!, isExcluded!);
407     }
408
    ftrace | funcSig
409     function _excludeFromLimits(address account!, bool isExcluded!) internal {
410         isExcludedFromLimits[account!] = isExcluded!;
411         emit ExcludeFromLimits(account!, isExcluded!);
412     }
  
```



## ⚠ Max Transaction and Holding Modify function

Contract renounced, function can not be triggered by owner.

If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot

```

414         ftrace | funcSig
415         function updateMaxWalletAmount(uint256 _maxWalletAmount!) public onlyOwner {
416             require(_maxWalletAmount! >= _maxWalletSafeLimit(), "MaxWallet: Limit too low");
417             maxWalletAmount = _maxWalletAmount!;
418             emit MaxWalletAmountUpdated(_maxWalletAmount!);
419         }
420
421         ftrace | funcSig
422         function _maxWalletSafeLimit() private view returns (uint256) {
423             return totalSupply() / 1000;
424         }
425
426         ftrace | funcSig
427         function _maxTxSafeLimit() private view returns (uint256) {
428             return totalSupply() * 5 / 10000;
429         }
430
431         ftrace | funcSig
432         function updateMaxBuyAmount(uint256 _maxBuyAmount!) public onlyOwner {
433             require(_maxBuyAmount! >= _maxTxSafeLimit(), "MaxTx: Limit too low");
434             maxBuyAmount = _maxBuyAmount!;
435             emit MaxBuyAmountUpdated(_maxBuyAmount!);
436         }
437
438         ftrace | funcSig
439         function updateMaxSellAmount(uint256 _maxSellAmount!) public onlyOwner {
440             require(_maxSellAmount! >= _maxTxSafeLimit(), "MaxTx: Limit too low");
441             maxSellAmount = _maxSellAmount!;
442             emit MaxSellAmountUpdated(_maxSellAmount!);
443         }
  
```

## ⚠ Blacklist [ Set wallets exclude from dividends ]

Contract renounced, function can not be triggered by owner.

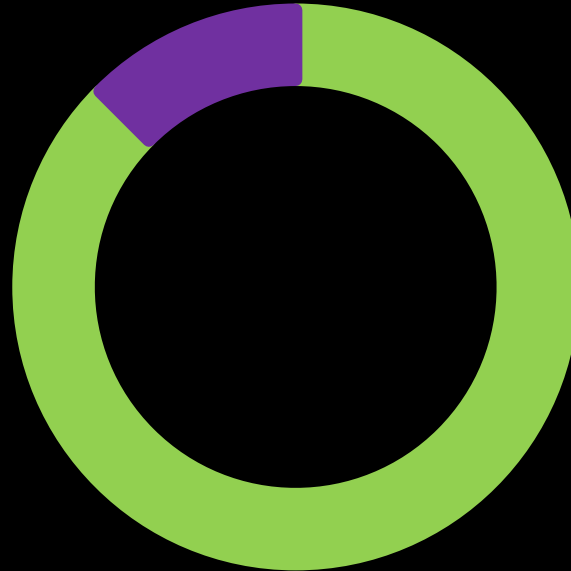
Case: Set Wallets exclude from dividends. Not Blacklist from trading.

```

253         ftrace | funcSig
254         function excludeFromDividends(address account!, bool isExcluded!) external onlyOwner {
255             _excludeFromDividends(account!, isExcluded!);
256         }
257
258         ftrace | funcSig
259         function _excludeFromDividends(address account!, bool isExcluded!) internal override {
260             dividendTracker.excludeFromDividends(account!, balanceOf(account!), isExcluded!);
261         }
  
```

## Contract Security

Total Findings: 8



■ **High Severity Issues:** High possibility to cause problems, need to be resolved.

■ **Medium Severity Issue:** Will likely cause problems, recommended to resolve.

■ **Low Severity Issues:** Won't cause problems, but for improvement purposes could be adjusted.

■ **Informational Severity Issues:** Not harmful in any way, information for the developer team.

