RugFreeCoins Audit

Decom Credit Token

Smart Contract Security Audit

April 09, 2022

Contents

Audit details

Audited project
Decom Credit Token

Contract Address
0xDCbd5274cAdBeE2Fce708B9787dBa1010A342e2E

Client contact
Decom Token Team

Blockchain
Binance smart chain

Project website
https://decomlabs.org/

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 the Decom Team to perform an audit of the smart contract.

https://bscscan.com/token/0xDCbd5274cAdBeE2Fce708B9787dBa1010A342e2E

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 improving the security posture of the smart contract by remediating the issues that were identified.

About the project

Decom is a token built on the Binance Smart Chain that is with an innovative investment use case the main purpose of which is to seek out constant revenue sources, and heading towards building even greater Community, building a large-scale SaaS platform for providing marketing services with trustless peer-to-peer transactions based on escrow deals and feedback system. Each transaction, purchase and sell incur 6% fee.

Features

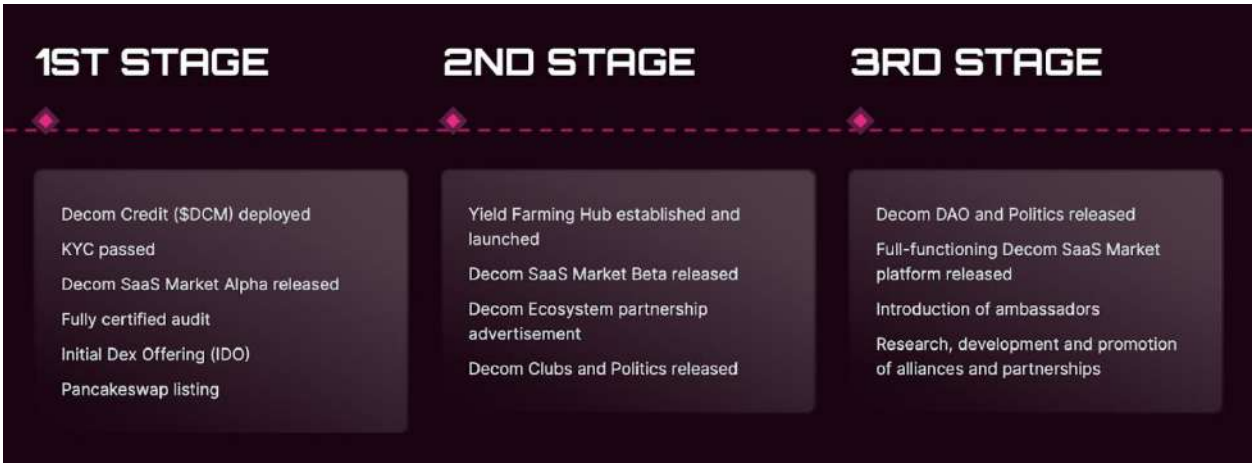
- The **sustainability fee of 4% when buying and selling for dev a** is what allows Decom token to hold the aforementioned promise. Tokens will be swapped into BNB and will be sent to a dev wallet per transaction. This way, Decom token will have enough funds to promote the coin and spend for future development without selling tokens as the traditional way.

- The additional component included under the sustainability section is a **liquidity fee of 2% when buying and selling**, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity.

- The vision is focus toward Decentralized Marketing in the crypto space, where buyers and sellers should be able to conduct secure and fair deals, independent of third parties, and minimize mark-ups on services by eliminating or reducing the number of intermediaries.

- Enables marketing agents to provide their services on Decom Market with minimal verification to prevent the sale of illegal items or services and allows customers to shop for marketing items with a decentralized wallet. Decentralized marketing platform Decom Market also offers decentralized financial functions such as yield farm and pool.

Roadmap


1ST STAGE
Decom Credit ($DCM) deployed
KYC passed
Decom SaaS Market Alpha released
Fully certified audit
Initial Dex Offering (IDO)
Pancakeswap listing
2ND STAGE
Yield Farming Hub established and launched
Decom SaaS Market Beta released
Decom Ecosystem partnership advertisement
Decom Clubs and Politics released
3RD STAGE
Decom DAO and Politics released
Full-functioning Decom SaaS Market platform released
Introduction of ambassadors
Research, development and promotion of alliances and partnerships

Tokenomics

6% fee when buying & selling

- 4% of trade goes to the marketing wallet in BNB
- 2% of trade goes to the liquidity pool.

