



RugFreeCoins Audit



MovingOn Finance

Smart Contract Security Audit

May 05, 2022

Contents

Audit details	1
Disclaimer	2
Background	3
About the project	4
Target market and the concept	8
Potential to grow with score points	13
Total Points	13
Contract details	14
Contract code function details	15
Contract description table	17
Security issue checking status	25
Owner privileges	26
Audit conclusion	28

Audit details



Audited project
MovingOn Finance Token



Contract Address
0xc4901c34cd8FB49107c1CB874EfF5cAA2eAeD7d1



Client contact
MovingOn Finance Team



Blockchain
Binance smart chain



Project website
<https://www.movingon.finance/>

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 MovingOn Finance Team to perform an audit of the smart contract.

<https://bscscan.com/token/0xc4901c34cd8fb49107c1cb874eff5caa2eaed7d1>

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

MovingOn Finance 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, it is a method of health training, based on that, users can earn corresponding profits. That is the contemporary trend --> **Move-To-Earn**. Users can own their favorite NFTs to do move outdoors to earn profits with MOVON tokens. Each transaction, purchase incurs 1% fee, and sale incurs a 15% fee.

Features

- The **sustainability fee of 1% when buying and 10% when selling for marketing and reward pool** is what allows MovingOn Finance to hold the aforementioned promise. Tokens will be swapped into BNB and will be sent to a marketing wallet. This way, MovingOn Finance 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 **5% when selling**, which is allocated for staking pool.

Roadmap

Start-UP

- Connect ideas
- Set up business model

Phase 1

- Documents
- Application design
- Website
- Social network connection

Phase 2

- Data Deployment
- Build MOVON application
- Deploy smart contracts
- Audit
- Integration test: Uber, Lyft, Grab, Didi, Ola

Phase 3

- Marketing plans
- Airdrop campaign
- Support partner
- Influencers
- Fairlaunch on Pinksale

Phase 4

- Listing PancakeSwap
- Listing CMC/CGK
- NFT implementation
- Technology partner
- Internal Testing

Phase 5

- Launch and integrate NFT
- GPS Integration
- Public Testing
- Fix bugs
- Launch app beta

Phase 6

- CEX listing
- Marketing
- Official launch - MOVON app
- Review on Appstore and GooglePlay
- Achievement Ranking

Phase 7

- Cross-chain implementation
- Multi-chain partner
- Physical product development
- Product copyright

Tokenomics

1% fee when buying

- 1% of trade goes to the marketing wallet in BNB.

15% fee when buying

- 10% of trade goes to the marketing wallet in BNB.
- 5% of trade goes to the staking wallet in tokens.

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 collecting NFTs or trading NFTs.
- Anyone who's interested in taking part with staking.
- Anyone who's interested in exercise and get rewards through activities: Walking, Running and Cycling.
- Anyone who own transport vehicles such as motorbikes and cars can participate in Drive activities to receive rewards
- Anyone who's interested in taking part with the future plans of the MovingOn Finance Token Ecosystem.
- Anyone who's interested in making financial transactions with any other party using MovingOn Finance as the currency.

Core concept

Sustainable mechanism

The sustainability fee of 1% when buying and 10% when selling for marketing and rewards pool is what allows MovingOn Finance 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 marketing wallet. This way, MovingOn Finance will have access to the funds without selling tokens as the traditional way, which will enable them to consume funds without hurting the project.

