



# Audit Report

## **DOGE-1**

December 2021

Type       BEP20

Address     0xBF5C0dcFd2925fC2f4324cf3E0C9f31C0E36F771

Audited by  © coinscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>2</b>
<b>Audit Updates</b>	<b>2</b>
<b>Contract Analysis</b>	<b>3</b>
<b>ELFM - Exceed Limit Fees Manipulation</b>	<b>3</b>
<b>Description</b>	<b>4</b>
<b>Recommendation</b>	<b>4</b>
<b>ULTW - Unlimited Liquidity to Team Wallet</b>	<b>5</b>
<b>Description</b>	<b>5</b>
<b>Recommendation</b>	<b>5</b>
<b>BC - Blacklisted Contracts</b>	<b>6</b>
<b>Description</b>	<b>6</b>
<b>Recommendation</b>	<b>6</b>
<b>Contract Diagnostics</b>	<b>7</b>
<b>Contract Functions</b>	<b>8</b>
<b>Contract Flow</b>	<b>13</b>
<b>Domain Info</b>	<b>14</b>
<b>Summary</b>	<b>15</b>
<b>Disclaimer</b>	<b>16</b>
<b>About Coinscope</b>	<b>17</b>

## Contract Review

<b>Contract Name</b>	DOGE1
<b>Compiler Version</b>	v0.8.4+commit.c7e474f2
<b>Optimization</b>	200 runs
<b>Licence</b>	Unlicense
<b>Explorer</b>	<a href="https://bscscan.com/token/0xBF5C0dcFd2925fC2f4324cf3E0C9f31C0E36F771">https://bscscan.com/token/0xBF5C0dcFd2925fC2f4324cf3E0C9f31C0E36F771</a>
<b>Symbol</b>	DOGE-1
<b>Decimals</b>	9
<b>Total Supply</b>	100,000,000,000
<b>Source</b>	contract.sol
<b>Domain</b>	doge-1-satellite.com

## Audit Updates

<b>Initial Audit</b>	27th December 2021
<b>Corrected</b>	

# Contract Analysis

● Critical
 ● Medium
 ● Pass

Severity	Code	Description
<span style="color: blue;">●</span>	MT	Contract Owner is not able to mint new tokens
<span style="color: blue;">●</span>	BT	Contract Owner is not able to burn tokens from specific wallet
<span style="color: red;">●</span>	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
<span style="color: blue;">●</span>	ST	Contract Owner is not able to pause transactions for everyone else except him
<span style="color: blue;">●</span>	OCTD	Contract Owner is not able to transfer tokens from specific address
<span style="color: orange;">●</span>	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
<span style="color: orange;">●</span>	BC	Contract Owner is not able to blacklist wallets from selling

## ELFM - Exceed Limit Fees Manipulation

<b>Criticality</b>	critical
<b>Location</b>	<a href="https://bscscan.com/address/0xbf5c0dcfd2925fc2f4324cf3e0c9f31c0e36f771#code#L846">https://bscscan.com/address/0xbf5c0dcfd2925fc2f4324cf3e0c9f31c0e36f771#code#L846</a>

### Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setTaxFeePercent` function with a high percentage value.

```
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {  
    _taxFee = taxFee;  
}
```

### Recommendation

The contract could embody a check for the maximum acceptable value.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

## ULTW - Unlimited Liquidity to Team Wallet

<b>Criticality</b>	medium
<b>Location</b>	<a href="https://bscscan.com/address/0xbf5c0dcfd2925fc2f4324cf3e0c9f31c0e36f771#code#L646">https://bscscan.com/address/0xbf5c0dcfd2925fc2f4324cf3e0c9f31c0e36f771#code#L646</a>

### Description

The contract transfers funds to the team wallet. These funds have been swiped from the swap & liquidity feature. The owner may take advantage of it by setting a high fee to the `_feeRate` variable.

```
function swapTokens(uint256 contractTokenBalance) private lockTheSwap {
    swapTokensForEth(contractTokenBalance);

    //Send to Marketing address
    uint256 contractETHBalance = address(this).balance;
    if(contractETHBalance > 0) {
        sendETHToFee(address(this).balance);
    }
}
```

### Recommendation

The contract could embody a check for the maximum acceptable value.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

## BC - Blacklisted Contracts

<b>Criticality</b>	medium
<b>Location</b>	<a href="https://bscscan.com/address/0xBF5C0dcFd2925fC2f4324cf3E0C9f31C0E36F771#code#L605">https://bscscan.com/address/0xBF5C0dcFd2925fC2f4324cf3E0C9f31C0E36F771#code#L605</a>

### Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `_isSniper` function.

```
require(!_isSniper[to], "You have no power here!");  
require(!_isSniper[msg.sender], "You have no power here!");
```

### Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

# Contract Diagnostics

Pass	Name
✓	Integer Underflow
✓	Parity Multisig Bug
✓	Callstack Depth Attack
✓	Transaction-Ordering Dependency
✓	Timestamp Dependency
✓	Re-Entrancy



# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>SafeMath</b>	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
<b>Address</b>	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	

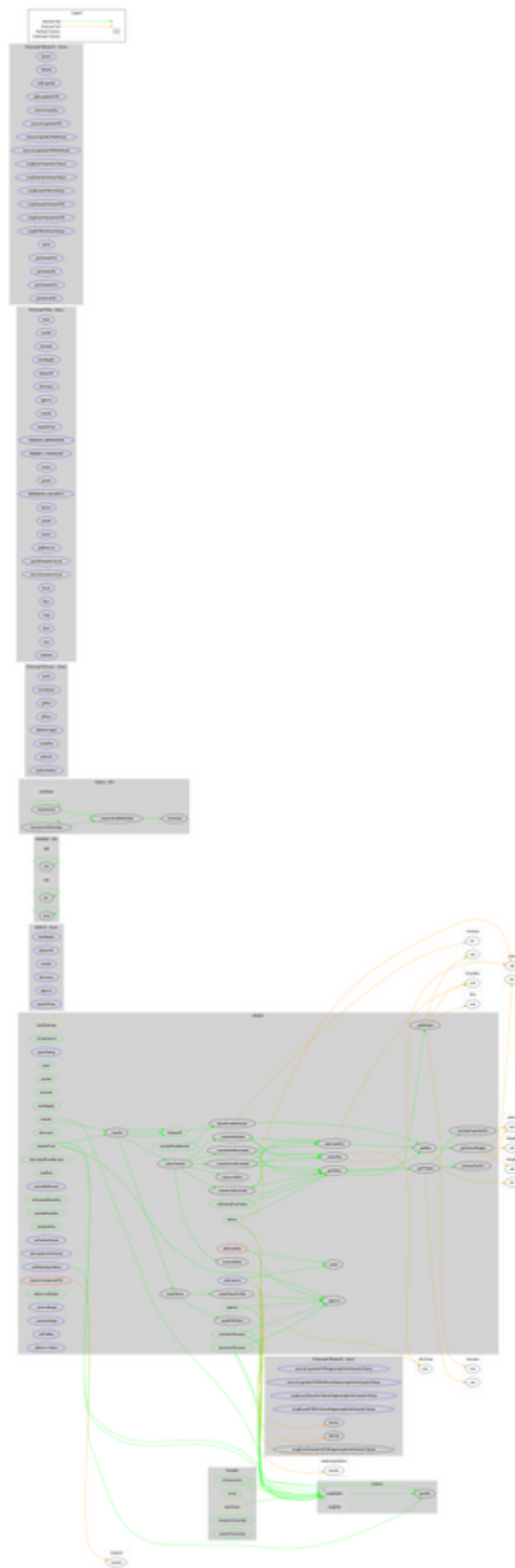
	_functionCallWithValue	Private	✓	
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
<b>IUniswapV2Pair</b>	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-

	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
<b>IUniswapV2Router01</b>	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		

	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
<b>DOGE1</b>	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	initContract	External	✓	onlyOwner
	openTrading	External	✓	onlyOwner
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	totalFees	Public		-
	deliver	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	_approve	Private	✓	
	_transfer	Private	✓	
	swapTokens	Private	✓	lockTheSwap

	sendETHToFee	Private	✓	
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
	_transferBothExcluded	Private	✓	
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private	✓	
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setTaxFeePercent	External	✓	onlyOwner
	setLiquidityFeePercent	External	✓	onlyOwner
	setMarketingAddress	External	✓	onlyOwner
	transferToAddressETH	Private	✓	
	isRemovedSniper	Public		-
	_removeSniper	External	✓	onlyOwner
	_amnestySniper	External	✓	onlyOwner
	setFeeRate	External	✓	onlyOwner
	<Receive Ether>	External	Payable	-

# Contract Flow



## Domain Info

<b>Domain Name</b>	doge-1-satellite.com
<b>Registry Domain ID</b>	2660239752_DOMAIN_COM-VRSN
<b>Creation Date</b>	2021-12-08T08:38:17Z
<b>Updated Date</b>	2021-12-08T08:38:19Z
<b>Registry Expiry Date</b>	
<b>Registrar WHOIS Server</b>	whois.google.com
<b>Registrar URL</b>	https://domains.google.com
<b>Registrar</b>	Google LLC
<b>Registrar IANA ID</b>	895

The domain has been created 19 days before the creation of the audit.

There is no public billing information, the creator is protected by the privacy settings.

## Summary

DOGE-1 is aiming to be an ambitious meme token. There are some functions that can be abused by the owner, like manipulating fees and transferring funds to the team's wallet. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.



# 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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

## About Coinscope

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.



The Coinscope.co team

<https://www.coinscope.co>