RugFreeCoins Audit

MoonPuppyDoge Token

Smart Contract Security Audit

July 26, 2021

Contents

Audit details

Audited project

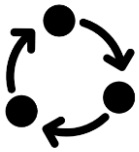
MoonPuppyDoge Token

Contract Address

0xb6b9fcee03d3c5dfc3f3f0dc713358bbcb2be80c

Client contact

MoonPuppyDoge Team



Blockchain

Binance smart chain

Project website

https://moonpuppydoge.com/

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

Rugfreecoins was commissioned by MoonPuppyDoge to perform an audit of the smart contract.

https://bscscan.com/address/0xb6b9fcee03d3c5dfc3f3f0dc713358bbcb2be80c

The focus of this audit is to verify that the smart contract is secure, resilient and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, long term sustainability and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

About the project

MoonPuppyDoge is a token built on the Binance Smart Chain. Each transaction, purchase incur a 11% fee, and sales incur an 15% fee.

Features

- MoonPuppyDoge Buy-Back function in the contract automatically buys back and burns tokens after every sale, to keep the price stable.
- MoonPuppyDoge token holders benefit through static rewards, that tokens will be distributed among every holder proportional to how many tokens each individual holds.
- The liquidity fee, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity. This is a key element for decentralized exchanges like Pancakeswap.
- **The 3% Charity fee** per transaction will be swapped to BNB and sent to a private wallet which will be allocated for charity. This will empower the MoonPuppyDoge community in the long run and motivate more people to join in!

Tokenomics

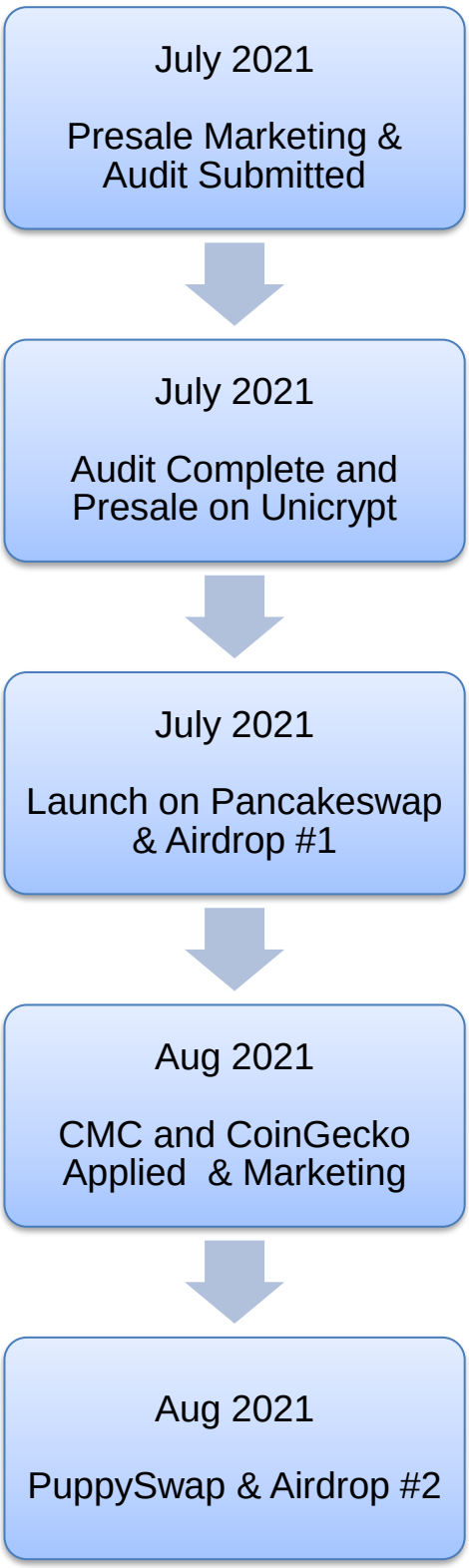
11% when buying

- 2% of trade goes to holders pockets.
- 3% of every trade goes to a charity wallet.
- 6% of trade used to buy back tokens.