Target market and the concept

Target market

- Anyone who's interested in the 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 taking part with farming.
- Anyone who's ready to take part with Decom marketing services.
- Anyone who's ready to take part with Decom escrow deals and feedback system.
- Anyone who's interested in taking part with the future plans of the Decom Token Ecosystem.
- Anyone who's interested in making financial transactions with any other party using Decom as the currency.

Core concept

Sustainable mechanism

The **sustainability fee of 4% when buying and selling for dev** is what allows Decom to promote the token and use funds to further the development of the platform. Tokens will be swapped into BNB and will be sent to a dev wallet. This way, Decom will have access to the funds without selling tokens as the traditional way, which will enable them to consume funds without hurting the project.

The liquidity fee of 2% when buying and selling, which is a redistribution mechanism that ensures the trading pool always has sufficient liquidity.

Submit offers

You can submit and find any marketing offer on the Decom Market, select the parameters and find the right agent.

Find an agent

Scalable options and a list of marketing services, collaboration and profitable deals without intermediaries - all in the decentralised Decom SaaS platform.

Communicate

Hitting someone up was never so easy. Use integrated chats to pop up in the visible area of your wished marketing agent.

Feedback System

Profiles on Decom Market are rated, with an integrated feedback system, after each deal the platform will offer to rate the marketer.

Governance

Decom Credit ($DCM) will integrate the DAO Governance protocol, all holders will be offered voting pools to further develop the Decom Ecosystem.

Earn Cashback

$DCM serves as access to the Decom Market, with which you can pay for a monthly subscription and receive cashback on deals completed.

Potential to grow with score points

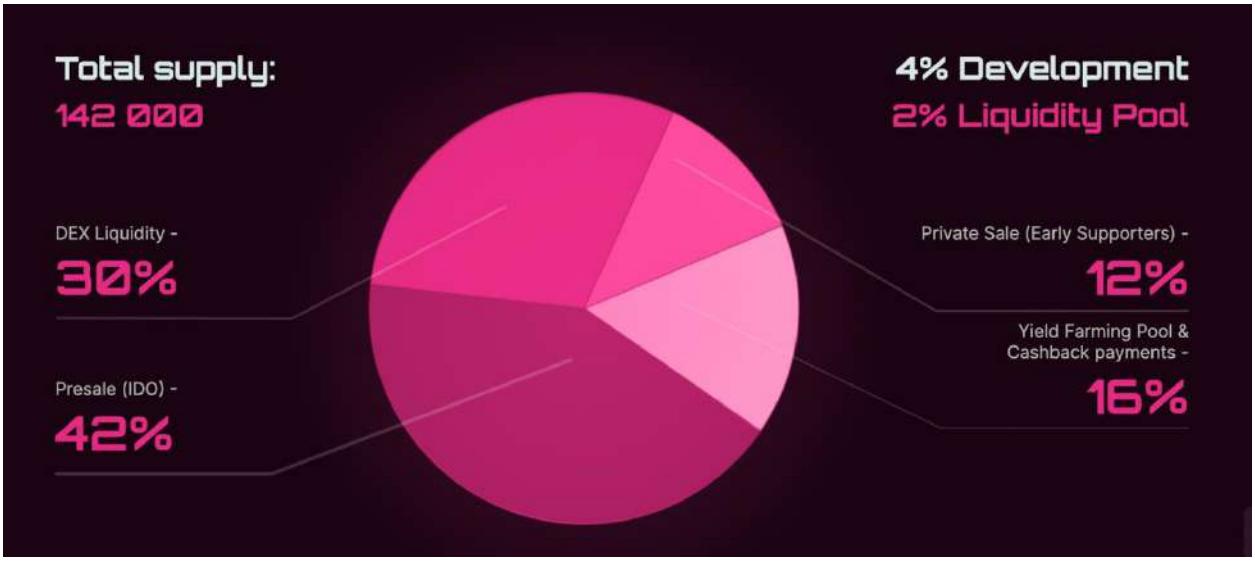
1.	Project efficiency	9/10
2.	Project uniqueness	9/10
3	Information quality	9/10
4	Service quality	9/10
5	System quality	9/10
6	Impact on the community	9/10
7	Impact on the business	9/10
8	Preparing for the future	9/10
Total Points		**9/10**

Contract details

Token contract details for 9th April 2022

Contract name	Decom Credit
Contract address	0xDCbd5274cAdBeE2Fce708B9787dBa1010A342e2E
Token supply	142,000
Token ticker	DCM
Decimals	9
Token holders	1
Transaction count	1
Development wallet address	0x3cbf6fcb57e87cecfeea0e1525a72e81b0451b15
Contract deployer address	0xd08EA382C095479aBb1ffe2709744Fd1562f13e5
Contract's current owner address	0x6743e0dbdb2ab1014044486f1fa4cb9a73ef2fbe

Token Distribution as follows:



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	High Centralisation Risk
		Business logics	Low issue
		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

The 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 their visibility and mutability.

