



Audit Report

MNC

January 2022

Type BEP20
Network BSC
Address 0xC79Fa73643fa4336748c89792994958b6003051f
Audited by © coinscope

Table of Contents

Table of Contents	1
Contract Review	3
Audit Updates	3
Contract Analysis	4
ELFM - Exceed Limit Fees Manipulation	5
Description	5
Recommendation	5
Contract Diagnostics	6
L01 - Public Function could be Declared External	7
Description	7
Recommendation	7
L04 - Conformance to Solidity Naming Conventions	8
Description	8
Recommendation	8
L09 - Dead Code Elimination	9
Description	9
Recommendation	9
L07 - Missing Events Arithmetic	10
Description	10
Recommendation	10
L08 - Tautology or Contradiction	11
Description	11
Recommendation	11
Contract Functions	12
Contract Flow	15
Domain Info	16

Summary	17
Disclaimer	18
About Coinscope	19

Contract Review

Contract Name	BurnableTaxHolderToken
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xC79Fa73643fa4336748c89792994958b6003051f
Symbol	MNC
Decimals	18
Total Supply	776,999,998
Source	contract.sol
Domain	monytoken.com

Audit Updates

Initial Audit	13th 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

ELFM - Exceed Limit Fees Manipulation

Criticality	minor
Location	contract.sol#L706,L713,L721

Description

The contract owner has the authority to increase the fees a bit more than the allowed limit of 25%. The owner may take advantage of it by calling the `changeReflectionFee`, `changeBurnFee` and `changeTaxFee` functions with the maximum allowed limit. As a result the total fee will be 30%

```
function changeTaxFee(uint256 taxFee_) public onlyOwner() returns(bool) {
    require(taxFee_ >= 0, "Tax fee must be greater or equal to zero");
    require(taxFee_ <= 10, "Tax fee must be lower or equal to 10");
    _taxFee = taxFee_;
    return true;
}
```

Recommendation

The contract could embody a check for the maximum acceptable value of the total fees.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	L01	Public Function could be Declared External
●	L04	Conformance to Solidity Naming Conventions
●	L09	Dead Code Elimination
●	L07	Missing Events Arithmetic
●	L08	Tautology or Contradiction

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L775,L766,L747 and 27 more

Description

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

```
includeAccountinReward  
excludeAccountFromReward  
reflectionFromToken  
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L230,L226

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.

```
_totalSupply  
_balances
```

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	contract.sol#L411,L442,L465 and 1 more

Description

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

```
_transfer  
_mint  
_burn  
...
```

Recommendation

Remove unused functions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L721,L713,L706

Description

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

```
_taxFee = taxFee_  
_burnFee = burnFee_  
_reflectionFee = newReflectionFee
```

Recommendation

Emit an event for critical parameter changes.

L08 - Tautology or Contradiction

Criticality	minor
Location	contract.sol#L721,L713,L706

Description

Detects expressions that are tautologies or contradictions. For instance, an uint variable will always be greater than or equal to zero.