## Contract Security

### List of Found Issues

 **High severity Issues: (0)**

 **Medium severity issues: (0)**

 **Low severity issues: (7)**

- Missing Events
- Long number literals
- Outdated Compiler Version
- Multiple Compiler Versions
- Floating Pragma
- Missing Zero Address Validation
- Unchecked Transfer

 **Informational severity issues: (1)**

- Public Functions Should be Declared External

## Contract Weakness Classisication

THE SMART CONTRACT WEAKNESS CLASSIFICATION REGISTRY (SWC REGISTRY) IS AN IMPLEMENTATION OF THE WEAKNESS CLASSIFICATION SCHEME PROPOSED IN EIP-1470. IT IS LOOSELY ALIGNED TO THE TERMINOLOGIES AND STRUCTURE USED IN THE COMMON WEAKNESS ENUMERATION (CWE) WHILE OVERLAYING A WIDE RANGE OF WEAKNESS VARIANTS THAT ARE

ID	Description	AI	Manual	Result
SWC-100	Function Default Visibility	Passed	Passed	Passed
SWC-101	Integer Overflow and Underflow	Passed	Passed	Passed
SWC-102	Outdated Compiler Version	low	Passed	Passed
SWC-103	Floating Pragma	low	Passed	Passed
SWC-104	Unchecked Call Return Value	Passed	Passed	Passed
SWC-105	Unprotected Ether Withdrawal	Passed	Passed	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed	Passed	Passed
SWC-107	Reentrancy	Passed	Passed	Passed
SWC-108	State Variable Default Visibility	Passed	Passed	Passed
SWC-109	Uninitialized Storage Pointer	Passed	Passed	Passed
SWC-110	Assert Violation	Passed	Passed	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed	Passed	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed	Passed	Passed
SWC-113	DoS with Failed Call	Passed	Passed	Passed
SWC-114	Transaction Order Dependence	Passed	Passed	Passed
SWC-115	Authorization through tx.origin	Passed	Passed	Passed
SWC-116	Block values as a proxy for time	Passed	Passed	Passed
SWC-117	Signature Malleability	Passed	Passed	Passed
SWC-118	Incorrect Constructor Name	Passed	Passed	Passed

SWC-119	Shadowing State Variables	Passed	Passed	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed	Passed	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed	Passed	Passed
SWC-122	Lack of Proper Signature Verification	Passed	Passed	Passed
SWC-123	Requirement Violation	Passed	Passed	Passed
SWC-124	Write to Arbitrary Storage Location	Passed	Passed	Passed
SWC-125	Incorrect Inheritance Order	Passed	Passed	Passed
SWC-126	Insufficient Gas Griefing	Passed	Passed	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed	Passed	Passed
SWC-128	DoS With Block Gas Limit	Passed	Passed	Passed
SWC-129	Typographical Error	low	Passed	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed	Passed	Passed
SWC-131	Presence of unused variables	Passed	Passed	Passed
SWC-132	Unexpected Ether balance	Passed	Passed	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed	Passed	Passed
SWC-134	Message call with hardcoded gas amount	Passed	Passed	Passed