Contract	**Type**	**Bases**		
L	Function Name	Visibility	Mutability	Modifiers
IUniswapV2 Factory	**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❗
IUniswapV2 Router01	**Interface**			
L	factory	External ❗		NO❗
L	WETH	External ❗		NO❗
L	addLiquidity	External ❗	🛑	NO❗
L	addLiquidityETH	External ❗	💵	NO❗

└	removeLiquidity	External ❗	🛑	NO❗
└	removeLiquidityETH	External ❗	🛑	NO❗
└	removeLiquidityWithPermit	External ❗	🛑	NO❗
└	removeLiquidityETHWithPermit	External ❗	🛑	NO❗
└	swapExactTokensForTokens	External ❗	🛑	NO❗
└	swapTokensForExactTokens	External ❗	🛑	NO❗
└	swapExactETHForTokens	External ❗	💵	NO❗
└	swapTokensForExactETH	External ❗	🛑	NO❗
└	swapExactTokensForETH	External ❗	🛑	NO❗
└	swapETHForExactTokens	External ❗	💵	NO❗
└	quote	External ❗		NO❗
└	getAmountOut	External ❗		NO❗
└	getAmountIn	External ❗		NO❗
└	getAmountsOut	External ❗		NO❗
└	getAmountsIn	External ❗		NO❗
IUniswapV2 Router02	**Interface**	**IUniswapV 2 Router01**		
└	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO❗

L	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO❗
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
SafeMath	**Library**			
L	tryAdd	Internal 🔒		
L	trySub	Internal 🔒		
L	tryMul	Internal 🔒		
L	tryDiv	Internal 🔒		
L	tryMod	Internal 🔒		
L	add	Internal 🔒		
L	sub	Internal 🔒		
L	mul	Internal 🔒		
L	div	Internal 🔒		
L	mod	Internal 🔒		
L	sub	Internal 🔒		
L	div	Internal 🔒		
L	mod	Internal 🔒		
IERC20	**Interface**			
L	totalSupply	External ❗		NO❗
L	balanceOf	External ❗		NO❗

└	transfer	External ❗	🛑	NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
Context	**Implementation**			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	**Implementation**	**Context**		
└		Public ❗	🛑	NO❗
└	owner	Public ❗		NO❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_transferOwnership	Internal 🔒	🛑	
DCM	**Implementation**	**IERC20, Ownable**		
└		Public ❗	🛑	NO❗
└		External ❗	💵	NO❗
└	totalSupply	External ❗		NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗

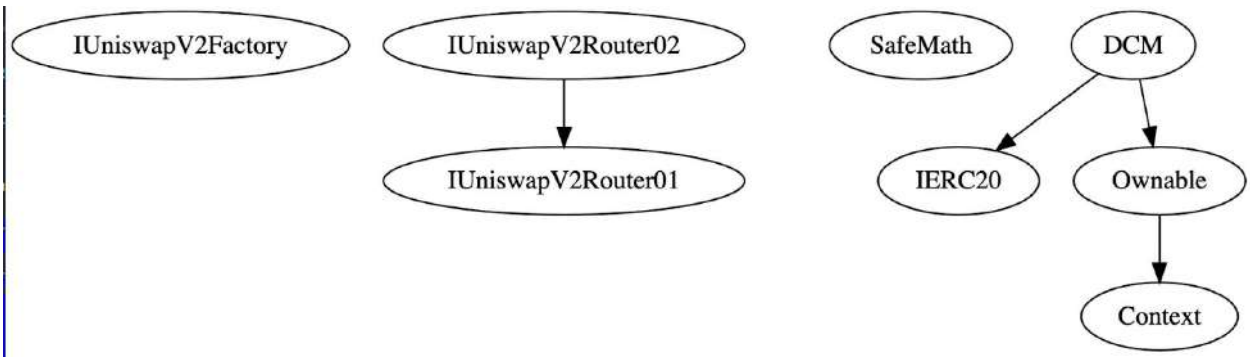
└	decimals	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	allowance	External ❗		NO❗
└	approve	Public ❗	🛑	NO❗
└	_approve	Internal 🔒	🛑	
└	approveMax	External ❗	🛑	NO❗
└	transfer	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
└	_transferFrom	Internal 🔒	🛑	
└	_basicTransfer	Internal 🔒	🛑	
└	shouldTakeFee	Internal 🔒		
└	takeFee	Internal 🔒	🛑	
└	shouldSwapBack	Internal 🔒		
└	clearStuckBalance	External ❗	🛑	onlyOwner
└	updateBuyFees	Public ❗	🛑	onlyOwner
└	updateSellFees	Public ❗	🛑	onlyOwner
└	updateSwapPercentages	Public ❗	🛑	onlyOwner
└	tradingStatus	Public ❗	🛑	onlyOwner
└	whitelistPreSale	Public ❗	🛑	onlyOwner
└	swapBackInBnb	Internal 🔒	🛑	swapping
└	swapAndLiquify	Private 🔐	🛑	

