Audit Report

TUMB

January 2022

Type	BEP20
Network	BSC
Address	0xA0C5E65bB1c07116E1b5d361d610a4C8709Bd58C
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	tumbToken
Compiler Version	v0.7.0+commit.9e61f92b
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xA0C5E65bB1c07116E1b5d361d610a4C8709Bd58C
Symbol	TMB
Decimals	9
Total Supply	500,000,000,000,000
Source	contract.sol
Domain	tumblermix.com

Audit Updates

Initial Audit	17th January 2022
Corrected	

Contract Analysis

Critical Medium Minor Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	OTUT	Owner Transfer User's Tokens
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L05	Unused State Variable
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination
	L06	Missing Events Access Control

L01 - Public Function could be Declared External

Criticality	minor
Location	BEP20.sol#L44,L29,L18 and 10 more

Description

Public functions that are never called by the contract should be declared external to save gas.

```
burnFrom
burn
withdrawTokens
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	TumbleToken.sol#L14

Description

Constant state variables should be declared constant to save gas.

```
_price
```

Recommendation

Add the constant attribute to state variables that never change.

L05 - Unused State Variable

Criticality	minor
Location	TumbleToken.sol#L14

Description

There are segments that contains unused state variable.

```
_price
```

Recommendation

Remove unused state variables.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	TumbleToken.sol#L10

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
tumbToken
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L09 - Dead Code Elimination

Criticality	minor
Location	Address.sol#L77,L155,L140 and 11 more

Description

Functions that are not used in the contract, and make the code's size bigger.

```
mul
mod
div
...
```

Recommendation

Remove unused functions.

L06 - Missing Events Access Control

Criticality	minor
Location	Ownable.sol#L23

Description

Detected missing events for critical access control parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
owner = newOwner
```

Recommendation

Emit an event for critical parameter changes.

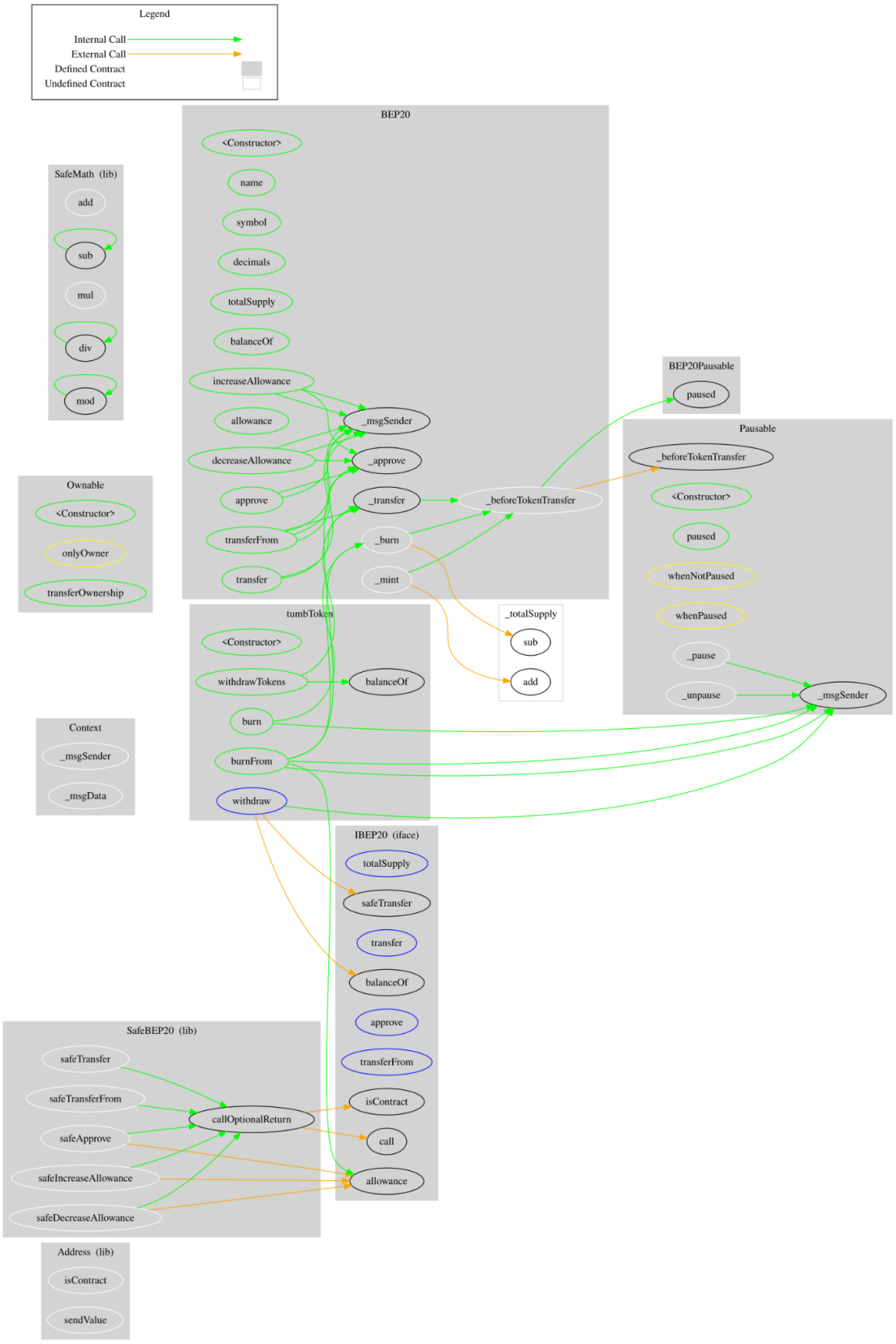
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
BEP20	Implementation	Context, IBEP20		
	<Constructor>	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	✓	
	_beforeTokenTransfer	Internal	✓	
BEP20Pausable	Implementation	BEP20, Pausable		
	_beforeTokenTransfer	Internal	✓	
Context	Implementation			

	_msgSender	Internal		
	_msgData	Internal		
IBEP20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Ownable	Implementation			
	<Constructor>	Public	✓	-
	transferOwnership	Public	✓	onlyOwner
Pausable	Implementation	Context, Ownable		
	<Constructor>	Public	✓	-
	paused	Public		-
	_pause	Internal	✓	onlyOwner whenNotPaused
	_unpause	Internal	✓	onlyOwner whenPaused
SafeBEP20	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	
	safeDecreaseAllowance	Internal	✓	
	callOptionalReturn	Private	✓	
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		

	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
tumbToken	Implementation	BEP20Pausable		
	<Constructor>	Public	✓	BEP20
	withdrawTokens	Public	✓	onlyOwner
	burn	Public	✓	-
	burnFrom	Public	✓	-
	withdraw	External	✓	onlyOwner
	withdraw	External	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	
Registry Domain ID	2666129224_DOMAIN_COM-VRSN
Creation Date	2022-01-05T07:11:42.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created 12 days before the creation of the audit.

There is no public billing information, the creator is protected by the privacy settings.

Summary

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. There are no fees on transactions.

Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Coinscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Coinscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Coinscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Coinscope team disclaims any liability for the resulting losses.

About Coinscope

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co