SWC-135	Code With No Effects	Passed	Passed	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed	Passed	Passed

## Detected High and Medium Severity Vulnerability Description.

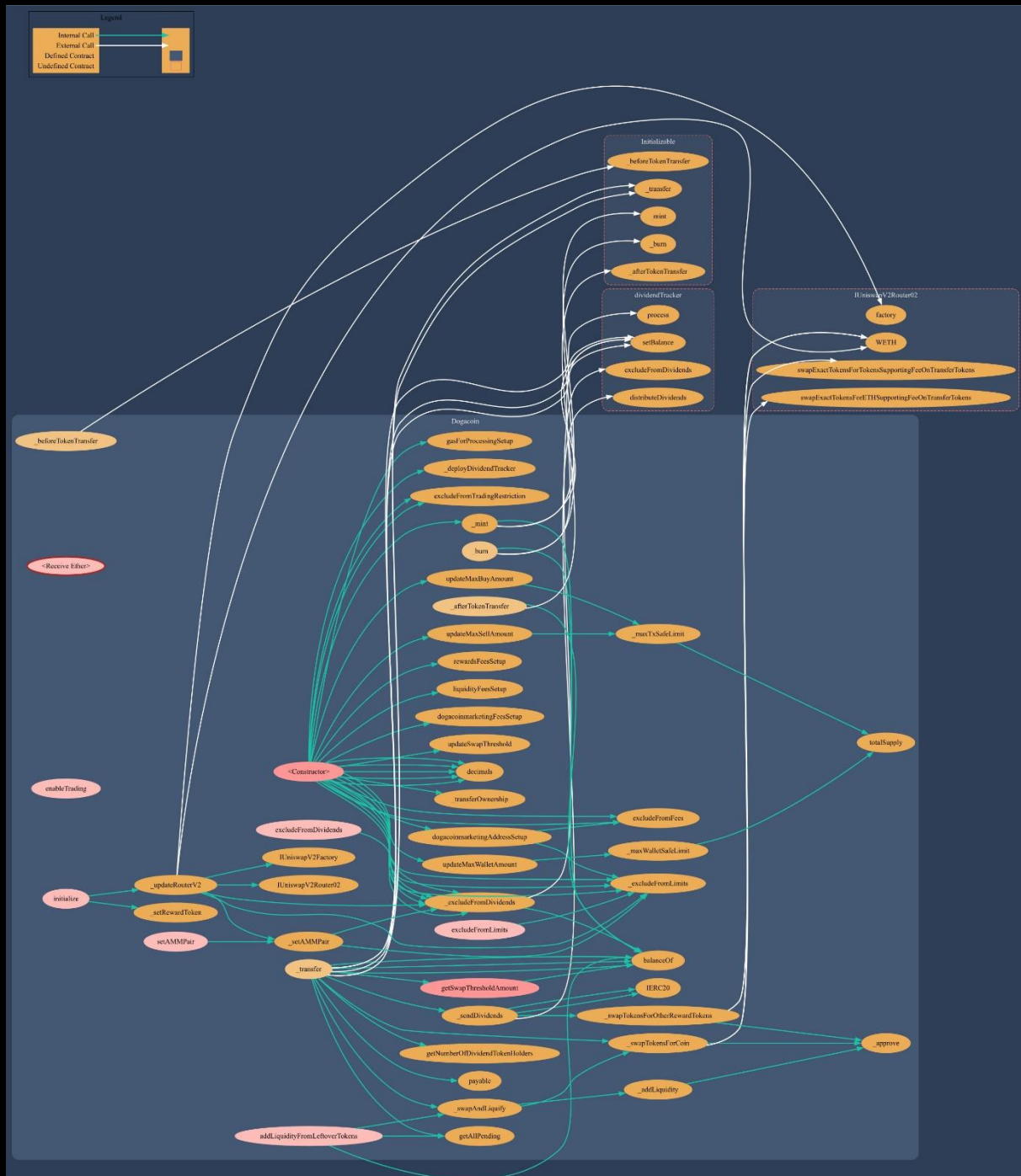
 No High or Medium Severity Vulnerability Issues found

 Outdated Compiler Version

Item: 1	Location:	Line 7	Severity:	 Low
---------	-----------	--------	-----------	---

<b>Function</b>	Using an outdated compiler version can be problematic especially if there are publicly disclosed bugs and issues that affect the current compiler version. The following outdated versions were detected: /doga.sol - 0.8.19
<b>Remedation</b>	It is recommended to use a recent version of the Solidity compiler that should not be the most recent version, and it should not be an outdated version as well. Using very old versions of Solidity prevents the benefits of bug fixes and newer security checks. Consider using the solidity version v0.8.24, which patches most solidity vulnerabilities.

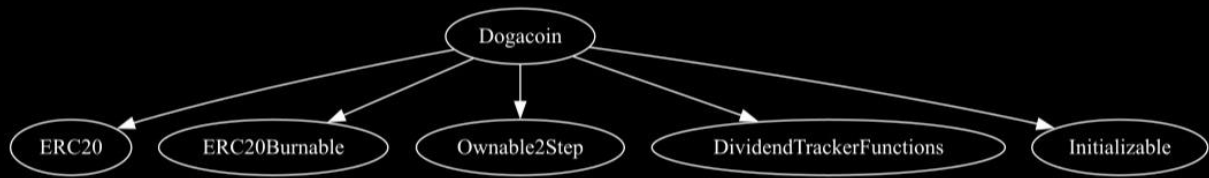
## Contract Flow Graph





















































## Inheritance Graph



## Contract Functions



















Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
<b>Dogacoin</b>	Implementation	ERC20, ERC20Burnable, Ownable2Step, DividendTracker Functions, Initializable		
L		Public 		ERC20
L	initialize	External 		initializer
L		External 		NO 
L	decimals	Public 		NO 
L	_swapTokensForCoin	Private 		
L	updateSwapThreshold	Public 		onlyOwner
L	getSwapThresholdAmount	Public 		NO 
L	getAllPending	Public 		NO 
L	dogacoinmarketingAddressSetup	Public 		onlyOwner
L	dogacoinmarketingFeesSetup	Public 		onlyOwner
L	_swapAndLiquify	Private 		
L	_addLiquidity	Private 		
L	addLiquidityFromLeftoverTokens	External 		NO 
L	liquidityFeesSetup	Public 		onlyOwner




































L	_swapTokensForOtherRewardTokens	Private 🔒	⬢	
L	_sendDividends	Private 🔒	⬢	
L	excludeFromDividends	External ⚠	⬢	onlyOwner
L	_excludeFromDividends	Internal 🔒	⬢	
L	rewardsFeesSetup	Public ⚠	⬢	onlyOwner
L	_burn	Internal 🔒	⬢	
L	_mint	Internal 🔒	⬢	
L	excludeFromFees	Public ⚠	⬢	onlyOwner
L	_transfer	Internal 🔒	⬢	
L	_updateRouterV2	Private 🔒	⬢	
L	setAMMPair	External ⚠	⬢	onlyOwner
L	_setAMMPair	Private 🔒	⬢	
L	excludeFromLimits	External ⚠	⬢	onlyOwner
L	_excludeFromLimits	Internal 🔒	⬢	
L	updateMaxWalletAmount	Public ⚠	⬢	onlyOwner
L	_maxWalletSafeLimit	Private 🔒		
L	_maxTxSafeLimit	Private 🔒		
L	updateMaxBuyAmount	Public ⚠	⬢	onlyOwner
L	updateMaxSellAmount	Public ⚠	⬢	onlyOwner

L	enableTrading	External 		onlyOwner
L	excludeFromTradingRestriction	Public 		onlyOwner
L	_beforeTokenTransfer	Internal 		
L	_afterTokenTransfer	Internal 		
<b>ERC20</b>	Implementation	Context, IERC20, IERC20Metadata		
L		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 
