



TechRate
AUDIT COMPANY

Smart Contract Security Audit

TechRate

December, 2021

Audit Details



Audited project

BINANCE MULTI-CHAIN CAPITAL



Deployer address

0x5A5444F6b5D511F61ff7C3152054D4030f3891ca



Client contacts:

BINANCE MULTI-CHAIN CAPITAL team



Blockchain

Binance Smart Chain



Project website:

<https://bmcc.finance>

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by BINANCE MULTI-CHAIN CAPITAL to perform an audit of smart contracts:

<https://bscscan.com/address/0xb6d8ee99d5d6cfe7d80b666e6ff5e74e3f72756b#code>

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 05.12.2021

Contract name	BINANCE MULTI-CHAIN CAPITAL
Contract address	0xb6D8EE99D5d6cfe7D80b666e6fF5e74e3f72756b
Total supply	1,000,000,000,000
Token ticker	BMCC
Decimals	9
Token holders	151
Transactions count	856
Top 100 holders dominance	97.25%
This balance	4289002613630020896
Amount in pool	229775999537579769888
Contract deployer address	0x5A5444F6b5D511F61ff7C3152054D4030f3891ca
Contract's current owner address	0x5A5444F6b5D511F61ff7C3152054D4030f3891ca

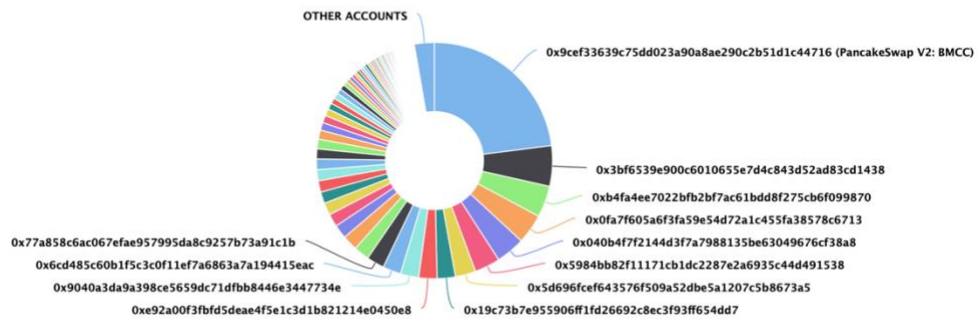
BINANCE MULTI-CHAIN CAPITAL Token Distribution

The top 100 holders collectively own 97.25%
(972,541,247,202.71 Tokens) of BINANCE MULTI-CHAIN CAPITAL

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 151

BINANCE MULTI-CHAIN CAPITAL Top 100 Token Holders

Source: BscScan.com



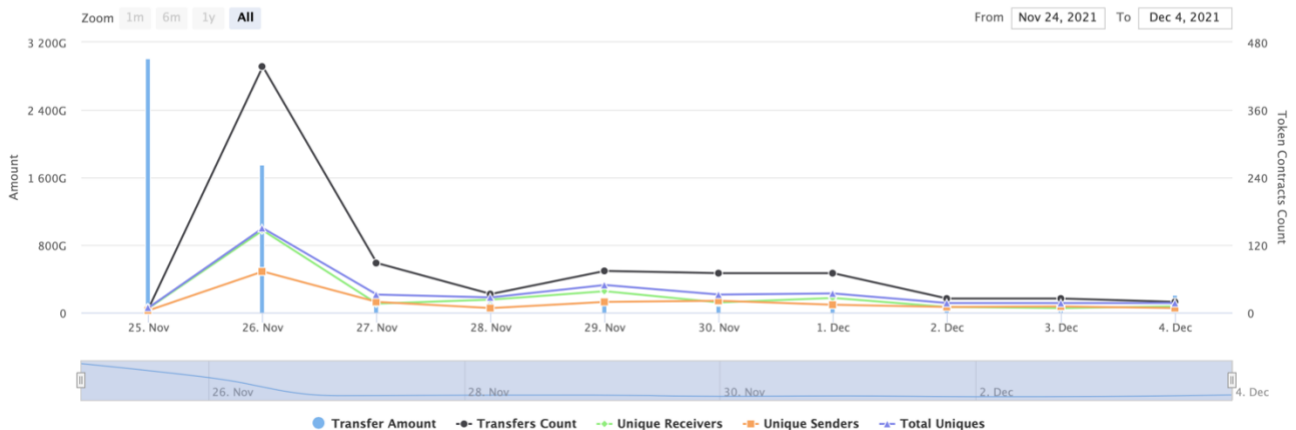
(A total of 972,541,247,202.71 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

BINANCE MULTI-CHAIN CAPITAL Contract Interaction Details

Time Series: Token Contract Overview


Thu 25, Nov 2021 - Sat 4, Dec 2021

Token Contract 0xb6d8ee99d5d6cfe7d80b666e6ff5e74e3f72756b (BINANCE MULTI-CHAIN CAPITAL)
Source: BscScan.com



BINANCE MULTI-CHAIN CAPITAL

Top 10 Token Holders

Rank	Address	Quantity	Percentage
1	 PancakeSwap V2: BMCC	229,775,999,537.579769888	22.9776%
2	0x3bf6539e900c6010655e7d4c843d52ad83cd1438	55,434,005,160.482224125	5.5434%
3	0xb4fa4ee7022bfb2bf7ac61bdd8f275cb6f099870	42,922,120,380.906727187	4.2922%
4	0x0fa7f605a6f3fa59e54d72a1c455fa38578c6713	40,763,318,812.855800069	4.0763%
5	0x040b4f7f2144d3f7a7988135be63049676cf38a8	39,569,081,320.436865442	3.9569%
6	0x5984bb82f11171cb1dc2287e2a6935c44d491538	35,008,773,376.606936964	3.5009%
7	0x5d696cef643576f509a52dbe5a1207c5b8673a5	28,034,943,200.796027353	2.8035%
8	0x19c73b7e955906ff1d26692c8ec3f93ff654dd7	25,025,600,103.795888693	2.5026%
9	0xe92a00f3bfd5deae4f5e1c3d1b821214e0450e8	25,000,250,000	2.5000%
10	0x9040a3da9a398ce5659dc71dfbb8446e3447734e	25,000,000,000	2.5000%



