Audit Report

Metacrypto Universe

February 2022

Type	BEP20
Network	BSC
Address	0xDAeB37E1053f00619417812e6E7971b56048625d
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
L02 - State Variables could be Declared Constant 8
Description 8
Recommendation 8
L04 - Conformance to Solidity Naming Conventions 9
Description 9
Recommendation 9
L09 - Dead Code Elimination 10
Description 10
Recommendation 10
L07 - Missing Events Arithmetic 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	CoinToken
Compiler Version	v0.8.2+commit.661d1103
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/address/0xDAeB37E1053f00619417812e6E7971b56048625d#code
Symbol	MTCU
Decimals	9
Total Supply	300,000,000
Source	contract.sol
Domain	metacryptouniverse.com

Audit Updates

Initial Audit	2nd February 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	critical
Location	contract.sol#L1

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `updateFee` function with a high percentage value.

```
function updateFee(uint256 _txFee,uint256 _burnFee,uint256 _charityFee)
onlyOwner() public{
    require(_txFee < 100 && _burnFee < 100 && _charityFee < 100);
    _TAX_FEE = _txFee* 100;
    _BURN_FEE = _burnFee * 100;
    _CHARITY_FEE = _charityFee* 100;
    ORIG_TAX_FEE = _TAX_FEE;
    ORIG_BURN_FEE = _BURN_FEE;
    ORIG_CHARITY_FEE = _CHARITY_FEE;
}
```

For instance, if the contract owner set the `taxFee` to `99` then the following expression will evaluate to `((tAmount * 9900) / 100) / 100` that yields to `99%` fees of the total amount.

```
uint256 tFee = ((tAmount.mul(taxFee)).div(_GRANULARITY)).div(100);
```

Recommendation

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

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
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination
	L07	Missing Events Arithmetic

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L618,L574,L565 and 18 more

Description

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

```
updateFee
reflectionFromToken
deliver
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L457,L459

Description

Constant state variables should be declared constant to save gas.

```
_MAX
_GRANULARITY
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L475,L474,L473 and 14 more

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.

```
ORIG_CHARITY_FEE
ORIG_BURN_FEE
ORIG_TAX_FEE
...
```

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#L241,L225,L11 and 8 more

Description

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

```
mod
_msgData
_getTaxFee
...
```

Recommendation

Remove unused functions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L618

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.

```
_TAX_FEE = _txFee * 100
```

Recommendation

Emit an event for critical parameter changes.