L	_transfer	Internal 		
L	_mint	Internal 		
L	_burn	Internal 		
L	_approve	Internal 		

L	_spendAllowance	Internal 🔒	🔒	
L	_beforeTokenTransfer	Internal 🔒	🔒	
L	_afterTokenTransfer	Internal 🔒	🔒	
<b>ERC20Burnable</b>	Implementation	Context, ERC20		
L	burn	Public 🔓	🔒	NO 🔓
L	burnFrom	Public 🔓	🔒	NO 🔓
<b>Ownable2Step</b>	Implementation	Ownable		
L	pendingOwner	Public 🔓		NO 🔓
L	transferOwnership	Public 🔓	🔒	onlyOwner
L	_transferOwnership	Internal 🔒	🔒	
L	acceptOwnership	Public 🔓	🔒	NO 🔓
<b>SafeMathUint</b>	Library			
L	toInt256Safe	Internal 🔒		
<b>SafeMathInt</b>	Library			
L	toUint256Safe	Internal 🔒		
<b>TruncatedERC20</b>	Implementation			
L		Public 🔓	🔒	NO 🔓
L	name	Public 🔓		NO 🔓
L	symbol	Public 🔓		NO 🔓
L	decimals	Public 🔓		NO 🔓

L	totalSupply	Public 🔒		NO 🔒
L	balanceOf	Public 🔒		NO 🔒
L	_mint	Internal 🔒	🔒	
L	_burn	Internal 🔒	🔒	
<b>DividendPayingTokenInterface</b>	Interface			
L	dividendOf	External 🔒		NO 🔒
<b>DividendPayingTokenOptionalInterface</b>	Interface			
L	withdrawableDividendOf	External 🔒		NO 🔒
L	withdrawnDividendOf	External 🔒		NO 🔒
L	accumulativeDividendOf	External 🔒		NO 🔒
<b>DividendPayingToken</b>	Implementation	TruncatedERC20 , DividendPayingTokenInterface, DividendPayingTokenOptionalInterface		
L		Public 🔒	🔒	TruncatedERC20
L	distributeDividends	Public 🔒	🔒	NO 🔒
L	_withdrawDividend	Internal 🔒	🔒	
L	dividendOf	Public 🔒		NO 🔒
L	withdrawableDividendOf	Public 🔒		NO 🔒
L	withdrawnDividendOf	Public 🔒		NO 🔒














L	accumulativeDividendOf	Public 		NO 
L	_mint	Internal 		
L	_burn	Internal 		
L	_setBalance	Internal 		
<b>IterableMapping</b>	Library			
L	get	Public 		NO 
L	getIndexOfKey	Public 		NO 
L	getKeyAtIndex	Public 		NO 
L	size	Public 		NO 
L	set	Public 		NO 
L	remove	Public 		NO 
<b>DividendTracker</b>	Implementation	Ownable, DividendPaying Token		
L		Public 		DividendPaying Token
L	setRewardToken	External 		onlyOwner
L	excludeFromDividends	External 		onlyOwner
L	claimWaitSetup	Public 		onlyOwner
L	getNumberOfTokenHolders	External 		NO 
L	getAccountData	Public 		NO 
L	getAccountDataAtIndex	Public 		NO 
L	claim	Public 		onlyOwner
L	_canAutoClaim	Private 		













L	setBalance	Public 		onlyOwner
L	process	External 		onlyOwner
<b>DividendTracker Functions</b>	Implementation	Ownable2Step		
L	_deployDividendTracker	Internal 		
L	_setRewardToken	Internal 		
L	gasForProcessingSetup	Public 		onlyOwner
L	claimWaitSetup	External 		onlyOwner
L	_excludeFromDividends	Internal 		
L	isExcludedFromDividends	Public 		NO 
L	claim	External 		NO 
L	getClaimWait	External 		NO 
L	getTotalDividendsDistributed	External 		NO 
L	withdrawableDividendOf	Public 		NO 
L	dividendTokenBalanceOf	Public 		NO 
L	dividendTokenTotalSupply	Public 		NO 
L	getAccountDividendsInfo	External 		NO 
L	getAccountDividendsInfoAtIndex	External 		NO 