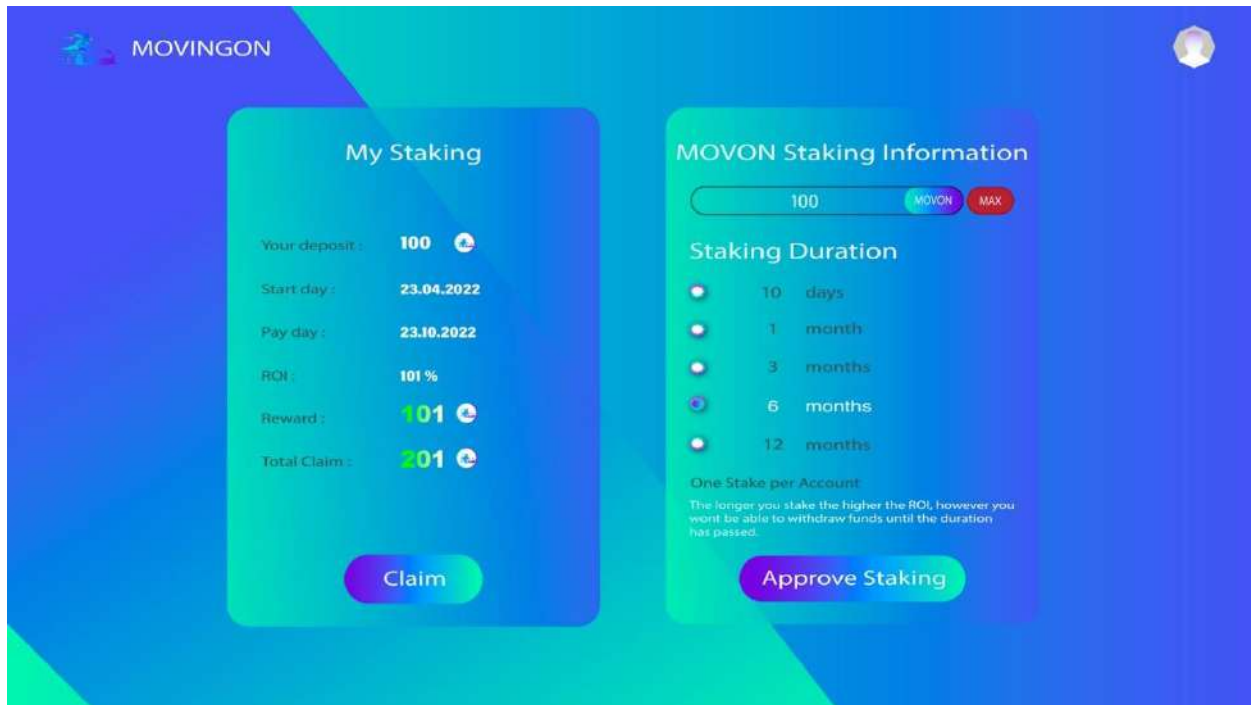
Staking mechanism

In addition to the Move-To-Earn mechanism, MovingOn Finance will implement a Staking product so that MOVON token holders can earn passive profits. Staking is essential to maintaining a safe and healthy network.

- MOVON token holders can option for staking packages (10 days, 1 month, 3 months, 6 months, 1 year). Fixed interest rate for each package
- The longer you save the higher the ROI, however you won't be able to withdraw funds until the duration has passed
- One Save per Wallet

Staking rewards distribution includes:

- 21% of the total supply will be distributed to Staking in 25 months
- 5% of each Sell transaction on PancakeSwap will be transferred to the Staking address as a reward.
- 2.5% of each transaction on Marketplace will be transferred to the Staking address as a reward.



The MOVON application

The MOVON application is divided into two main groups of activities:

Move-To-Earn: Users can exercise and get rewards through activities: Walking, Running, and Cycling. The application uses GPS - Global Positioning System and combines with other devices such as smartwatches to measure distance, calories, and heart rate,...

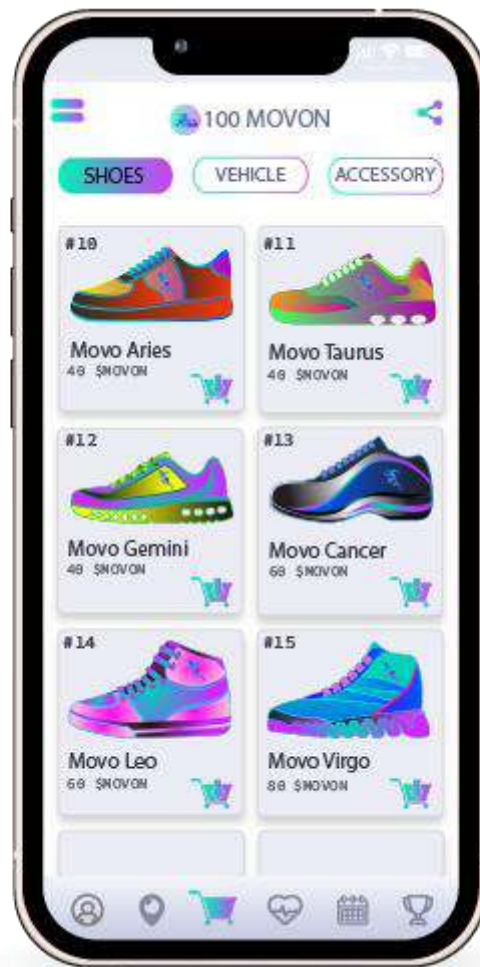
Drive-To-Earn: Users who own transport vehicles such as motorbikes and cars can participate in Drive activities to receive rewards. This activity is very suitable for technology taxi drivers (Uber, Lyft, Grab, Didi, Ola,...). The application uses GPS - Global Positioning System and other anti-cheat devices to measure the distance.



