Audit Report

Doggy rebaser

January 2022

Type	BEP20
Network	BSC
Address	0x6976f83ec3940f1dfcb7bd2011a5652b73021533
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	DRC
Compiler Version	v0.6.6+commit.6c089d02
Optimization	200 runs
Licence	
Explorer	https://bscscan.com/token/0x6976f83ec3940f1dfcb7bd2011a5652b73021533
Symbol	DRC
Decimals	9
Total Supply	1,000,000,000,000
Source	/contracts/DRC.sol, /contracts/SafeMath.sol, /contracts/Rebaser.sol, /contracts/Ownable.sol, /contracts/Context.sol, /contracts/Address.sol
Domain	doggyrebase.co.in

Audit Updates

Initial Audit	13th January 2022
Corrected	

Contract Analysis

Critical Medium Minor Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	OTUT	Owner Transfer User's Tokens
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling
●	MTS	Manipulate Total Supply

ST - Stop Transactions

Criticality	medium
Location	contract.sol#L1

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `_maxTxAmount` to zero.

```
if (sender != owner() && recipient != owner() && !inSwapAndLiquify) {
    require(
        amount <= _maxTxAmount,
        "DRC: Transfer amount exceeds the maxTxAmount."
    );
```

Recommendation

The contract could embody a check for not allowing setting the _maxTxAmount less than a reasonable amount. A suggested implementation could check that the maximum amount should be more than a fixed percentage of the total supply.

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.

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L1210

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by setting the `BurnFee` to a high value. This can be accomplished by configuring the `setBurnTop` and `setBurnBottom` functions.

```
function setBurnTop(uint16 burntop) external onlyOwner {
    BURN_TOP = burntop;
}

function setBurnBottom(uint16 burnbottom) external onlyOwner {
    BURN_BOTTOM = burnbottom;
}

// Line 1210, function _getRValues
rfeeValues.BurnFee = ((BURN_TOP * fee) / BURN_BOTTOM).mul(currentRate);
rfeeValues.RewardFee = fee.mul(currentRate).sub(rfeeValues.BurnFee);

// Line 1230, function _getRValues2
uint256 rTransferAmount = rAmount
    .sub(rfeeValues.FYFee)
    .sub(rfeeValues.BurnFee)
    .sub(rfeeValues.RewardFee)
    .sub(rfeeValues.BFee)
    .sub(rfeeValues.CFee);
```

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.

MTS - Manipulate Total Supply

Criticality	medium
Location	contract.sol#L1278

Description

Owner is able to manipulate total supply. This change will have a direct impact on the token price and Market Cap depending on the event of rebase (negative, or positive).

```
_totalSupply = (
    (
        initSupply
            .sub(_rOwned[BurnAddress].div(currentRate))
            .mul(DRCScalingFactor)
            .div(internalDecimals)
    )
);
```

Recommendation

The owner should carefully manage the adjustment of the circulating supply (increases or decreases), according to the token’s price fluctuations.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L07	Missing Events Arithmetic

L01 - Public Function could be Declared External

Criticality	minor
Location	contracts/DRC.sol#L26,L17,L63 and 10 more

Description

Public functions that are never called by the contract should be declared external to save gas.

```
transferRebasership
Rebaser
transferOwnership
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contracts/DRC.sol#L119,L118,L169 and 4 more

Description

Constant state variables should be declared constant to save gas.

```
symbol
name
liquidityRewardRate
...
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/DRC.sol#L17,L180,L178 and 35 more

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
Rebaser
BUSDTokenAddress
CFee
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L07 - Missing Events Arithmetic

Criticality	minor
Location	contracts/DRC.sol#L310,L306,L301 and 4 more

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
BURN_BOTTOM = burnbottom
BURN_TOP = burntop
SELL_FEE = fee
...
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

