



Cyberscope

Audit Report

BIT GAME VERSE TOKEN

November 2022

Type BEP20

Network BSC

Address 0xa03110800894b3CcF8723D991d80875561F96777

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Source Files	3
Audit Updates	3
Contract Analysis	4
ST - Stops Transactions	5
Description	5
Recommendation	5
OCTD - Transfers Contract's Tokens	6
Description	6
Recommendation	6
BC - Blacklists Addresses	7
Description	7
Recommendation	7
Contract Diagnostics	8
L02 - State Variables could be Declared Constant	9
Description	9
Recommendation	9
L04 - Conformance to Solidity Naming Conventions	10
Description	10
Recommendation	10
L07 - Missing Events Arithmetic	11
Description	11
Recommendation	11
L13 - Divide before Multiply Operation	12
Description	12

Recommendation	12
Contract Functions	13
Contract Flow	16
Domain Info	17
Summary	18
Disclaimer	19
About Cyberscope	20

Contract Review

Contract Name	BitGameVerse
Compiler Version	v0.8.17+commit.8df45f5f
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0xa03110800894b3CcF8723D991d80875561F96777
Symbol	BGVT
Decimals	18
Total Supply	70,000,000,000
Domain	bgverse.io

Source Files

Filename	SHA256
contract.sol	e18c2bee4253ddb5ea873e4f79982c84919e4b53e707f5c7f12bb7138fd1212e

Audit Updates

Initial Audit	9th November 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Unresolved

ST - Stops Transactions

Criticality	critical
Location	contract.sol#L515, L516, L525, L534
Status	Unresolved

Description

The contract owner has the authority to stop the transactions for all users excluding the owner. The owner may take advantage of it by setting the `maxBuyLimit`, `maxWalletLimit` or `maxSellLimit` to zero, or by setting the `coolDownTime` to a high value. The contract may operate as a honeypot.

```
require(amount <= maxBuyLimit, "You are exceeding maxBuyLimit");
...
require(balanceOf(to) + amount <= maxWalletLimit, "You are exceeding maxWalletLimit");
...
require(amount <= maxSellLimit, "You are exceeding maxSellLimit");
...
require(timePassed >= coolDownTime, "Cooldown enabled");
```

Recommendation

The contract could embody a check for not allowing setting the `maxBuyLimit`, `maxWalletLimit` or `maxSellLimit` less than a reasonable amount and `coolDownTime` more than a reasonable amount or none at all.

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.

OCTD - Transfers Contract's Tokens

Criticality	minor
Location	contract.sol#L716
Status	Unresolved

Description

The contract owner has the authority to claim all the balance of the contract. The owner may take advantage of it by calling the `rescueAnyBEP20Tokens` function.

```
function rescueAnyBEP20Tokens(  
    address _tokenAddr,  
    address _to,  
    uint256 _amount  
) public onlyOwner {  
    IERC20(_tokenAddr).transfer(_to, _amount);  
}
```

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 - Blacklists Addresses

Criticality	critical
Location	contract.sol#L672, L676
Status	Unresolved

Description

The contract owner has the authority to stop addresses from transactions. The owner may take advantage of it by calling the `updateIsBlacklisted` and `bulkIsBlacklisted` functions.

```
function updateIsBlacklisted(address account, bool state) external onlyOwner {
    _isBlacklisted[account] = state;
}
```

```
function bulkIsBlacklisted(address[] memory accounts, bool state) external onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        _isBlacklisted[accounts[i]] = state;
    }
}
```

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 / Informative

Severity	Code	Description	Status
●	L02	State Variables could be Declared Constant	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L07	Missing Events Arithmetic	Unresolved
●	L13	Divide before Multiply Operation	Unresolved

L02 - State Variables could be Declared Constant

Criticality	minor / informative
Location	contract.sol#L138,137,152,161,163
Status	Unresolved

Description

Constant state variables should be declared constant to save gas.

```
swapEnabled  
tradingEnabled  
_tTotal  
deadline  
deadWallet
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L714,149,168,160,713,167,88,715,190
Status	Unresolved

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.

```
_to  
_decimals  
_symbol  
genesis_block  
_tokenAddr  
_name  
WETH  
_amount  
valuesFromGetValues
```

Recommendation

Follow the Solidity naming convention.

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

L07 - Missing Events Arithmetic

Criticality	minor / informative
Location	contract.sol#L663,692,668,697
Status	Unresolved

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.

```
coolDownTime = time * 1  
maxBuyLimit = maxBuy * 10 ** decimals()  
swapTokensAtAmount = amount * 10 ** _decimals  
maxWalletLimit = amount * 10 ** decimals()
```

Recommendation

Emit an event for critical parameter changes.

L13 - Divide before Multiply Operation

Criticality	minor / informative
Location	contract.sol#L599
Status	Unresolved

Description

Performing divisions before multiplications may cause lose of prediction.

