



Cyberscope

# Audit Report

## **Metfx**

May 2022

Github <https://github.com/METFXWORLD/metfx-token-contract>

Commit [6f1eaa4c07b8b60f341024017cfd61976f250ad7](https://github.com/METFXWORLD/metfx-token-contract/commit/6f1eaa4c07b8b60f341024017cfd61976f250ad7)

Audited by © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>3</b>
<b>Source Files</b>	<b>3</b>
<b>Audit Updates</b>	<b>3</b>
<b>Contract Analysis</b>	<b>4</b>
<b>ST - Stop Transactions</b>	<b>5</b>
Description	5
Recommendation	5
<b>Contract Diagnostics</b>	<b>6</b>
<b>L01 - Public Function could be Declared External</b>	<b>7</b>
Description	7
Recommendation	7
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>8</b>
Description	8
Recommendation	8
<b>L05 - Unused State Variable</b>	<b>9</b>
Description	9
Recommendation	9
<b>L07 - Missing Events Arithmetic</b>	<b>10</b>
Description	10
Recommendation	10
<b>L09 - Dead Code Elimination</b>	<b>11</b>
Description	11
Recommendation	11
<b>L13 - Divide before Multiply Operation</b>	<b>12</b>
Description	12

<b>Recommendation</b>	<b>12</b>
<b>Contract Functions</b>	<b>13</b>
<b>Contract Flow</b>	<b>18</b>
<b>Domain Info</b>	<b>19</b>
<b>Summary</b>	<b>20</b>
<b>Disclaimer</b>	<b>21</b>
<b>About Cyberscope</b>	<b>22</b>

## Contract Review

<b>Contract Name</b>	MetFlix
<b>Compiler Version</b>	v0.8.13+commit.abaa5c0e
<b>Optimization</b>	200 runs
<b>Licence</b>	
<b>Testing Deploy</b>	<a href="https://testnet.bscscan.com/token/0x872Abd014ce8A81410437Ce227Cf7C4Bb458d293">https://testnet.bscscan.com/token/0x872Abd014ce8A81410437Ce227Cf7C4Bb458d293</a>
<b>Symbol</b>	MFLX
<b>Decimals</b>	18
<b>Total Supply</b>	1,000,000,000
<b>Domain</b>	metfx.io
<b>Github</b>	<a href="https://github.com/METFXWORLD/metfx-token-contract">https://github.com/METFXWORLD/metfx-token-contract</a>
<b>Commit</b>	6f1eaa4c07b8b60f341024017cfd61976f250ad7

## Source Files

<b>Filename</b>	<b>SHA256</b>
<b>contract.sol</b>	178d2c11dfd13a34e6be9e7218ab97b3f3aae14ff01878117c613e897f937683

## Audit Updates

<b>Initial Audit</b>	29th May 2022
<b>Corrected</b>	3rd June 2022

# 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

## ST - Stop Transactions

Criticality	medium
Location	contract.sol#L1072

### Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `maxTransactionAmount` or/and `maxWallet` to zero.

```
//when buy
if (automatedMarketMakerPairs[from] && !_isExcludedMaxTransactionAmount[to]) {
    require(amount <= maxTransactionAmount, "Buy transfer amount exceeds the maxTransactionAmount.");
    require(amount + balanceOf(to) <= maxWallet, "Max wallet exceeded");
}

//when sell
else if (automatedMarketMakerPairs[to] && !_isExcludedMaxTransactionAmount[from]) {
    require(amount <= maxTransactionAmount, "Sell transfer amount exceeds the maxTransactionAmount.");
}
```

### Recommendation

The contract could embody a check for not allowing setting the `maxTransactionAmount` and `maxWallet` less than a reasonable amount. A suggested implementation could check that the minimum amount should be more than a fixed percentage of the total supply.