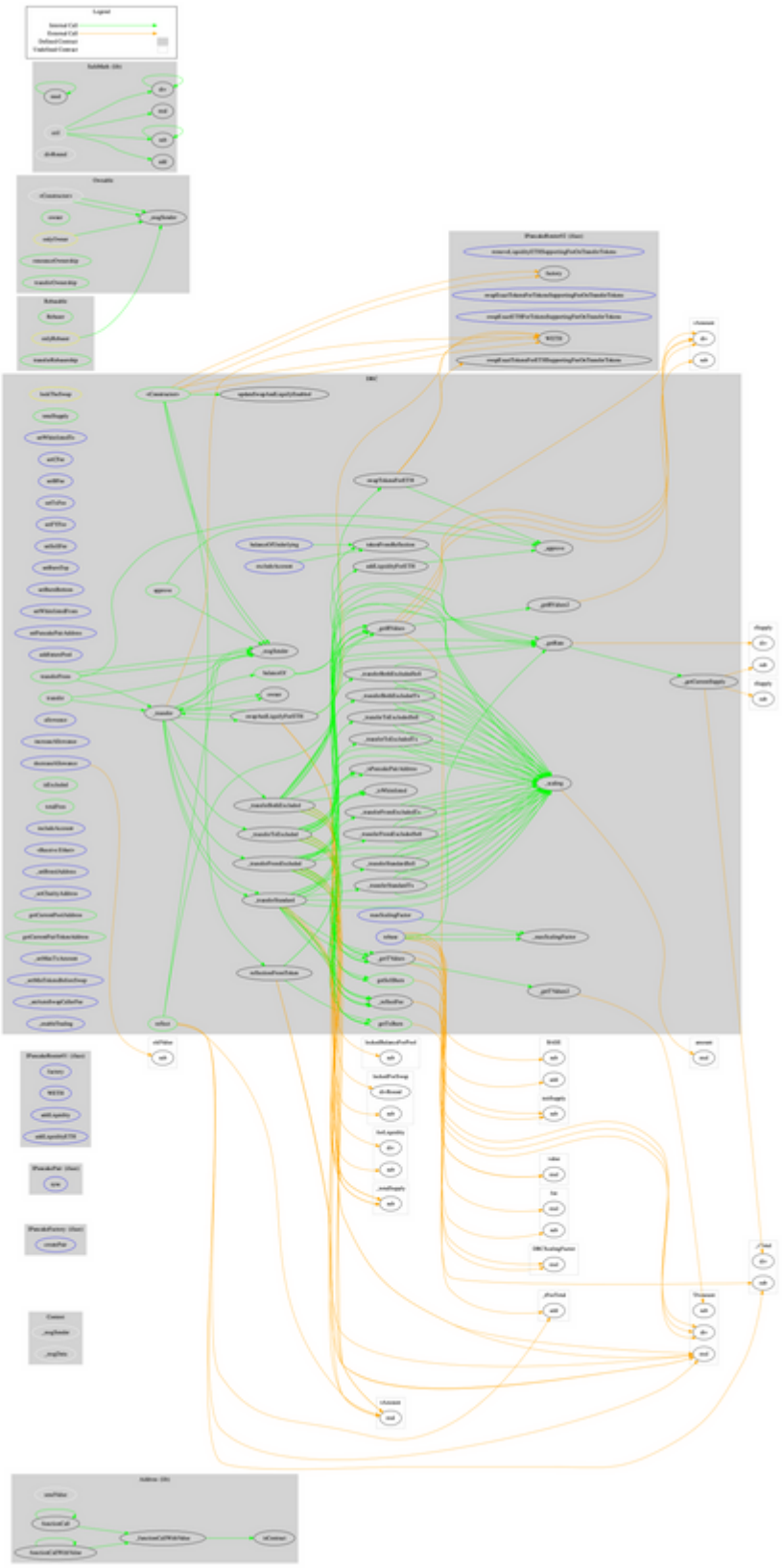
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IPancakeFactory	Interface			
	createPair	External	✓	-
IPancakePair	Interface			
	sync	External	✓	-
IPancakeRouter01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
IPancakeRouter02	Interface	IPancakeRouter01		

