# SMART CONTRACT SECURITY AUDIT

WATCHTOWER

# 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 it's 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 it's 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 Smash Cash to complete a Smart Contract audit.**
**The objective of the Audit is to achieve the following:**

- **Review the Project and experience and Development team**
- **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 the 12th November 2021** **Solidity compiler v0.8.10**

| | |
|---|---|
| Contract name | Smash Cash |
| Contract address | 0x3D0e93bfCb8FB46331Ea8c98B6ab8C575aB424C3 |
| Total supply | 1,000,000,000 |
| Token ticker | SMASH |
| Decimals | 18 |
| Token holders | 20 |
| Transactions count | 25 |
| Top 5 holders dominance | Not Launched |
| Tax fee | 0% |
| Total fees | 0% ~ BUY / 0% ~ SELL |
| Contract deployer address | 0x9259950b5C9Bc3f4bf95a04be5eB652DCFB8790C |
| Contract's current owner address | 0x9259950b5C9Bc3f4bf95a04be5eB652DCFB8790C |

# Project Overview

## Project Details: (Website: https://smashcash.io/)

Smash Cash ensures Transaction Anonymity and Privacy on 10 most popular Blockchains and support 15 Tokens by separating the on-chain link between destination and recipient addresses

## Tokenomics:

Supply: 1,000,000,000 (1 Billion)
**0% Tax for Buys and 0% for Sells:**

## Team Review:

Watchtower reviewed a number of factors including the teams background and Cryptocurrency experience, social media interaction and availability, project momentum, token risks and community trust score.
The Smash Cash team have a good understanding of Cryptocurrency.
Their website is professionally built and the proposed platform has real utility.

## TEAM DOXXED/KYC:

Watchtower is not aware of the team being doxxed nor have they been privately doxxed to Watchtower.

# CONTRACT FUNCTIONS DETAILS

## Functions (Public)

This contract has 24 available public functions which the owner can call.
They can be viewed on BSC Scan.

### LINK:

https://bscscan.com/token/0x3d0e93bfcb8fb46331ea8c98b6ab8c575ab424c3#writeContract

### Function risks:

-Although no scam functions have been identified, the functions available do allow the owners a high level of control over trading.

## Imported Libraries / Interfaces

- IBEP20
- IBEP20Metadata
- Context
- Ownable
- SafeMath
- Address
- IUniswapV2Factory
- IpancakePair
- IpancakeRouter01
- ipancakeRouter02

## Overview



# 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

**Centralisation Risk (Not expected to be called once the project is launched)**

1. The Owner can call EnableTrading() as many times as he wants. This will always update the _launchTime and restart the anti-sniper process. This means that users could be blacklisted.

## Medium Severity Issues

1. **tokenLockTime** is useless due to it can always be changed by the Owner however the team have shown that tokens have been lock using trust swap.
2. **LockToken** allows the Owner to take tokens from any address that is set as TeamTokenWallet (Must be set as the team token wallet and not suspected to be malicious but poses a risk).

## Low Severity Issues

**Centralisation Risk:**

1. The owners can set Max sell, Max buy and Max transaction to 0, pausing trading.
2. Line 908: Typo Error —> maxSellLimit instead of maxBuy

# CONCLUSION

**Watchtower reviewed the Smash Cash deployed and verified contract to conduct this audit.**
**Watchtower is satisfied that the Smash Cash team are operating with integrity and have discussed the issues raised in the Audit.**

***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**