NFTs

These are tokens that have been designed to be unique. They are used to identify a specific owner. Once you own the NFT, you can then use it or sell it as you please. You could set any price you want on the [Marketplace](#).

Shoes



Vehicle



Potential to grow with score points

1.	Project efficiency	9/10
2.	Project uniqueness	10/10
3	Information quality	10/10
4	Service quality	9/10
5	System quality	9/10
6	Impact on the community	10/10
7	Impact on the business	9/10
8	Preparing for the future	10/10
9	Smart contract security	10/10
10	Smart contract functionality assessment	10/10
Total Points		9.6/10

Contract details

Token contract details for 5th May 2022

Contract name	MovingOn Finance
Contract address	0xc4901c34cd8FB49107c1CB874EfF5cAA2eAeD7d1
Token supply	100,000,000
Token ticker	MOVON
Decimals	18
Token holders	2
Transaction count	6
Treasury address	0x1b51122c0740c55206be4b3413cdb44156c79488
Staking address	0x1529e3b77da40531a05ca186ceed1b2f6a3e1ba2
Contract deployer address	0x7F87c1C5e3d0Ace34CBD23D5eDff04Ebb3bED989
Contract's current owner address	0x00














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
		Self-destruct 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











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
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!
L	transfer	External !		NO!
L	allowance	External !		NO!
L	approve	External !		NO!
L	transferFrom	External !		NO!
Context	Implementation			
L	_msgSender	Internal 		
L	_msgData	Internal 		
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!
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	swapExactTokensForETH	External !		NO!
L	swapETHForExactTokens	External !		NO!
L	quote	External !		NO!
L	getAmountOut	External !		NO!
L	getAmountIn	External !		NO!
L	getAmountsOut	External !		NO!
L	getAmountsIn	External !		NO!



IUniswapV2 Router02	Interface	IUniswap V2 Router01		
L	removeLiquidityETHSupportingFeeOnTransferTokens	External !		NO!
L	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External !		NO!
L	swapExactTokensForTokensSupportingFeeOnTransferTokens	External !		NO!
L	swapExactETHForTokensSupportingFeeOnTransferTokens	External !		NO!
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External !		NO!
IUniswapV2 Pair	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!
Ownable	Implementation	Context		
L		Public !		NO!
L	owner	Public !		NO!
L	renounceOwnership	Public !		onlyOwner
L	transferOwnership	Public !		onlyOwner

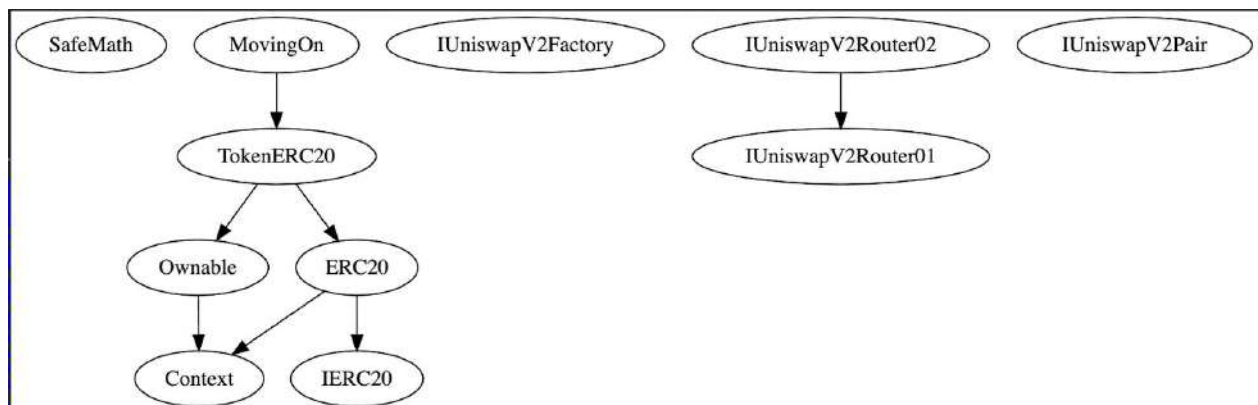
ERC20	Implementation	Context, IERC20		
L		Public !		NO!
L	name	Public !		NO!
L	symbol	Public !		NO!
L	decimals	Public !		NO!
L	totalSupply	Public !		NO!
L	balanceOf	Public !		NO!
L	transfer	Public !		NO!
L	allowance	Public !		NO!
L	approve	Public !		NO!
L	transferFrom	Public !		NO!
L	increaseAllowance	Public !		NO!
L	decreaseAllowance	Public !		NO!
L	_transfer	Internal 		
L	_mint	Internal 		
L	_burn	Internal 		
L	_approve	Internal 		
L	_setupDecimals	Internal 		
L	_beforeTokenTransfer	Internal 		