L	getLastProcessedIndex	External 		NO 











L	getNumberOfDividendTokenHolders	Public ¶		NO ¶
L	process	External ¶	⦿	NO ¶
<b>Initializable</b>	Implementation			
<b>IUniswapV2Factory</b>	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 ¶
<b>IUniswapV2Pair</b>	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 ¶
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 ¶
<b>IUniswapV2Router01</b>	Interface			
L	factory	External ¶		NO ¶
L	WETH	External ¶		NO ¶
L	addLiquidity	External ¶	⦿	NO ¶

L	addLiquidityETH	External ¶		NO ¶
L	removeLiquidity	External ¶		NO ¶
L	removeLiquidity ETH	External ¶		NO ¶
L	removeLiquidity WithPermit	External ¶		NO ¶
L	removeLiquidity ETHWithPermit	External ¶		NO ¶
L	swapExactTokes nsForTokens	External ¶		NO ¶
L	swapTokensFor ExactTokens	External ¶		NO ¶
L	swapExactETHF orTokens	External ¶		NO ¶
L	swapTokensFor ExactETH	External ¶		NO ¶
L	swapExactTokes nsForETH	External ¶		NO ¶
L	swapETHForExa ctTokens	External ¶		NO ¶
L	quote	External ¶		NO ¶
L	getAmountOut	External ¶		NO ¶
L	getAmountIn	External ¶		NO ¶
L	getAmountsOut	External ¶		NO ¶
L	getAmountsIn	External ¶		NO ¶
<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		
L	removeLiquidity ETHSupportingFeeOnTransferTokens	External ¶		NO ¶
L	removeLiquidity ETHWithPermit SupportingFeeO	External ¶		NO ¶

	nTransferTokens			
L	swapExactTokensForTokensSupportingFeeOnTransferTokens	External !		NO!
L	swapExactETHForTokensSupportingFeeOnTransferTokens	External !		NO!
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External !		NO!
<b>Ownable</b>	Implementation	Context		
L		Public !		NO!
L	owner	Public !		NO!
L	_checkOwner	Internal 		
L	renounceOwnership	Public !		onlyOwner
L	transferOwnership	Public !		onlyOwner
L	_transferOwnership	Internal 		
<b>IERC20</b>	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 
<b>Context</b>	Implementation			
L	_msgSender	Internal 		
L	_msgData	Internal 		



Function  
can modify  
state



Function  
is payable

## Audit Scope

### Audit Method.

Our smart contract audit is an extensive methodical examination and analysis of the smart contract's code that is used to interact with the blockchain. Goal: discover errors, issues and security vulnerabilities in the code. Findings getting reported and improvements getting suggested.

### Automatic and Manual Review

We are using automated tools to scan functions and weaknesses of the contract. Transfers, integer over-undeflow checks such as all CWE events.

### Tools we use:

Visual Studio Code

CWE

SWC

Solidity Scan

SVD

In manual code review our auditor looking at source code and performing line by line examination. This method helps to clarify developer's coding decisions and business logic.

## Skeleton Ecosystem

<https://skeletonecosystem.com>

<https://github.com/SkeletonEcosystem/Audits>