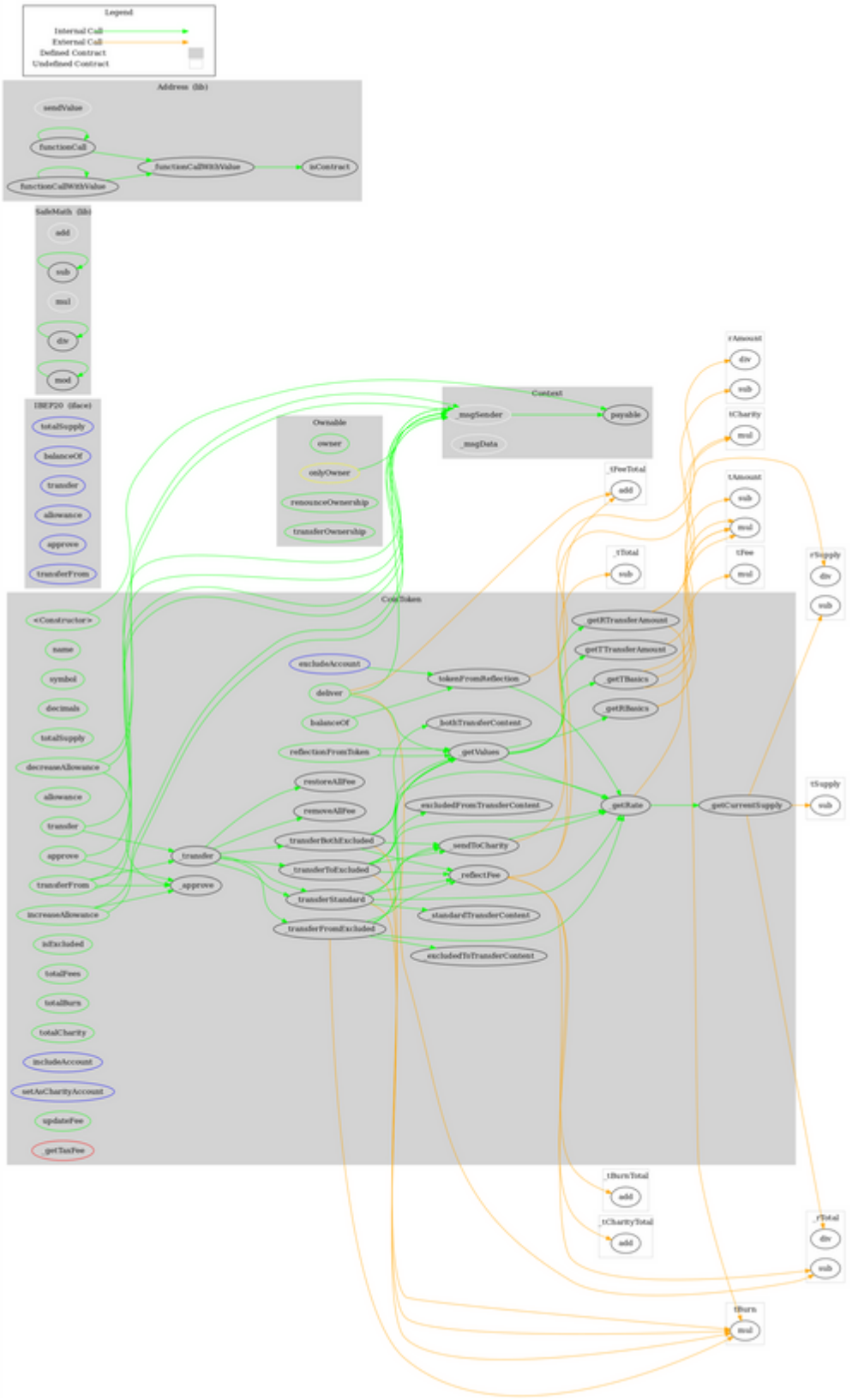
Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IBEP20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	

	_functionCallWithValue	Private	✓	
Ownable	Implementation	Context		
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
CoinToken	Implementation	Context, IBEP20, Ownable		
	<Constructor>	Public	Payable	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcluded	Public		-
	totalFees	Public		-
	totalBurn	Public		-
	totalCharity	Public		-
	deliver	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeAccount	External	✓	onlyOwner
	includeAccount	External	✓	onlyOwner
	setAsCharityAccount	External	✓	onlyOwner
	updateFee	Public	✓	onlyOwner
	_approve	Private	✓	
	_transfer	Private	✓	
	_transferStandard	Private	✓	

	_standardTransferContent	Private	✓	
	_transferToExcluded	Private	✓	
	_excludedFromTransferContent	Private	✓	
	_transferFromExcluded	Private	✓	
	_excludedToTransferContent	Private	✓	
	_transferBothExcluded	Private	✓	
	_bothTransferContent	Private	✓	
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTBasics	Private		
	getTTransferAmount	Private		
	_getRBasics	Private		
	_getRTransferAmount	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_sendToCharity	Private	✓	
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	_getTaxFee	Private		

Contract Flow



Domain Info

Domain Name	metacryptouniverse.com
Registry Domain ID	2656728830_DOMAIN_COM-VRSN
Creation Date	2021-11-22T18:11:09Z
Updated Date	2022-01-22T06:05:40Z
Registry Expiry Date	
Registrar WHOIS Server	whois.publicdomainregistry.com
Registrar URL	www.publicdomainregistry.com
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID	303

The domain has been created 2 months before the creation of the audit.

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

Summary

Metacrypto Universe is aiming to build an NFT/P2E video game based on cryptomining. The Project has a friendly and growing community. The Smart Contract analysis reported one issue. The contract Owner can increase the fees without limit. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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