



Cyberscope

Audit Report

Z Versus Project

July 2022

Type BEP20

Network BSC

Address 0xc8b52f5a2feaa7a4390b099f2f5e45e46760c1b2

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Source Files	3
Audit Updates	3
Contract Analysis	4
MT - Mint Tokens	5
Description	5
Recommendation	5
ST - Stop Transactions	6
Description	6
Recommendation	6
BC - Blacklisted Contracts	7
Description	7
Recommendation	7
Contract Diagnostics	8
L01 - Public Function could be Declared External	9
Description	9
Recommendation	9
L04 - Conformance to Solidity Naming Conventions	10
Description	10
Recommendation	10
L11 - Unnecessary Boolean equality	11
Description	11
Recommendation	11
Contract Functions	12
Contract Flow	14

Domain Info	15
Summary	16
Disclaimer	17
About Cyberscope	18

Contract Review

Contract Name	CoinToken
Compiler Version	v0.4.24+commit.e67f0147
Optimization	200 runs
Licence	Apache-2.0
Explorer	https://bscscan.com/token/0xC8b52F5a2fEAa7A4390B099f2f5E45E46760c1b2
Symbol	ZVERSUS
Decimals	9
Total Supply	1,000,000,000
Domain	zversus.io

Source Files

Filename	SHA256
contract.sol	e994b0153c44e8ed42db01bb21bb0afb8d17e9e719a17123ebfa329c1cc0ec0a

Audit Updates

Initial Audit	11th July 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

MT - Mint Tokens

Criticality	critical
Location	contract.sol#L256

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mint` function. As a result the contract tokens will be highly inflated.

```
function mint(address account, uint256 amount) onlyOwner public {  
  
    totalSupply = totalSupply.add(amount);  
    balances[account] = balances[account].add(amount);  
    emit Mint(address(0), account, amount);  
    emit Transfer(address(0), account, amount);  
}
```

Recommendation

The owner should carefully manage the credentials of the owner's account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

ST - Stop Transactions

Criticality	minor
Location	contract.sol#L85

Description

The contract owner has the authority to stop transactions for all users. The owner may do that by calling the `pause` function.

```
function pause() onlyOwner whenNotPaused public {  
    paused = true;  
    emit Pause();  
}
```

Recommendation

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.

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L220

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `blacklistAddress` function.

```
function blackListAddress(address listAddress, bool isBlackListed) public  
whenNotPaused onlyOwner returns (bool success) {  
    return super._blackList(listAddress, isBlackListed);  
}
```

Recommendation

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
●	L11	Unnecessary Boolean equality

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L51,85,93,101,107,220,244,256

Description

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

```
mint  
burn  
blackListAddress  
allowance  
balanceOf  
unpause  
pause  
transferOwnership
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality

minor

Location

contract.sol#L125,138,142,156,163,168,174,200,204,208,212,216,244

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  
_subtractedValue  
_spender  
_addedValue  
_to  
_from  
_owner  
...
```

Recommendation

Follow the Solidity naming convention.

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

L11 - Unnecessary Boolean equality

Criticality

minor

Location

contract.sol#L125,142

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
require(bool)(tokenBlacklist[msg.sender] == false)
```

Recommendation

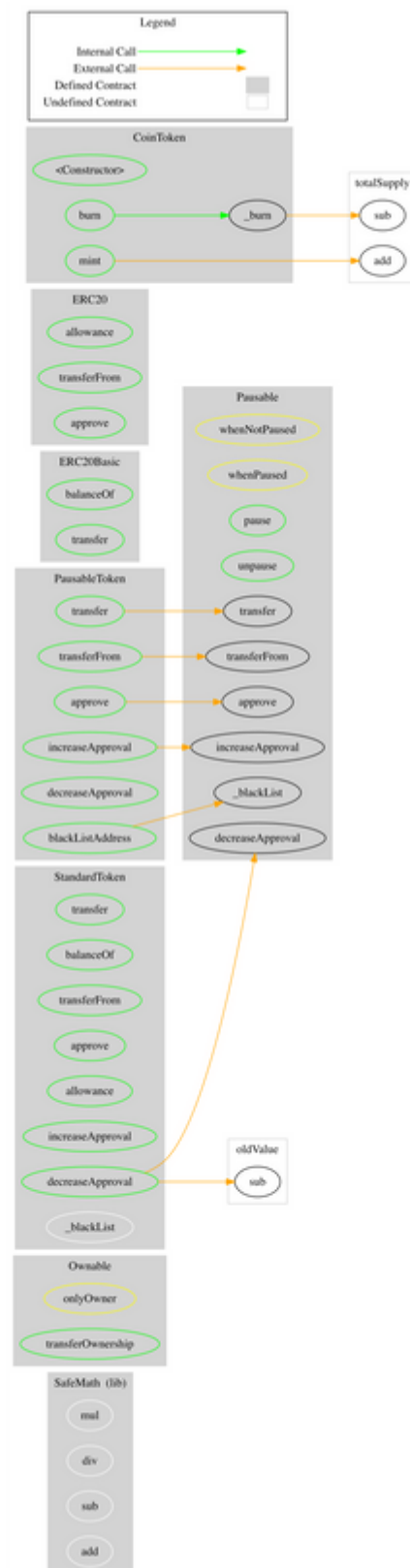
Remove the equality to the boolean constant.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMath	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
Ownable	Implementation			
	transferOwnership	Public	✓	onlyOwner
Pausable	Implementation	Ownable		
	pause	Public	✓	onlyOwner whenNotPaused
	unpause	Public	✓	onlyOwner whenPaused
ERC20Basic	Implementation			
	balanceOf	Public		-
	transfer	Public	✓	-
ERC20	Implementation	ERC20Basic		
	allowance	Public		-
	transferFrom	Public	✓	-
	approve	Public	✓	-
StandardToken	Implementation	ERC20		
	transfer	Public	✓	-
	balanceOf	Public		-
	transferFrom	Public	✓	-
	approve	Public	✓	-

	allowance	Public		-
	increaseApproval	Public	✓	-
	decreaseApproval	Public	✓	-
	_blackList	Internal	✓	
PausableToken	Implementation	StandardToken, Pausable		
	transfer	Public	✓	whenNotPaused
	transferFrom	Public	✓	whenNotPaused
	approve	Public	✓	whenNotPaused
	increaseApproval	Public	✓	whenNotPaused
	decreaseApproval	Public	✓	whenNotPaused
	blackListAddress	Public	✓	whenNotPaused onlyOwner
CoinToken	Implementation	PausableToken		
	<Constructor>	Public	✓	-
	burn	Public	✓	-
	_burn	Internal	✓	
	mint	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	zversus.io
Registry Domain ID	d78703517ed94161b1e8de375cc31687-DONUTS
Creation Date	2022-01-10T13:51:00Z
Updated Date	2022-04-20T12:38:14Z
Registry Expiry Date	2023-01-10T13:51:00Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created in 6 months before the creation of the audit.

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

Summary

There are some functions that can be abused by the owner like minting tokens and blacklisting addresses. If the contract owner abuses the mint functionality, then the contract will be highly inflated. 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.

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.

Cyberscope 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>