└	swapTokensForEth	Private		
└	addLiquidity	Private		
└	setIsFeeExempt	External		onlyOwner
└	setFeeReceivers	External		onlyOwner
└	setSwapBackSettings	External		onlyOwner

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**

No low severity issues found

- **Centralization risk**

High severity centralization risk

❖ The owner can change all buy and sell fees without any maximum limit (can set 100%)

```
ftrace | funcSig
function updateBuyFees(uint256 dev⬆, uint256 liquidity⬆) public onlyOwner {
    buyDevFee = dev⬆;
    buyLiquidityFee = liquidity⬆;
    buyTotalFees = dev⬆.add(liquidity⬆);
}

ftrace | funcSig
function updateSellFees(uint256 dev⬆, uint256 liquidity⬆) public onlyOwner {
    selDevFee = dev⬆;
    sellLiquidityFee = liquidity⬆;
    sellTotalFees = dev⬆.add(liquidity⬆);
}
```

❖ The owner can enable/disable trading anytime

```
ftrace | funcSig
function tradingStatus(bool _status⬆) public onlyOwner {
    tradingOpen = _status⬆;
}
```

Owner privileges

- The owner can get contract bnb balance to owner wallet

```
ftrace | funcSig
function clearStuckBalance(uint256 amountPercentage⬆) external onlyOwner {
    uint256 amountBNB = address(this).balance;
    payable(msg.sender).transfer((amountBNB * amountPercentage⬆) / 100);
}
```

- The owner can change all buy and sell fees

```
ftrace | funcSig
function updateBuyFees(uint256 dev⬆, uint256 liquidity⬆) public onlyOwner {
    buyDevFee = dev⬆;
    buyLiquidityFee = liquidity⬆;
    buyTotalFees = dev⬆.add(liquidity⬆);
}

ftrace | funcSig
function updateSellFees(uint256 dev⬆, uint256 liquidity⬆) public onlyOwner {
    selDevFee = dev⬆;
    sellLiquidityFee = liquidity⬆;
    sellTotalFees = dev⬆.add(liquidity⬆);
}
```

- The owner can change swap percentages

```
ftrace | funcSig
function updateSwapPercentages(uint256 dev⬆, uint256 liquidity⬆)
    public
    onlyOwner
{
    devSwap = dev⬆;
    liquiditySwap = liquidity⬆;
    totalSwap = dev⬆.add(liquidity⬆);
}
```

❖ The owner can enable/disable trading

```
ftrace | funcSig
function tradingStatus(bool _status) public onlyOwner {
    tradingOpen = _status;
}
```

❖ The owner can whitelist address

```
ftrace | funcSig
function whitelistPreSale(address _preSale) public onlyOwner {
    isFeeExempt[_preSale] = true;
    isAuthorized[_preSale] = true;
}
```

❖ The owner can include/exclude wallets from fees

```
ftrace | funcSig
function setIsFeeExempt(address holder, bool exempt) external onlyOwner {
    isFeeExempt[holder] = exempt;
}
```

❖ The owner can change dev wallet address

```
ftrace | funcSig
function setFeeReceivers(address _wallet) external onlyOwner {
    devFeeReceiver = _wallet;
}
```

❖ The owner can enable/disable swapping and can change swap point

```
ftrace | funcSig
function setSwapBackSettings(bool _enabled⬆, uint256 _amount⬆)
    external
    onlyOwner
{
    swapEnabled = _enabled⬆;
    swapThreshold = _amount⬆;
}
```

Audit conclusion

RugFreeCoins team has performed in-depth testings, line by line manual code review, and automated audit of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, manipulations, and hacks. According to the smart contract audit.

Smart contract functional Status: **PASSED**

Number of risk issues: **2**

Solidity code functional issue level: **PASSED**

Number of owner privileges: **8**

Centralization risk correlated to the active owner: **HIGH**

Smart contract active ownership: **YES**