```
unitBalance = deltaBalance / (denominator - temp.liquidity)
```

Recommendation

The multiplications should be prior to the divisions.

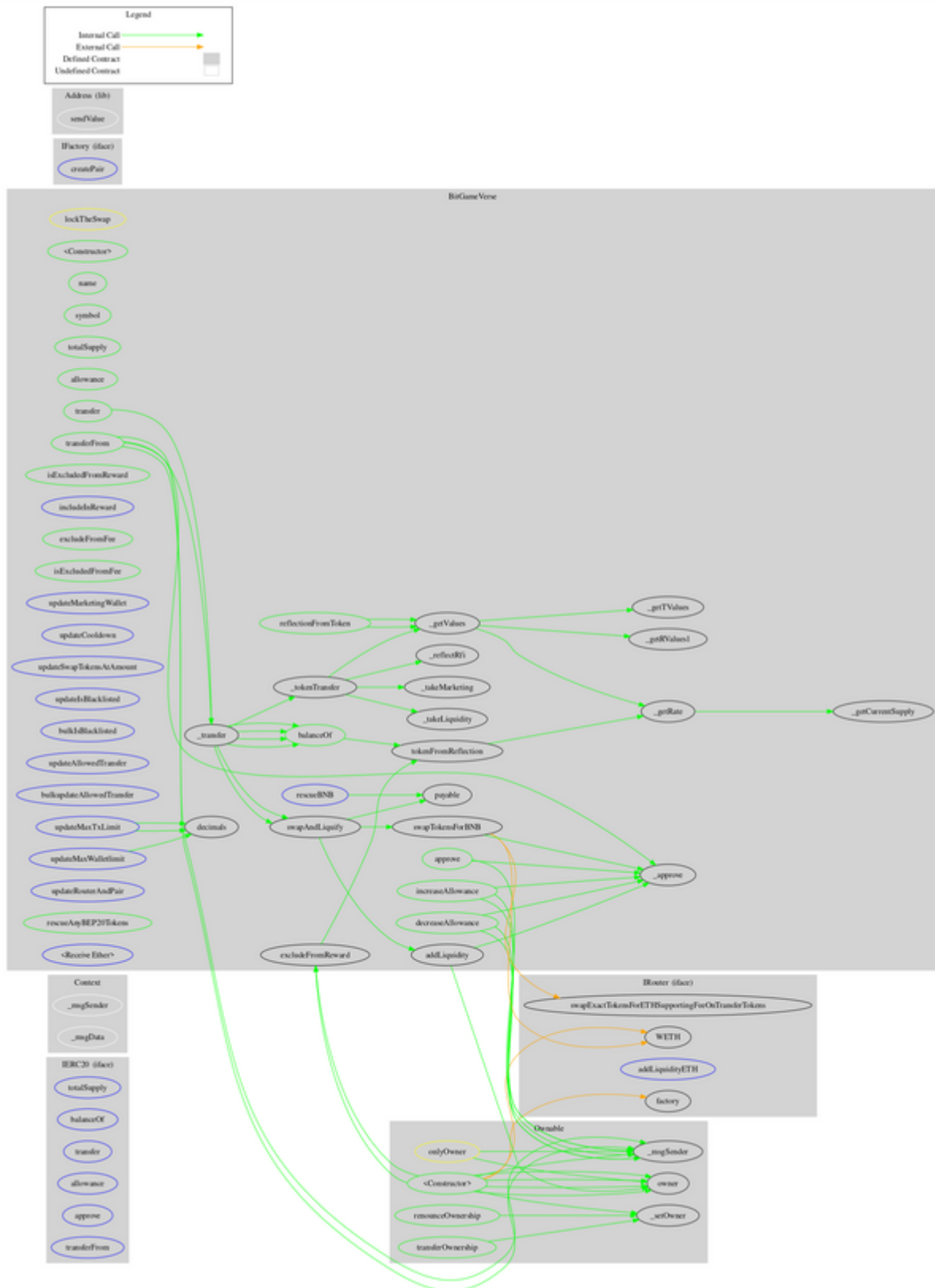
Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
IFactory	Interface			
	createPair	External	✓	-
IRouter	Interface			
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
	swapExactTokensForETHSupporting FeeOnTransferTokens	External	✓	-

Address	Library			
	sendValue	Internal	✓	
BitGameVerse	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	transfer	Public	✓	-
	isExcludedFromReward	Public		-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	excludeFromFee	Public	✓	onlyOwner
	isExcludedFromFee	Public		-
	_reflectRfi	Private	✓	
	_takeLiquidity	Private	✓	
	_takeMarketing	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues1	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	_tokenTransfer	Private	✓	

	swapAndLiquify	Private	✓	lockTheSwap
	addLiquidity	Private	✓	
	swapTokensForBNB	Private	✓	
	updateMarketingWallet	External	✓	onlyOwner
	updateCooldown	External	✓	onlyOwner
	updateSwapTokensAtAmount	External	✓	onlyOwner
	updateIsBlacklisted	External	✓	onlyOwner
	bulkIsBlacklisted	External	✓	onlyOwner
	updateAllowedTransfer	External	✓	onlyOwner
	bulkupdateAllowedTransfer	External	✓	onlyOwner
	updateMaxTxLimit	External	✓	onlyOwner
	updateMaxWalletlimit	External	✓	onlyOwner
	updateRouterAndPair	External	✓	onlyOwner
	rescueBNB	External	✓	onlyOwner
	rescueAnyBEP20Tokens	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-

Contract Flow



Domain Info

Domain Name	bgverse.io
Registry Domain ID	4a22538a0bd34102a502bc27592585eb-DONUTS
Creation Date	2022-02-06T18:45:45Z
Updated Date	2022-03-02T20:56:32Z
Registry Expiry Date	2023-02-06T18:45:45Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain was created 9 months before the creation of the audit. It will expire in 3 months.

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 stopping transactions and massively blacklisting addresses. 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 3% 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>