



Cyberscope

# Audit Report

## **FxRumble**

May 2023

Network    BSC

Address    0x7fDBcd8FFFBa514fcDD876354506dC9452f9b0e9

Audited by    © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Review</b>	<b>2</b>
Audit Updates	2
Source Files	2
<b>Findings Breakdown</b>	<b>3</b>
<b>Note</b>	<b>4</b>
<b>Analysis</b>	<b>5</b>
<b>Diagnostics</b>	<b>6</b>
RSML - Redundant SafeMath Library	7
Description	7
Recommendation	7
L09 - Dead Code Elimination	8
Description	8
Recommendation	8
L15 - Local Scope Variable Shadowing	10
Description	10
Recommendation	10
L19 - Stable Compiler Version	11
Description	11
Recommendation	11
<b>Functions Analysis</b>	<b>12</b>
<b>Inheritance Graph</b>	<b>15</b>
<b>Flow Graph</b>	<b>16</b>
<b>Summary</b>	<b>17</b>
<b>Disclaimer</b>	<b>18</b>
<b>About Cyberscope</b>	<b>19</b>

## Review

Contract Name	FXRUMBLE
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Explorer	<a href="https://bscscan.com/address/0x7fdbcd8ffba514fcdd876354506dc9452f9b0e9">https://bscscan.com/address/0x7fdbcd8ffba514fcdd876354506dc9452f9b0e9</a>
Address	0x7fdbcd8ffba514fcdd876354506dc9452f9b0e9
Network	BSC
Symbol	FXRUMBLE
Decimals	2
Total Supply	1.000.000.000

## Audit Updates

Initial Audit	03 May 2023
---------------	-------------

## Source Files

Filename	SHA256
FXRUMBLE.sol	51f7b8358cf865fcf21c02969156912b06f1db75aaad695a5ba4d09195765788

## Findings Breakdown



● Critical	0
● Medium	0
● Minor / Informative	4

Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	0	0	0	0
● Medium	0	0	0	0
● Minor / Informative	4	0	0	0

## Note

The contract uses 2 decimal points. This may produce precision issues if the initial price of the token is relatively high. For instance, if 1 \$FXRUMBLE is worth 1000 \$USDT, then the users will not be able to trade less than 10 \$USDT worth of \$FXRUMBLE. If a user tries to buy \$FXRUMBLE for 1 \$USDT, then he will receive 0 \$FXRUMBLE because of the decimals precision.

# Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

## Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	RSML	Redundant SafeMath Library	Unresolved
●	L09	Dead Code Elimination	Unresolved
●	L15	Local Scope Variable Shadowing	Unresolved
●	L19	Stable Compiler Version	Unresolved

## RSML - Redundant SafeMath Library

Criticality	Minor / Informative
Location	FXRUMBLE.sol
Status	Unresolved

### Description

SafeMath is a popular Solidity library that provides a set of functions for performing common arithmetic operations in a way that is resistant to integer overflows and underflows.

Starting with Solidity versions that are greater than or equal to 0.8.0, the arithmetic operations revert to underflow and overflow. As a result, the native functionality of the Solidity operations replaces the SafeMath library. Hence, the usage of the SafeMath library adds complexity, overhead and increases gas consumption unnecessarily.

```
library SafeMath {...}
```

### Recommendation

The team is advised to remove the SafeMath library. Since the version of the contract is greater than `0.8.0` then the pure Solidity arithmetic operations produce the same result.

If the previous functionality is required, then the contract could exploit the `unchecked { ... }` statement.

Read more about the breaking change on

<https://docs.soliditylang.org/en/v0.8.16/080-breaking-changes.html#solidity-v0-8-0-breaking-changes>.



## L09 - Dead Code Elimination

Criticality	Minor / Informative
Location	FXRUMBLE.sol#L208
Status	Unresolved

### Description

In Solidity, dead code is code that is written in the contract, but is never executed or reached during normal contract execution. Dead code can occur for a variety of reasons, such as:

- Conditional statements that are always false.
- Functions that are never called.
- Unreachable code (e.g., code that follows a return statement).

Dead code can make a contract more difficult to understand and maintain, and can also increase the size of the contract and the cost of deploying and interacting with it.

```
function _burn(address account, uint256 amount) internal
virtual {
    require(account != address(0), "BEP20: burn from the
zero address");
    _beforeTokenTransfer(account, address(0), amount);
    uint256 accountBalance = _balances[account];
    require(accountBalance >= amount, "BEP20: burn amount
exceeds balance");
    unchecked {
        _balances[account] = accountBalance.sub(amount);
    }
    emit Transfer(account, address(0), amount);
    _afterTokenTransfer(account, address(0), amount);
}
```

### Recommendation

To avoid creating dead code, it's important to carefully consider the logic and flow of the contract and to remove any code that is not needed or that is never executed. This can help improve the clarity and efficiency of the contract.

## L15 - Local Scope Variable Shadowing

<b>Criticality</b>	Minor / Informative
<b>Location</b>	FXRUMBLE.sol#L260
<b>Status</b>	Unresolved

### Description

Local scope variable shadowing occurs when a local variable with the same name as a variable in an outer scope is declared within a function or code block. When this happens, the local variable "shadows" the outer variable, meaning that it takes precedence over the outer variable within the scope in which it is declared.

```
uint256 totalSupply  
string memory symbol
```

### Recommendation

It's important to be aware of shadowing when working with local variables, as it can lead to confusion and unintended consequences if not used correctly. It's generally a good idea to choose unique names for local variables to avoid shadowing outer variables and causing confusion.

