COINSCOPE

Audit Report

QUARASHI NETWORK

February 2022

Type	ERC-20
Network	ETH
Address	0x0aFf88B4Cf3015c9c17f1dA1FCCb88C632F3505E
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	MainToken
Compiler Version	v0.4.24+commit.e67f0147
Optimization	200 runs
Licence	GNU GPLv3
Explorer	https://etherscan.io/token/0x0aff88b4cf3015c9c17f1da1fccb88c632f3505e
Symbol	QUA
Decimals	18
Total Supply	799,176,692.33293494629

Audit Updates

Initial Audit	9th of 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

Unused functionality

The contract has the ability to mint new tokens. All the functions that are related to minting require the *canMint* modifier. The canMint modifier is a boolean flag that determines if the mint action can start. This flag initially was enabled but now it is disabled. The mint flag is a one-way flag, that means that it can not switch on again. Thus, the mint functionality cannot be used any more.

The transaction that switched off the mint feature

https://etherscan.io/tx/0x1fe29e6c3af500a7b6f5e323992e30b0fece1af113f14d9d2831e448d8c88bdf

Freeze Functionality

The contract supports a feature called “Freeze”. Users can send an amount of tokens to an address and choose when these tokens will be available. Essentially, the recipient will have the tokens but she will not be able to use them until the time period elapses.

The contract combines the mint and freeze functionality. That means that the contract owner had the ability to mint and time-lock tokens to an address. This feature is not available any more since it required the *canMint* modifier

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

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L98,134,140,229,252,308 and 15 more

Description

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

```
decimals
symbol
name
...
```

Recommendation

Use the external attribute for functions never called from the contract

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L107,122,168,169,170,196 and 31 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.

```
_value
_to
_from
...
```

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#L57,41

Description

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

```
mul
div
```

Recommendation

Remove unused functions.

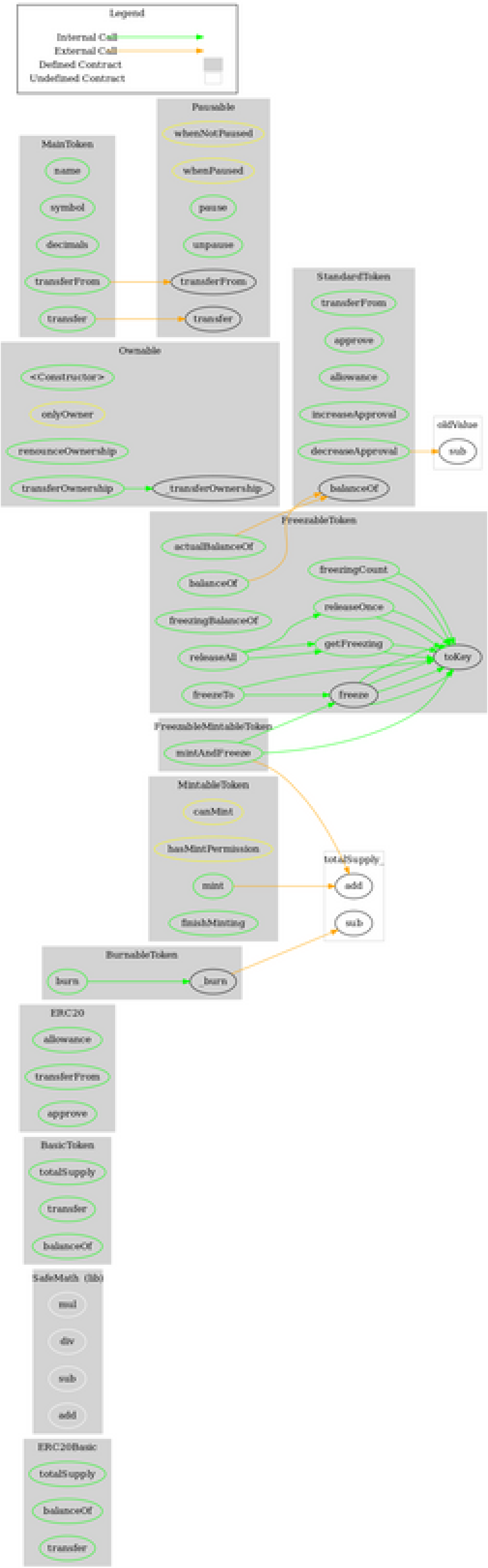
Contract Functions

Contract	**Type**	**Bases**		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
ERC20Basic	Implementation			
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
SafeMath	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
BasicToken	Implementation	ERC20Basic		
	totalSupply	Public		-
	transfer	Public	✓	-
	balanceOf	Public		-
ERC20	Implementation	ERC20Basic		
	allowance	Public		-
	transferFrom	Public	✓	-
	approve	Public	✓	-
StandardToken	Implementation	ERC20, BasicToken		
	transferFrom	Public	✓	-
	approve	Public	✓	-
	allowance	Public		-
	increaseApproval	Public	✓	-
	decreaseApproval	Public	✓	-

Ownable	Implementation			
	<Constructor>	Public	✓	-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
MintableToken	Implementation	StandardToken, Ownable		
	mint	Public	✓	hasMintPermision canMint
	finishMinting	Public	✓	onlyOwner canMint
FreezableToken	Implementation	StandardToken		
	balanceOf	Public		-
	actualBalanceOf	Public		-
	freezingBalanceOf	Public		-
	freezingCount	Public		-
	getFreezing	Public		-
	freezeTo	Public	✓	-
	releaseOnce	Public	✓	-
	releaseAll	Public	✓	-
	toKey	Internal		
	freeze	Internal	✓	
BurnableToken	Implementation	BasicToken		
	burn	Public	✓	-
	_burn	Internal	✓	
Pausable	Implementation	Ownable		
	pause	Public	✓	onlyOwner whenNotPaused
	unpause	Public	✓	onlyOwner

				whenPaused
FreezableMintableToken	Implementation	FreezableToken, MintableToken		
	mintAndFreeze	Public	✓	onlyOwner canMint
Consts	Implementation			
MainToken	Implementation	Consts, FreezableMintableToken, BurnableToken, Pausable		
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	transferFrom	Public	✓	-
	transfer	Public	✓	-

Contract Flow



Domain Info

Domain Name	quarashi.network
Registry Domain ID	74953879daf3467fb29bb3e7bb89fc11-DONUTS
Creation Date	2021-02-20T06:45:34Z
Updated Date	2021-07-23T19:03:45Z
Registry Expiry Date	2023-02-20T06:45:34Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created 12 months before the creation of the audit. It will expire in about 1 year.

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. Additionally, the contract contains some extra features like transfer and time-lock tokens. These features can be issued by the users. The audit describes these features and notes some minor recommendations.

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