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
●	L05	Unused State Variable
●	L07	Missing Events Arithmetic
●	L09	Dead Code Elimination
●	L13	Divide before Multiply Operation

## L01 - Public Function could be Declared External

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L341,345,353,358,362,367,373,378,485,508,541,927,1008,1040

### Description

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

```
isExcludedFromFees  
setAutomatedMarketMakerPair  
burn  
renounceOwnership  
nonces  
permit  
decreaseAllowance  
increaseAllowance  
transferFrom  
...
```

### Recommendation

Use the external attribute for functions never called from the contract.



## L04 - Conformance to Solidity Naming Conventions

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L314,317,320,323,326,329,466,523,572,850,851,927,987,995,1222,803,841

### 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.

```
_isExcludedMaxTransactionAmount  
deadAddress  
BuyBackTokens  
_treasureChestFee  
_liquidityFee  
_developmentFee  
_value  
treasureChestWalletUpdated  
developmentWalletUpdated  
...
```

### Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>

## L05 - Unused State Variable

**Criticality**

minor

**Location**

contract.sol#L311

### Description

There are segments that contain unused state variables.

```
ERC20TOKEN_ERC1820_INTERFACE_ID
```

### Recommendation

Remove unused state variables.

## L07 - Missing Events Arithmetic

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L965,970,974,987,995

### 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.

```
sellDevelopmentFee = _developmentFee
buyDevelopmentFee = _developmentFee
maxWallet = newNum * (10 ** 18)
maxTransactionAmount = newNum * (10 ** 18)
swapTokensAtAmount = newAmount
```

### Recommendation

Emit an event for critical parameter changes.

## L09 - Dead Code Elimination

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L78,103,113,52,438,402,741,765,756,725,292,301,280,288,297,267,284

### Description

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

```
subtractPercentage  
sqrt  
quadraticPricing  
percentageOfTotal  
percentageAmount  
bondingCurve  
average  
safeTransferFrom  
safeIncreaseAllowance  
...
```

### Recommendation

Remove unused functions.

## L13 - Divide before Multiply Operation

**Criticality**

minor

**Location**

contract.sol#L1046

### Description

Performing divisions before multiplications may cause lose of prediction.

```
tokensForDevelopment += fees * 33 / 99
tokensForDevelopment += fees * sellDevelopmentFee / sellTotalFees
fees = amount * buyTotalFees / 100
tokensForTreasureChest += fees * 33 / 99
tokensForTreasureChest += fees * sellTreasureChestFee / sellTotalFees
tokensForLiquidity += fees * 33 / 99
fees = amount * sellTotalFees / 100
```

### Recommendation

The multiplications should be prior to the divisions.

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Address</b>	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	_functionCallWithValue	Private	✓	
<b>IERC20</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		
	sqrt	Internal		
	percentageAmount	Internal		

	subtractPercentage	Internal		
	percentageOfTotal	Internal		
	average	Internal		
	quadraticPricing	Internal		
	bondingCurve	Internal		
<b>ERC20</b>	Implementation	IERC20		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	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	✓	
<b>Counters</b>	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	
<b>IERC2612Permit</b>	Interface			
	permit	External	✓	-
	nonces	External		-

