



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 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 FOMO 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 16th January 2022 Solidity compiler v0.6.12

Contract name	FOMO
Contract address	0x1F508e77Cd0D30792a2cf1558da3d5aD382328A4
Total supply	1,000,000,000
Token ticker	FOMO
Decimals	18
Token holders	2569
Transactions count	7036
Top 5 holders dominance	26%
Tax fee	Dynamic Tax
Total fees	0% ~ BUY / 0 - 30% ~ SELL
Contract deployer address	0x1749d0ce2636a7666EcaDbe85b8d4CAd8F92a5d9
Contract's current owner address	0x1749d0ce2636a7666EcaDbe85b8d4CAd8F92a5d9



Project Overview



Project Details: (Website: <https://fomo-global.com/>)

\$FOMO is a new token made by \$CNPP team. \$CNPP was one of the first charity DAO's on The Binance Smart Chain.

\$FOMO's tokenomics tax will reduce when LP increases. This will encourage holders to hold \$FOMO to a higher level. And the holders can also get Bonuses from the prize pool.

Tokenomics:

Supply: 1,000,000,000 (1 Billion)

0% Tax for Buys and from 0-30% for Sells depending on liquidity pool balance:

Sell tax will reduce as LP increases

Lp 200k – sell tax 30%

Lp 300k – sell tax 20%

Lp 400k – sell tax 10%

Lp 500k – sell tax 5%

Sell tax will reduce to 0% when the Liquidity Pool Balance reaches \$1M

Sell Tax will begin as follows:

- 10% Marketing Fee
- 5% Bonus Pool
- 15% Burn.

Please check their website for updated tax fees.

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 FOMO team have a good understanding of Cryptocurrency and have been apart of previous projects which were successful. The social media following is strong and they have over 2500 users currently.

TEAM DOXXED/KYC:

Watchtower is not aware of the team being Doxxed or completing KYC at this point in time.

CONTRACT FUNCTIONS DETAILS

Functions (Public)

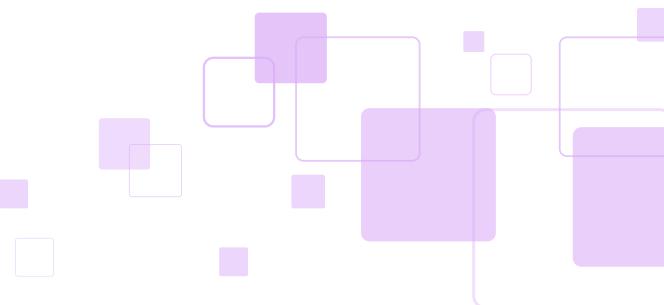
This contract has 23 available public functions which the owner can call. They can be viewed on BSC Scan once the contract is deployed.

LINK:

<https://bscscan.com/address/0x1f508e77cd0d30792a2cf1558da3d5ad382328a4#writeContract>

Function risks:

- swap() allows any user to get tokens and USDC from the contract, if isLocked is true
- Owner can burn tokens from any address



Contract Stress Test

Imported Libraries / Interfaces

- Ownable
- SafeMath
- IERC20
- ERC20
- Context
- IUniswapV2Factory
- IUniswapV2Pair
- IUniswapV2Router01
- IUniswapV2Router02

Overview

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



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

- swap() allows any user to get tokens and USDC from the contract, if isLocked is true

Centralization Risk:

- Owner can burn tokens from any address



Medium Severity Issues

Centralisation Risk

1. Owner can set fees to 100 and block any trade
2. Owner can blacklist the pair and block any trade
3. LP - tokens generated by liquidity fee are not locked. The owner could use them to remove liquidity.
4. Owner can set lunchTime to a future date, infinite times. This can cause users to get blacklisted



Low Severity Issues

- Fees declared as private.
- Contract has 2 methods of Burn:
 1. Send tokens to dead wallet and reduce circulating supply
 2. Burn tokens and reduce total supply
- Tokenomics have a tax fee range from 0-30%



CONCLUSION



Watchtower reviewed FOMO's Smart contract to conduct this audit.

Watchtower has noted the Libraries used and Smart contract vulnerabilities through the severity issues.

The Tokenomics of FOMO are unique and users should review them on their website.

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