```
require(bool,string)(taxFee_ >= 0,Tax fee must be greater or equal to zero)
require(bool,string)(burnFee_ >= 0,Burn fee must be greater or equal to zero)
require(bool,string)(newReflectionFee >= 0,Reflection fee must be greater or
equal to zero)
```

Recommendation

Fix the incorrect comparison by changing the value type or the comparison.

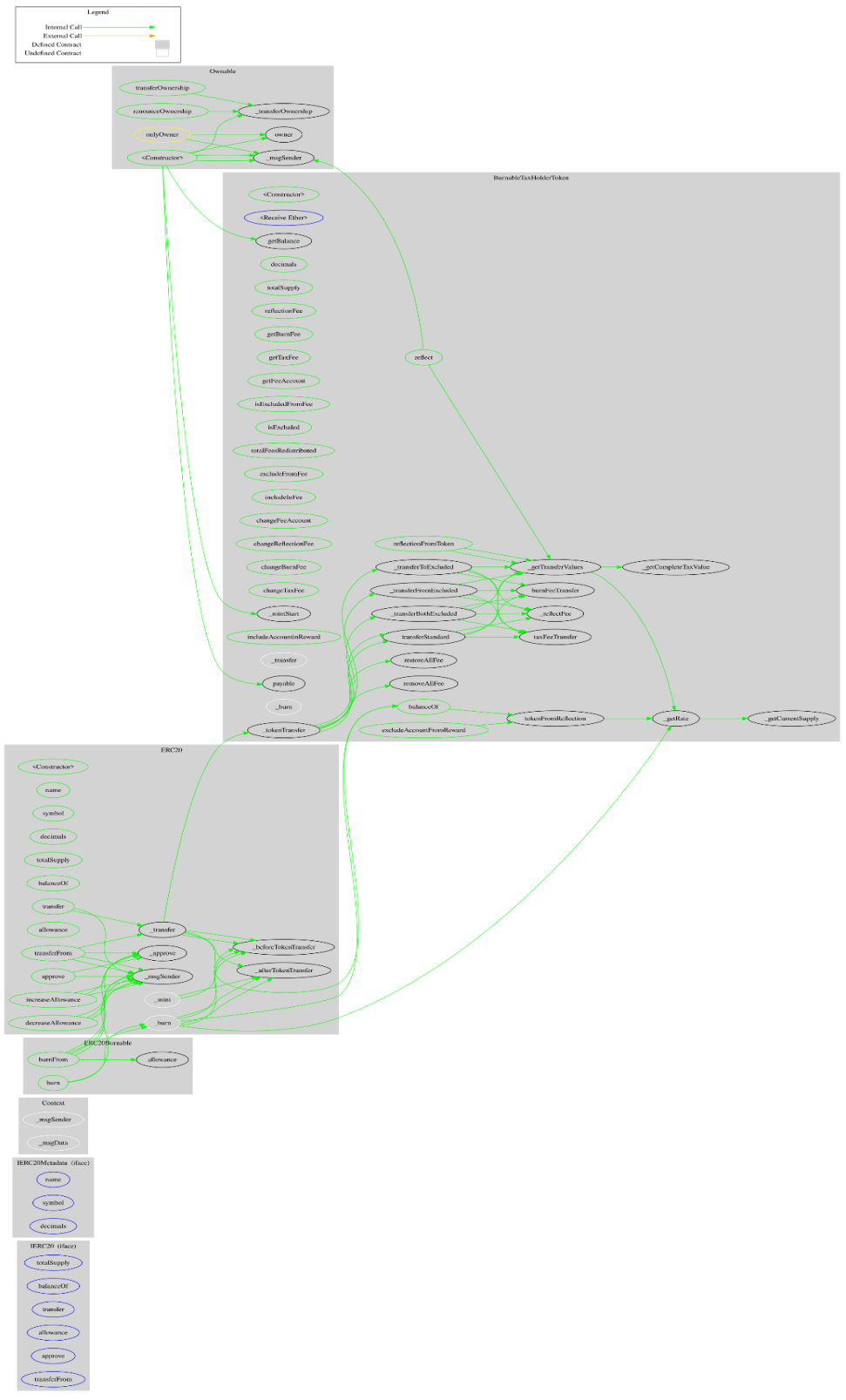
Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metad ata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC20	Implementation	Context, IERC20, IERC20Met adata		

	<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	✓	
	_afterTokenTransfer	Internal	✓	
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
BurnableTaxHolderToken	Implementation	ERC20Burnable, Ownable		
	<Constructor>	Public	Payable	ERC20
	<Receive Ether>	External	Payable	-
	getBalance	Private		
	decimals	Public		-
	totalSupply	Public		-
	reflectionFee	Public		-
	getBurnFee	Public		-
	getTaxFee	Public		-
	getFeeAccount	Public		-

isExcludedFromFee	Public		-
balanceOf	Public		-
isExcluded	Public		-
totalFeesRedistributed	Public		-
excludeFromFee	Public	✓	onlyOwner
includeInFee	Public	✓	onlyOwner
changeFeeAccount	Public	✓	onlyOwner
changeReflectionFee	Public	✓	onlyOwner
changeBurnFee	Public	✓	onlyOwner
changeTaxFee	Public	✓	onlyOwner
_mintStart	Private	✓	
reflect	Public	✓	-
reflectionFromToken	Public		-
tokenFromReflection	Private		
excludeAccountFromReward	Public	✓	onlyOwner
includeAccountinReward	Public	✓	onlyOwner
_transfer	Internal	✓	
_tokenTransfer	Private	✓	
removeAllFee	Private	✓	
restoreAllFee	Private	✓	
_transferStandard	Private	✓	
_transferToExcluded	Private	✓	
_transferFromExcluded	Private	✓	
_transferBothExcluded	Private	✓	
_getCompleteTaxValue	Private		
_getTransferValues	Private		
_reflectFee	Private	✓	
_getRate	Private		
_getCurrentSupply	Private		
burnFeeTransfer	Private	✓	
taxFeeTransfer	Private	✓	
_burn	Internal	✓	

Contract Flow



Domain Info

Domain Name	monytoken.com
Registry Domain ID	2651106893_DOMAIN_COM-VRSN
Creation Date	2021-10-29T14:30:48Z
Updated Date	2021-10-29T14:30:48Z
Registry Expiry Date	2022-10-29T14:30:48Z
Registrar WHOIS Server	whois.ascio.com
Registrar URL	http://www.ascio.com
Registrar	Ascio Technologies, Inc. Danmark - Filial af Ascio technologies, Inc. USA
Registrar IANA ID	106

The domain has been created 3 months before the creation of the audit. It will expire in 10 months.

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

Summary

Mony is aiming to build an all-in-one app store, payment gateway and merchant app. The token 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. There is a limit of max 30% fees that is slightly more than the allowed limit of 25%.

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>