14% when selling

- 2% of trade goes to holders pockets.
- 3% of every trade goes to a charity wallet.
- 3% of every trade goes to the liquidity pool.
- 6% of trade used to buy back tokens.

Roadmap


July 2021
Presale Marketing & Audit Submitted
July 2021
Audit Complete and Presale on Unicrypt
July 2021
Launch on Pancakeswap & Airdrop #1
Aug 2021
CMC and CoinGecko Applied & Marketing
Aug 2021
PuppySwap & Airdrop #2

Target market and the concept

Target market

- Anyone who's interested in Crypto space with long term investment plans.
- Anyone who's ready to earn a passive income by holding tokens.
- Anyone who's interested in trading tokens.
- Anyone who's interested in making financial transactions with any other party using MoonPuppyDoge as the currency.

Core concept

The static reward system

2% of tokens will be distributed among the holders per every buy and sell.

Sustainable mechanism

The buyback and burn mechanism collects 6% tax on each transaction, which is stored inside the contract. Whenever a buy or sell occurs, a fraction of the buyback amount is used to automatically purchase tokens from the liquidity pool. Those tokens are immediately burned after purchase, which keeps the token price stable.

The liquidity fee of 3%, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity.

Good cause

The 3% Charity fee per transaction will be swapped to BNB and sent to a private wallet that will be allocated for charity.

Potential to grow with score points

1.	Project efficiency	7/10
2.	Project uniqueness	6/10
3	Information quality	6/10
4	Service quality	7/10
5	System quality	6/10
6	Impact on the community	7/10
7	Impact on the business	7/10
8	Preparing for the future	4/10
Total Points		**6.25/10**

Contract details

Token contract details for 26th July 2021

Contract name	MoonPuppyDoge Token
Contract address	0xb6b9fcee03d3c5dfc3f3f0dc713358bbcb2be80c
Token supply	1,000,000,000,000,000
Token ticker	MPDOGE
Decimals	9
Token holders	1(Prior to the launch)
Transaction count	1 (Prior to the launch)
Contract deployer address	0xC1cf4fe56D84238FbE8ee813Bab547ceB454261f
Contract's current owner address	0xc1cf4fe56d84238fbe8ee813bab547ceb454261f

Contract code function details

No	Category	Item	Result
1	Coding conventions	BRC20 Token standards	pass
		compile errors	pass
		Compiler version security	pass
		visibility specifiers	pass
		Gas consumption	pass
		SafeMath features	pass
		Fallback usage	pass
		tx.origin usage	pass
		deprecated items	pass
		Redundant code	pass
		Overriding variables	pass
2	Function call audit	Authorization of function call	pass
		Low level function (call/delegate call) security	pass
		Returned value security	pass
		Selfdestruct function security	pass
3	Business security	Access control of owners	pass
		Business logics	pass
		Business implementations	pass
4	Integer overflow/underflow		pass
5	Reentrancy		pass
6	Exceptional reachable state		pass
7	Transaction ordering dependence		pass
8	Block properties dependence		pass
9	Pseudo random number generator (PRNG)		pass
10	DoS (Denial of Service)		pass
11	Token vesting implementation		pass
12	Fake deposit		pass
13	Event security		pass

Contract description table

Below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions and implementations with its visibility and mutability.