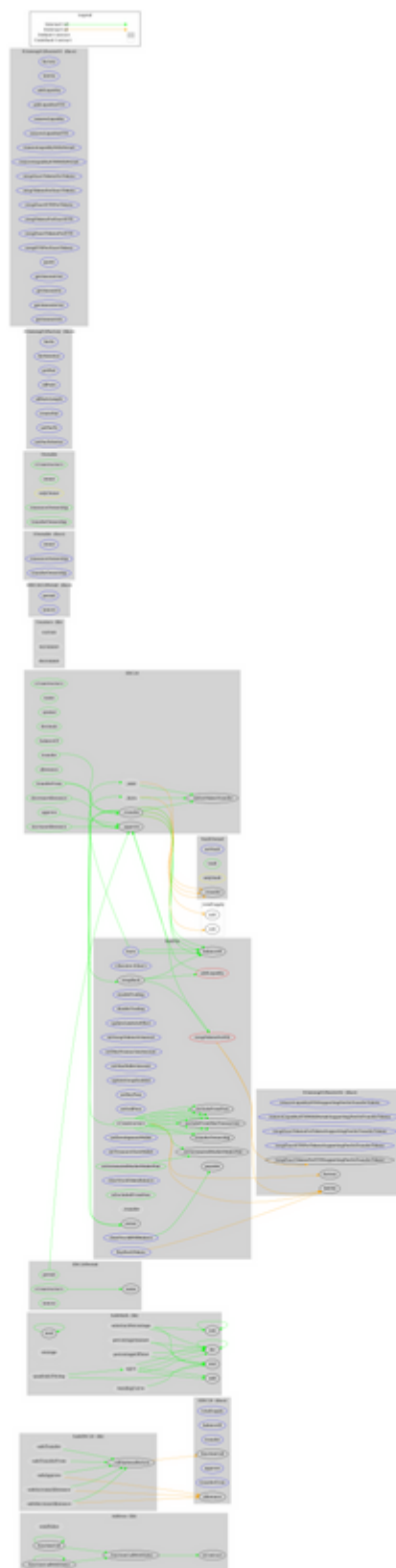
<b>ERC20Permit</b>	Implementation	ERC20, IERC2612P ermit		
	<Constructor>	Public	✓	-
	permit	Public	✓	-
	nonces	Public		-
<b>IOwnable</b>	Interface			
	owner	External		-
	renounceOwnership	External	✓	-
	transferOwnership	External	✓	-
<b>Ownable</b>	Implementation	IOwnable		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
<b>VaultOwned</b>	Implementation	Ownable		
	setVault	External	✓	onlyOwner
	vault	Public		-
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
<b>IUniswapV2Router01</b>	Interface			
	factory	External		-



	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
<b>SafeERC20</b>	Library			
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeApprove	Internal	✓	
	safeIncreaseAllowance	Internal	✓	

	safeDecreaseAllowance	Internal	✓	
	_callOptionalReturn	Private	✓	
<b>MetFlix</b>	Implementation	ERC20, VaultOwned		
	<Constructor>	Public	✓	ERC20
	<Receive Ether>	External	Payable	-
	burn	External	✓	-
	enableTrading	External	✓	onlyOwner
	disableTrading	External	✓	onlyOwner
	updateLimitsInEffect	External	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
	setMaxTransactionAmount	External	✓	onlyOwner
	setMaxWalletAmount	External	✓	onlyOwner
	excludeFromMaxTransaction	Public	✓	onlyOwner
	updateSwapEnabled	External	✓	onlyOwner
	setBuyFees	External	✓	onlyOwner
	setSellFees	External	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	setDevelopmentWallet	External	✓	onlyOwner
	setTreasureChestWallet	External	✓	onlyOwner
	clearStuckBNBBalance	External	✓	onlyOwner
	clearStuckTokenBalance	External	✓	onlyOwner
	isExcludedFromFees	Public		-
	_transfer	Internal	✓	
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	swapBack	Private	✓	
	BuyBackTokens	External	✓	onlyOwner

# Contract Flow



## Domain Info

<b>Domain Name</b>	metfx.io
<b>Registry Domain ID</b>	d2cf44ba7edb4a1baff3af71c6ed8b25-DONUTS
<b>Creation Date</b>	2022-01-11T23:47:57Z
<b>Updated Date</b>	2022-02-24T08:15:24Z
<b>Registry Expiry Date</b>	2023-01-11T23:47:57Z
<b>Registrar WHOIS Server</b>	whois.namesilo.com
<b>Registrar URL</b>	<a href="http://www.namesilo.com">http://www.namesilo.com</a>
<b>Registrar</b>	NameSilo, LLC
<b>Registrar IANA ID</b>	1479

The domain has been created 5 months before the creation of the audit. It will expire in 8 months.

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

## Summary

The Smart Contract analysis reported one medium severity issue. The contract owner has the authority to stop transactions. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats. There is also a limit of max 10% fees.

## 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.

Cyberscope 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 Cyberscope 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 Cyberscope 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 Cyberscope team disclaims any liability for the resulting losses.

# About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

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.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.



The Cyberscope team

<https://www.cyberscope.io>