Cyberscope

Audit Report

BitChain

December 2022

Type	BEP20
Network	BSC
Address	0x84ec718efc361a1b246680f1dbe0fb26045dcc16
Audited by	© cyberscope

Table of Contents

Table of Contents 1
Contract Review 2
Source Files 2
Audit Updates 2
Contract Analysis 3
Contract Diagnostics 4
DDP - Decimal Division Precision 5
Description 5
Recommendation 5
L04 - Conformance to Solidity Naming Conventions 6
Description 6
Recommendation 6
Contract Functions 7
Contract Flow 11
Domain Info 12
Summary 13
Disclaimer 14
About Cyberscope 15

Contract Review

Contract Name	BitChain
Compiler Version	v0.8.16+commit.07a7930e
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x84ec718efc361a1b246680f1dbe0fb26045dcc16
Symbol	BitCh
Decimals	18
Total Supply	1,000,000,000
Domain	thebitchain.io

Source Files

Filename	**SHA256**
contract.sol	41c1cf1faa0dff258a4a0b711b27444bdfcc919226c7c48ed8505d1ac7f287c3

Audit Updates

Initial Audit	10th December 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	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	Passed

Contract Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	DDP	Decimal Division Precision	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved

DDP - Decimal Division Precision

Criticality	minor / informative
Location	contract.sol#L982
Status	Unresolved

Description

The the calculated value is the result division. Since Solidity has not floating types, then the result of a division may miss the decimals precision. As a result, the splitted shares will not have the exact precision and some funds may not be calculated as expected.

```
uint256 stakingShare = ((contractBalanceBUSD * 6) / 11);
uint256 bitChDevShare = ((contractBalanceBUSD * 3) / 11);
uint256 bitChMarketingShare = ((contractBalanceBUSD * 2) / 11);
```

Recommendation

The contract could calculate the subtraction of the divided funds in the last calculation in order to avoid the division rounding issue.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contract.sol#L839,836,70,101,68,837,147,842,838
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.

```
bitChMarketingPercentage
stakingPercentage
PERMIT_TYPEHASH
MINIMUM_LIQUIDITY
DOMAIN_SEPARATOR
liquidityPercentage
WETH
burnRateStrategicBurnReserves
bitChDevPercentage
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-conventions.

Contract Functions

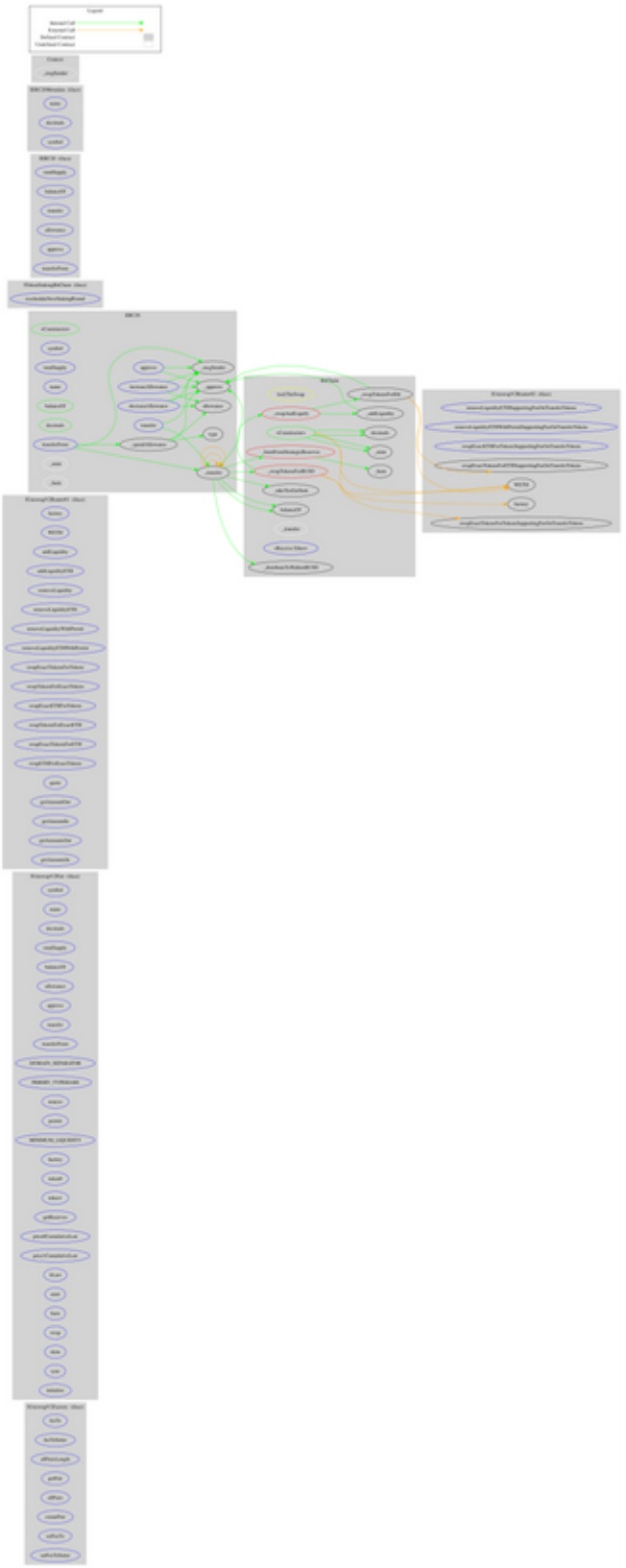
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	allPairsLength	External		-
	getPair	External		-
	allPairs	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	Interface			
	symbol	External		-
	name	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-

	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IUniswapV2Router01	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		-
IUniswapV2Router02	Interface	IUniswapV2Router01		

	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
ITokenStaking BitChain	Interface			
	rescheduleNewStakingRound	External	✓	-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	decimals	External		-
	symbol	External		-
Context	Implementation			
	_msgSender	Internal		
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	symbol	External		-
	totalSupply	External		-

	name	External		-
	balanceOf	Public		-
	decimals	Public		-
	allowance	Public		-
	transfer	External	✓	-
	approve	External	✓	-
	transferFrom	External	✓	-
	decreaseAllowance	External	✓	-
	increaseAllowance	External	✓	-
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_transfer	Internal	✓	
BitChain	Implementation	ERC20		
	<Constructor>	Public	✓	ERC20
	_takeTaxGetSum	Private	✓	
	_burnFromStrategicReserves	Private	✓	
	_swapAndLiquify	Private	✓	lockTheSwap
	_swapTokensForEth	Private	✓	
	_addLiquidity	Private	✓	
	_swapTokensForBUSD	Private	✓	lockTheSwap
	_distributeToWalletsBUSD	Private	✓	
	_transfer	Internal	✓	
	<Receive Ether>	External	Payable	-

Contract Flow



Domain Info

Domain Name	thebitchain.io
Registry Domain ID	bcc3de349166481ca8c48c815db9d555-DONUTS
Creation Date	2022-12-09T10:32:06Z
Updated Date	2022-12-09T10:32:06Z
Registry Expiry Date	2023-12-09T10:32:06Z
Registrar WHOIS Server	whois.name.com
Registrar URL	http://www.name.com
Registrar	Name.com, Inc.
Registrar IANA ID	625

The domain was created 1 day before the creation of the audit. It will expire in 12 months.

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

Summary

BitChain is an interesting project that has a friendly and growing community. 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. The fees are fixed to 10%.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope’s prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope’s position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io