Contract	Type	Bases		
└	Function Name	Visibility	Mutability	Modifiers
Context	**Implementation**			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
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 🔒		
Address	**Library**			
└	isContract	Internal 🔒		
└	sendValue	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCall	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	functionCallWithValue	Internal 🔒	🛑	
└	_functionCallWithValue	Private 🔐	🛑	
Ownable	**Implementation**	**Context**		
└		Public ❗	🛑	NO❗
└	owner	Public ❗		NO❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	getUnlockTime	Public ❗		NO❗
└	getTime	Public ❗		NO❗
└	lock	Public ❗	🛑	onlyOwner
└	unlock	Public ❗	🛑	NO❗
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❗
└	factory	External ❗		NO❗
└	token0	External ❗		NO❗
└	token1	External ❗		NO❗
└	getReserves	External ❗		NO❗

L	price0CumulativeLast	External ❗		NO❗
L	price1CumulativeLast	External ❗		NO❗
L	kLast	External ❗		NO❗
L	burn	External ❗	🛑	NO❗
L	swap	External ❗	🛑	NO❗
L	skim	External ❗	🛑	NO❗
L	sync	External ❗	🛑	NO❗
L	initialize	External ❗	🛑	NO❗
IUniswapV2Router01	**Interface**			
L	factory	External ❗		NO❗
L	WETH	External ❗		NO❗
L	addLiquidity	External ❗	🛑	NO❗
L	addLiquidityETH	External ❗	💵	NO❗
L	removeLiquidity	External ❗	🛑	NO❗
L	removeLiquidityETH	External ❗	🛑	NO❗
L	removeLiquidityWithPermit	External ❗	🛑	NO❗
L	removeLiquidityETHWithPermit	External ❗	🛑	NO❗
L	swapExactTokensForTokens	External ❗	🛑	NO❗
L	swapTokensForExactTokens	External ❗	🛑	NO❗
L	swapExactETHForTokens	External ❗	💵	NO❗
L	swapTokensForExactETH	External ❗	🛑	NO❗

L	swapExactTokens ForETH	External ❗	🛑	NO❗
L	swapETHForExact Tokens	External ❗	💵	NO❗
L	quote	External ❗		NO❗
L	getAmountOut	External ❗		NO❗
L	getAmountIn	External ❗		NO❗
L	getAmountsOut	External ❗		NO❗
L	getAmountsIn	External ❗		NO❗
IUniswapV2Router02	**Interface**	**IUniswapV2Rou ter01**		
L	removeLiquidityET HSupportingFeeO nTransferTokens	External ❗	🛑	NO❗
L	removeLiquidityET HWithPermitSupp ortingFeeOnTransf erTokens	External ❗	🛑	NO❗
L	swapExactTokens ForTokensSupport ingFeeOnTransfer Tokens	External ❗	🛑	NO❗
L	swapExactETHFor TokensSupporting FeeOnTransferTo kens	External ❗	💵	NO❗
L	swapExactTokens ForETHSupporting FeeOnTransferTo kens	External ❗	🛑	NO❗
MoonPuppyDoge	**Implementation**	**Context, IERC20, Ownable**		
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	isExcludedFromReward	Public ❗		NO❗
L	totalFees	Public ❗		NO❗
L	minimumTokensBeforeSwapAmount	Public ❗		NO❗
L	buyBackUpperLimitAmount	Public ❗		NO❗
L	deliver	Public ❗	🛑	NO❗
L	reflectionFromToken	Public ❗		NO❗
L	tokenFromReflection	Public ❗		NO❗
L	excludeFromReward	Public ❗	🛑	onlyOwner
L	includeInReward	External ❗	🛑	onlyOwner
L	_approve	Private 🔐	🛑	
L	_transfer	Private 🔐	🛑	
L	swapTokens	Private 🔐	🛑	lockTheSwap