## L19 - Stable Compiler Version

<b>Criticality</b>	Minor / Informative
<b>Location</b>	FXRUMBLE.sol#L2
<b>Status</b>	Unresolved

### Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.8.0;
```

### Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

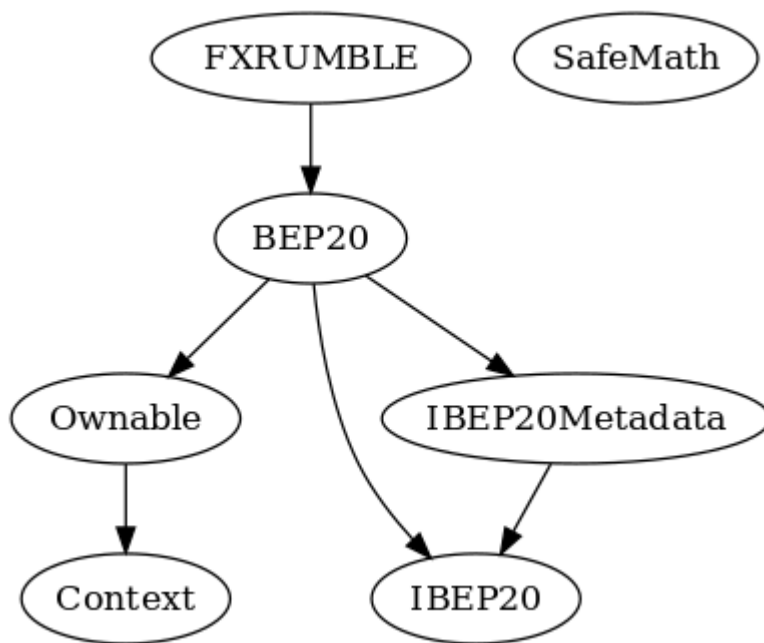
## Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>Ownable</b>	Implementation	Context		
		Public	✓	-
	owner	Public		-
	transferOwnership	Public	✓	onlyOwner
<b>IBEP20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>SafeMath</b>	Library			

	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
<b>IBEP20Metadata</b>	Interface	IBEP20		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>BEP20</b>	Implementation	Ownable, IBEP20, IBEP20Meta data		
		Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-

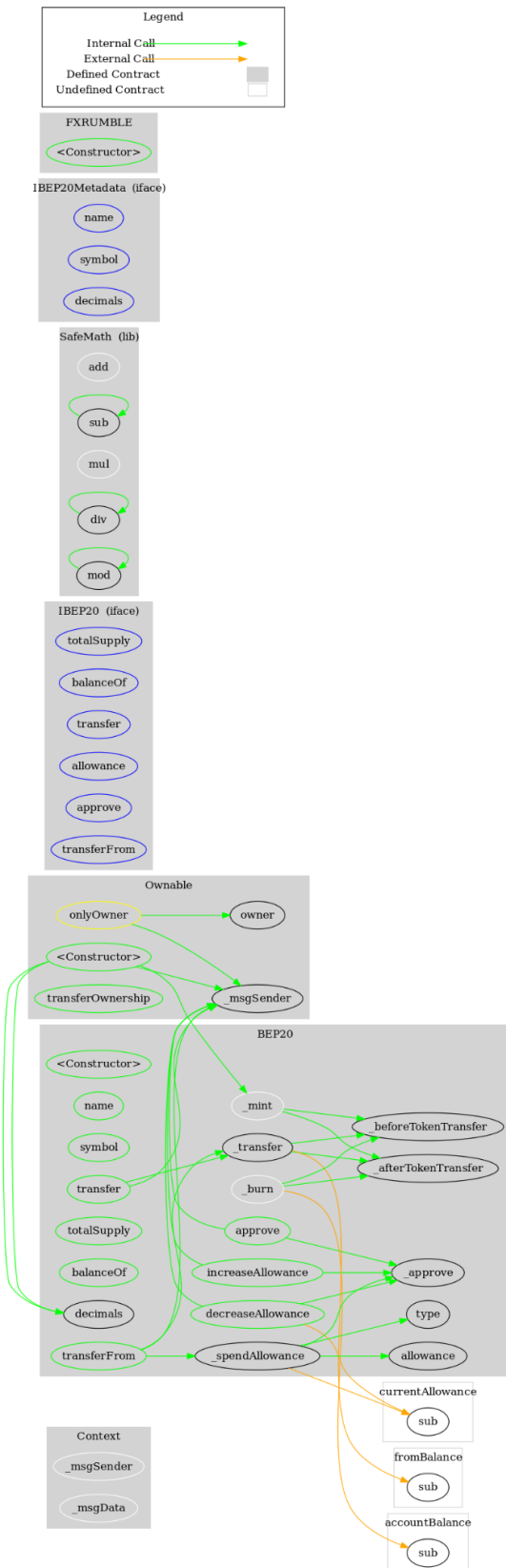
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
<b>FXRUMBLE</b>	Implementation	BEP20		
		Public	✓	BEP20

## Inheritance Graph





# Flow Graph



## Summary

FxBumble contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. FxBumble is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions.

## Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security. Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

## About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.



**The Cyberscope team**

<https://www.cyberscope.io>