



SMART CONTRACT SECURITY AUDIT

WATCHTOWER

AUDIT DETAILS



Project Name

Carrot Cake Bake



Contract address

0xc65465f871f7d106c8cecff6840a33ec949bb780



Deployer Address:

0xb9cf64f3871366eb3B2875d3c0C21B0D288c413F



Blockchain

Binance Smart Chain



Project website:

<https://carrotcakefinance.com/>



DISCLAIMER

Watchtower has completed this report to provide a summary of the Smart Contract functions, and any security, dependency or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as at the date of this report. In order to understand the full scope of our analysis, it is vital for you to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against Watchtower or its Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your own independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

DISCLAIMER: By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any and all duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise, and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and Watchtower and its members (including holding companies, shareholders, backups, representatives, chiefs, officers and other agents) Watchtower and its subsidiaries owe no obligation of care towards you or any other person, nor does Watchtower make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:

Watchtower is an Anti-Scam Token Utility which reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity.

Watchtowers Development Team consists of a number of Smart Contract creators, Auditors Developers and Blockchain experts.

Watchtowers Website Scanner reviews a number of Risk factors to provide an adequate Risk summary of token projects.

In Addition to this the team also helps with Creation of Smart Contracts for legitimate projects, Audits and Promotion.





OVERVIEW

Watchtower was commissioned by Carrot Cake Bake to complete a Smart Contract audit.

The objective of the Audit is to achieve the following:

- Ensure that the Smart Contract functions are necessary and operate as intended.
- Identify any vulnerabilities in the Smart Contract code.

DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or provide financial advice in any way,
All investments are made at your own risk.

(<https://www.cryptowatchtower.io/>)



SMART CONTRACT REVIEW



Contract Created on 08.20.2021

Contract name	CARROT CAKE BAKE
Contract address	0xc65465f871f7d106c8cecff6840a33ec949bb780
Total supply	100,000,000,000
Token ticker	CCB
Decimals	18
Token holders	69
Transactions count	1609
Top 5 holders dominance	23.8% Includes 5% marketing wallet
Tax fee	15%
Total fees	15%
Contract deployer address	0xb9cf64f3871366eb3B2875d3c0C21B0D288c413F
Contract's current owner address	0xb9cf64f3871366eb3B2875d3c0C21B0D288c413F



CONTRACT FUNCTIONS DETAILS

FUNCTIONS (PUBLIC)

1. Approve spender
2. Blacklist
3. Claim
4. Decrease allowance
5. Exclude from Dividends
6. Exclude from fees
7. Exclude multiple accounts from fees
8. Increase Allowance
9. Process Dividend tracker
10. Renounce ownership
11. Set automated Market Maker Pair
12. Set CAKE rewards Fee
13. Set Liquidity Fee
14. Set Marketing Fee
15. Set Marketing wallet
16. Transfer to
17. Transfer from
18. Transfer Ownership
19. Update Claim Wait
20. Update Dividend Tracker
21. Update Gas for Processing
22. Update Uniswap V2 Router



Function Risks

Upon review of Smart Contract Coding and Functions available for the Owner to change Watchtower is satisfied that no malicious coding has been found, The Functions and fees in our review from the time of launch til present, (approx 1 month) conveys genuine and legitimate operations.

Note: Rewards contracts generally allow the owner to change tax fees and as a result they can increase the fees to a higher amount, making it difficult to sell.

Watchtowers review found that the Owner has been genuine in operating the smart contract functions by excluding the dev and locked wallets from rewards.

Liquidity Lock proof was provided however the Top 5 Wallets hold 23% of tokens which is classified as a Price Impact Risk which has been explained to the team for them to address. Watchtower is satisfied the contract functions are operating as intended with genuine intentions.



Imported Libraries / Interfaces

- Context
- Ownable
- IERC20
- IERC20 Metadata
- DividendPayingTokenOptionalInterface
- DividendPayingTokenInterface
- SafeMathInt
- SafeMathUint
- SafeMath
- ERC20
- DividendPayingToken
- IUniswapV2Router01
- IUniswapV2Router02
- IUniswapV2Factory
- IUniswapV2Pair

Overview

1. ADDITION OF COMMENTS:	10
2. CALL STACK DEPTH ATTACK:	10
3. TIME STAMP DEPENDENCY:	10
4. PARTY MULTISIG BUG:	10
5. USE OF LIBRARIES/DEPENDENCIES (FROM TRUSTED SOURCES):	10
a. TRANSACTION-ORDERING DEPENDENCY:	10
6. ACCESS CONTROL AND AUTHORIZATION:	9
7. REENTRANCY ATTACKS:	10
8. ERC/BEP STANDARD VIOLATIONS:	10
9. USAGE OF VISIBILITY LEVELS:	10



ISSUES CHECKING STATUS



Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Passed
10. Methods execution permissions.	Passed



Issue description	Checking status
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed



SECURITY ISSUES



High Severity Issues

No High Severity Issues found.



Medium Severity Issues

No Medium Severity issues found.



Low Severity Issues

No Low Severity issues found.



CONCLUSION

Watchtowers review of Carrot Cake Bake although Satisfactory did convey a concern around the Price Impact Risk of Top token holders.

The top 5 wallets hold 23% of Supply after Burn.

The Contract transfers, function behaviours and contract efficiency was analysed. Watchtower is satisfied there are no severity issues with the Contract.

Watchtower Disclaimer:

Please check the disclaimer page and note, this Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please do your own research. By reading this report you accept and agree to the disclaimer and understand investments are made at your own risk.

(<https://www.cryptowatchtower.io/>)

Contact Us

 @Watchtower_WTW

 Watchtower-WTW

 Watchtowercrypto