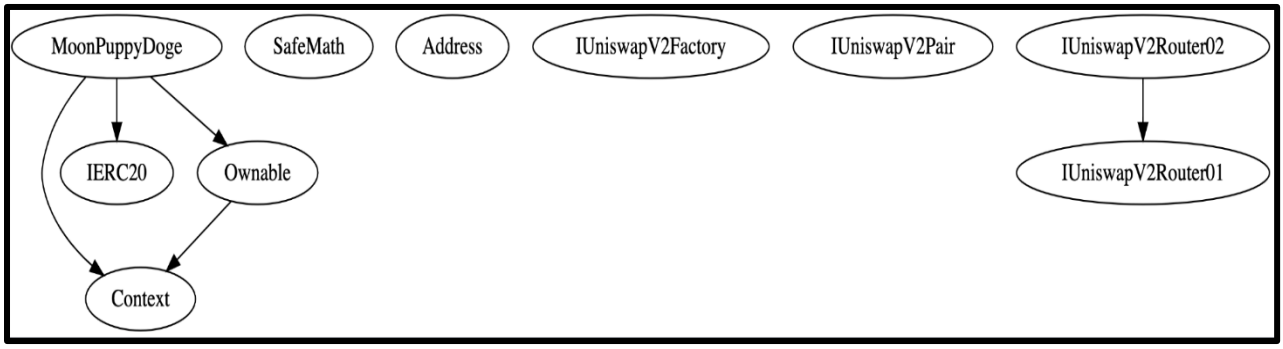
L	buyBackTokens	Private 🔐	🛑	lockTheSwap
L	swapTokensForEth	Private 🔐	🛑	
L	swapETHForTokens	Private 🔐	🛑	
L	addLiquidity	Private 🔐	🛑	
L	_tokenTransfer	Private 🔐	🛑	
L	_transferStandard	Private 🔐	🛑	
L	_transferToExcluded	Private 🔐	🛑	
L	_transferFromExcluded	Private 🔐	🛑	
L	_transferBothExcluded	Private 🔐	🛑	
L	_reflectFee	Private 🔐	🛑	
L	_getValues	Private 🔐		
L	_getTValues	Private 🔐		
L	_getRValues	Private 🔐		
L	_getRate	Private 🔐		
L	_getCurrentSupply	Private 🔐		
L	_takeLiquidity	Private 🔐	🛑	
L	calculateTaxFee	Private 🔐		
L	calculateLiquidityFee	Private 🔐		
L	removeAllFee	Private 🔐	🛑	
L	restoreAllFee	Private 🔐	🛑	
L	isExcludedFromFee	Public ❗		NO❗
L	excludeFromFee	Public ❗	🛑	onlyOwner
L	includeInFee	Public ❗	🛑	onlyOwner

L	setTaxFeePercent	External ❗	🛑	onlyOwner
L	setLiquidityFeePercent	External ❗	🛑	onlyOwner
L	setMaxTxAmount	External ❗	🛑	onlyOwner
L	setMarketingDivisor	External ❗	🛑	onlyOwner
L	setNumTokensSellToAddToLiquidity	External ❗	🛑	onlyOwner
L	setBuybackUpperLimit	External ❗	🛑	onlyOwner
L	setMarketingAddress	External ❗	🛑	onlyOwner
L	setSwapAndLiquifyEnabled	Public ❗	🛑	onlyOwner
L	setBuyBackEnabled	Public ❗	🛑	onlyOwner
L	prepareForPreSale	External ❗	🛑	onlyOwner
L	afterPreSale	External ❗	🛑	onlyOwner
L	transferToAddressETH	Private 🔐	🛑	
L		External ❗	💵	NO❗

Legend

Symbol	Meaning
🛑	**Function can modify state**
💵	**Function is payable**

Inheritance Hierarchy



Security issue checking status

- **High severity issues**
  No high severity issues found.

  .

- **Medium severity issues**
  No medium severity issues found

- **Low severity issues**

  hardcoded addresses.

  Hardcoded uniswapV2Router address makes it impossible to migrate to a new version of DEX in case of future upgrades of PancakeSwap periphery.