TokenERC20	Implementation	Ownable, ERC20		
L		Public !		ERC20 Ownable
L	setAntiWhaleAmount	Public !		onlyTreasury
L	isAntiWhaleEnded	Public !		NO!
L	setStakingAddress	External !		onlyTreasury
L	setTransferFeeRate	Public !		onlyTreasury
L	setPresaleAddress	Public !		onlyTreasury
L	sweepBNB	Public !		onlyTreasury
L	sweepToken	Public !		onlyTreasury
MovingOn	Implementation	TokenERC20		
L		Public !		TokenERC20
L	burn	Public !		NO!
L	_transfer	Internal 		
L	shouldSwapBack	Internal 		
L	swapBack	Internal 		swapping
L	swapTokensForEth	Private 		
L	shouldTakeFee	Internal 		
L	takeFee	Internal 		swapping
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

No low severity issues found

❖ Centralization risk

No Centralization issues found

Owner privileges

- ❖ The owner can enable antiwhale system (Once it's enabled it will end after 15 min) the owner can enable it only one time

```
ftrace | funcSig
function setAntiWhaleAmount(uint256 _amount↑) public onlyTreasury {
    // set anti whale amount also activate antibot
    require(antiWhaleAmount == 0, "Can active antiWhale once"); // antiWhale can only activate once
    antiWhaleAmount = _amount↑;
    antiWhaleStartTime = block.timestamp - 10; // safty margin 10s
}
```

- ❖ The owner can change staking address

```
ftrace | funcSig
function setStakingAddress(address _stakingAddress↑) external onlyTreasury {
    stakingAddress = _stakingAddress↑;
}
```

- ❖ The owner can change buy fees maximum up to 1% and sell fees maximum up to 15%

```
ftrace | funcSig
function setTransferFeeRate(
    uint256 _buyFeeRate↑,
    uint256 _treasuryAndMarketingFeeRate↑,
    uint256 _stakeFeeRate↑
) public onlyTreasury {
    require(_buyFeeRate↑ <= 1, "BUY_FEE_RATE_NO_HIGHER_THAN_1_PERCENT");
    require(
        _stakeFeeRate↑ + _treasuryAndMarketingFeeRate↑ <= 15,
        "SELL_FEE_RATE_NO_HIGHER_THAN_15_PERCENT"
    );
    buyFeeRate = _buyFeeRate↑;
    treasuryAndMarketingFee = _treasuryAndMarketingFeeRate↑;
    stakingFee = _stakeFeeRate↑;
}
```


- ❖ The owner can add multiple presale addresses

```
ftrace | funcSig
function setPresaleAddress(address _presaleAddress↑) public onlyTreasury {
    presaleAddress[_presaleAddress↑] = true;
}
```

- ❖ The owner can get BNB and other BEP20 tokens in the contract

```
ftrace | funcSig
function sweepBNB(address _to↑) public onlyTreasury {
    payable(_to↑).transfer(address(this).balance);
}

ftrace | funcSig
function sweepToken(address _token↑, address _to↑) public onlyTreasury {
    IERC20(_token↑).transfer(_to↑, IERC20(_token↑).balanceOf(address(this)));
}
```

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: **NONE**

Solidity code functional issue level: **PASSED**

Number of owner privileges: **5**

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

Smart contract active ownership: **YES**