Contract functions details

+ Context

- [Int] _msgSender

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ Ownable (Context)

- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
- modifiers: onlyOwner

+ [Int] IUniswapV2Factory

- [Ext] createPair #

+ [Int] IUniswapV2Router02

- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidityETH (\$)

+ BMCC (Context, IERC20, Ownable)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Prv] tokenFromReflection
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Prv] _approve #

- [Prv] _transfer #
- [Prv] swapTokensForEth #
 - modifiers: lockTheSwap
- [Prv] sendETHToFee #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _getRValues
- [Prv] _takeTeam #
- [Prv] _reflectFee #
- [Ext] <Fallback> (\$)
- [Ext] openTrading #
 - modifiers: onlyOwner
- [Ext] setMarketingWallet #
- [Ext] excludeFromFee #
- [Ext] includeToFee #
- [Ext] setNoTaxMode #
- [Ext] setTeamFee #
- [Ext] setTaxFee #
- [Pub] setBots #
 - modifiers: onlyOwner
- [Pub] delBot #
 - modifiers: onlyOwner
- [Pub] isBot
- [Ext] manualswap #
- [Ext] manualsend #
- [Pub] thisBalance
- [Pub] amountInPool

(\$)= payable function

= non-constant function

Issues Checking Status

Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Low issues
10. Methods execution permissions.	Passed
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. Out of gas

Issue:

- The function `setBots()` uses the loop to add bots from list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

```
function setBots(address[] memory bots_) public onlyOwner {
    for (uint i = 0; i < bots_.length; i++) {
        if (bots_[i] != uniswapV2Pair && bots_[i] != address(uniswapV2Router)) {
            _bots[bots_[i]] = true;
        }
    }
}
```

Recommendation:

Check that the array length is not too big.

Owner privileges (In the period when the owner is not renounced)

- Owner can open trading.

```
function openTrading() external onlyOwner() {
    require(!tradingOpen, "trading is already open");
    IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(0x10ED43C718714eb63d5aA57B78B54704E256024E);
    uniswapV2Router = _uniswapV2Router;
    _approve(address(this), address(uniswapV2Router), _tTotal);
    uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this), _uniswapV2Router.WETH());
    uniswapV2Router.addLiquidityETH{value: address(this).balance}(address(this), balanceOf(address(this)), 0, 0, owner(), block.timestamp);
    IERC20(uniswapV2Pair).approve(address(uniswapV2Router), type(uint).max);
    tradingOpen = true;
    walletLimitDuration = block.timestamp + (60 minutes);
}
```

- Owner can add and remove bots.

```
function setBots(address[] memory bots_) public onlyOwner {
    for (uint i = 0; i < bots_.length; i++) {
        if (bots_[i] != uniswapV2Pair && bots_[i] != address(uniswapV2Router)) {
            _bots[bots_[i]] = true;
        }
    }
}

function delBot(address notbot) public onlyOwner {
    _bots[notbot] = false;
}
```

- Fee address can change marketing wallet address.

```
function setMarketingWallet (address payable marketingWalletAddress) external {
    require(_msgSender() == _FeeAddress);
    _isExcludedFromFee[_marketingWalletAddress] = false;
    _marketingWalletAddress = marketingWalletAddress;
    _isExcludedFromFee[marketingWalletAddress] = true;
}
```

- Fee address can include in and exclude from fees.

```
function excludeFromFee (address payable ad) external {
    require(_msgSender() == _FeeAddress);
    _isExcludedFromFee[ad] = true;
}

function includeToFee (address payable ad) external {
    require(_msgSender() == _FeeAddress);
    _isExcludedFromFee[ad] = false;
}
```

- Fee address can enable / disable tax mode.

```
function setNoTaxMode(bool onoff) external {
    require(_msgSender() == _FeeAddress);
    _noTaxMode = onoff;
}
```

- Fee address can change team and tax fees.

```
function setTeamFee(uint256 team) external {
    require(_msgSender() == _FeeAddress);
    require(team <= 10);
    _teamFee = team;
}

function setTaxFee(uint256 tax) external {
    require(_msgSender() == _FeeAddress);
    require(tax <= 10);
    _taxFee = tax;
}
```

- Fee address can manually swap contract tokens.

```
function manualswap() external {
    require(_msgSender() == _FeeAddress);
    uint256 contractBalance = balanceOf(address(this));
    swapTokensForEth(contractBalance);
}
```

- Fee address can withdraw half of the contract BTCs to fee address and half to marketing wallet address.

```
function manualsend() external {
    require(_msgSender() == _FeeAddress);
    uint256 contractETHBalance = address(this).balance;
    sendETHToFee(contractETHBalance);
}
```

Conclusion

Smart contracts contain low severity issues and owner privileges!
Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:

<https://bscscan.com/tx/0xe5bf95e4629d0a42da05b450a308c991809087064b40e321af0f39a41eb7f9e8>

Renounce ownership details provided by the team:

<https://bscscan.com/tx/0x8f393df1040f516cd1811d59db467fc29e583186fcb0999a368dd1b3b74b40ee>

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.