Owner privileges

- The owner can include/exclude wallets from rewards.

```
ftrace | funcSig
function excludeFromReward(address account⬆) public onlyOwner() {

    require(!_isExcluded[account⬆], "Account is already excluded");
    if(_rOwned[account⬆] > 0) {
        _tOwned[account⬆] = tokenFromReflection(_rOwned[account⬆]);
    }
    _isExcluded[account⬆] = true;
    _excluded.push(account⬆);
}

ftrace | funcSig
function includeInReward(address account⬆) external onlyOwner() {
    require(_isExcluded[account⬆], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account⬆) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account⬆] = 0;
            _isExcluded[account⬆] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The owner can include/exclude wallet from fees.

```
ftrace | funcSig
function excludeFromFee(address account⬆) public onlyOwner {
    _isExcludedFromFee[account⬆] = true;
}

ftrace | funcSig
function includeInFee(address account⬆) public onlyOwner {
    _isExcludedFromFee[account⬆] = false;
}
```

❖ The owner can change the tax fee.

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

❖ The owner can change the liquidity fee.

```
ftrace | funcSig
function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner() {
    _liquidityFee = liquidityFee;
}
```

❖ The owner can change the max transaction amount.

```
ftrace | funcSig
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner() {
    _maxTxAmount = maxTxAmount;
}
```

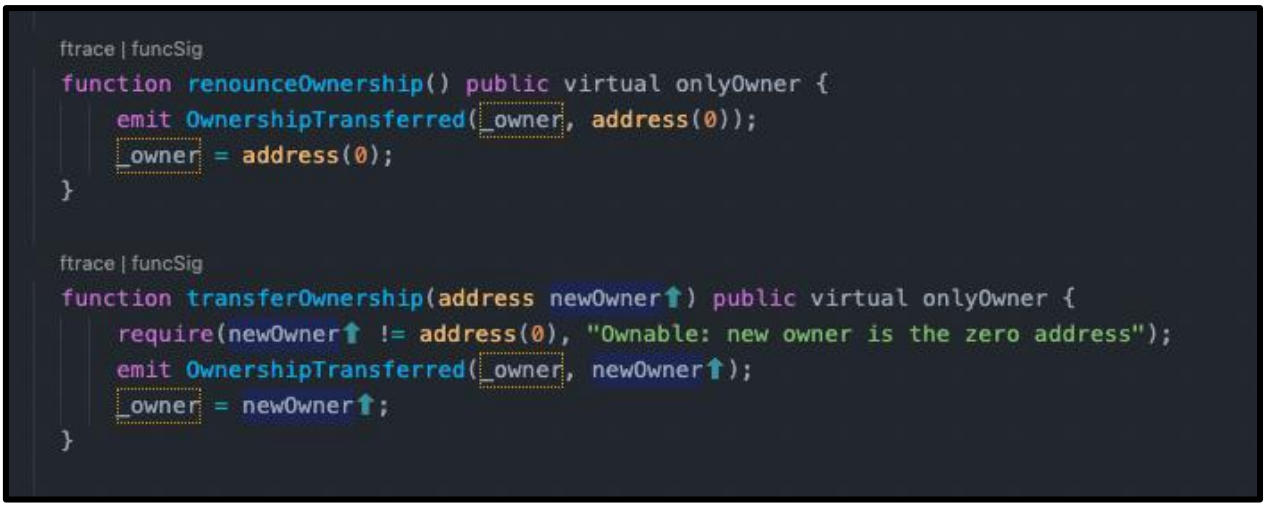
❖ The owner can change the marketing fee.

```
ftrace | funcSig
function setMarketingDivisor(uint256 divisor) external onlyOwner() {
    marketingDivisor = divisor;
}
```

❖ The owner can change the marketing address.

```
ftrace | funcSig
function setMarketingAddress(address _marketingAddress) external onlyOwner() {
    marketingAddress = payable(_marketingAddress);
}
```

❖ The owner can transfer and renounce the ownership.



Audit conclusion

While conducting the audit of the MoonPuppyDoge smart contract,it was observed that there is nothing alamaring with the code and the contract contains only a low severity issue.