	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
DRC	Implementation	Ownable, Rebasable		
	<Constructor>	Public	✓	Ownable Rebasable
	totalSupply	Public		-
	getSellBurn	Public		-
	getTxBurn	Public		-
	_isWhitelisted	Internal		
	_isPancakePairAddress	Internal		
	setWhitelistedTo	External	✓	onlyOwner
	setCFee	External	✓	onlyOwner
	setBFee	External	✓	onlyOwner
	setTxFee	External	✓	onlyOwner
	setFYFee	External	✓	onlyOwner
	setSellFee	External	✓	onlyOwner
	setBurnTop	External	✓	onlyOwner
	setBurnBottom	External	✓	onlyOwner
	setWhitelistedFrom	External	✓	onlyOwner
	setPancakePairAddress	External	✓	onlyOwner
	addfuturePool	External	✓	onlyOwner
	maxScalingFactor	External		-
	_maxScalingFactor	Internal		
	transfer	Public	✓	-
	transferFrom	Public	✓	-
	balanceOf	Public		-
	balanceOfUnderlying	External		-
	allowance	External		-
	approve	Public	✓	-

	increaseAllowance	External	✓	-
	decreaseAllowance	External	✓	-
	_approve	Private	✓	
	isExcluded	Public		-
	totalFees	Public		-
	reflect	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeAccount	External	✓	onlyOwner
	includeAccount	External	✓	onlyOwner
	_transfer	Private	✓	
	<Receive Ether>	External	Payable	-
	swapAndLiquifyForETH	Private	✓	lockTheSwap
	swapTokensForETH	Private	✓	
	addLiquidityForETH	Private	✓	
	_transferStandard	Private	✓	
	_transferStandardSell	Private	✓	
	_transferStandardTx	Private	✓	
	_transferToExcluded	Private	✓	
	_transferToExcludedSell	Private	✓	
	_transferToExcludedTx	Private	✓	
	_transferFromExcluded	Private	✓	
	_transferFromExcludedSell	Private	✓	
	_transferFromExcludedTx	Private	✓	
	_transferBothExcluded	Private	✓	
	_transferBothExcludedSell	Private	✓	
	_transferBothExcludedTx	Private	✓	
	_scaling	Private		
	_reflectFee	Private	✓	
	_getTValues	Private		
	_getTValues2	Private		
	_getRValues	Private		
	_getRValues2	Private		
	_getRate	Private		
	_getCurrentSupply	Private		

	_setBreedAddress	External	✓	onlyOwner
	_setCharityAddress	External	✓	onlyOwner
	rebase	External	✓	onlyRebaser
	getCurrentPoolAddress	Public		-
	getCurrentPairTokenAddress	Public		-
	_setMaxTxAmount	External	✓	onlyOwner
	_setMinTokensBeforeSwap	External	✓	onlyOwner
	_setAutoSwapCallerFee	External	✓	onlyOwner
	updateSwapAndLiquifyEnabled	Public	✓	onlyOwner
	_enableTrading	External	✓	onlyOwner
Ownable	Implementation	Context		
	<Constructor>	Internal	✓	
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
Rebasable	Implementation	Ownable		
	<Constructor>	Internal	✓	
	Rebaser	Public		-
	transferRebasership	Public	✓	onlyOwner
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
	ceil	Internal		
	divRound	Internal		

Contract Flow



Domain Info

Domain Name	doggyrebase.co.in
Registry Domain ID	D5EE6757717ED4214BAF0A9C5EA06159E-IN
Creation Date	2021-12-14T13:37:43Z
Updated Date	2021-12-19T13:37:44Z
Registry Expiry Date	2022-12-14T13:37:43Z
Registrar WHOIS Server	
Registrar URL	www.openprovider.com
Registrar	Hosting Concepts B.V. d/b/a Openprovider
Registrar IANA ID	1647

The domain has been created 30 days before the creation of the audit. It will expire in 11 months.

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

Summary

Doggy Rebaser token is a decentralized synthetic rebase asset with built-in advanced financial tools. There are some functions that can be abused by the owner, like manipulating fees and indirectly stopping the transaction. The contract contains a total supply manipulation mechanism. This is a powerful functionality but the contract owner should carefully manage the adjustment of the circulating supply. 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