



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Biconomic
\$BMB

09/01/2023

TOKEN OVERVIEW

Fees

- Buy fees: 2%
- Sell fees: 3%
- Transfer fees: 5%

Fees privileges

- Can change buy fees up to 49%, sell fees up to 49% and transfer fees up to 49%

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can't change max tx amount or max wallet amount

Blacklist

- Blacklist function not detected

Other privileges

- Can exclude / include from fees
-

TABLE OF CONTENTS

1

DISCLAIMER

2

INTRODUCTION

3-4

AUDIT OVERVIEW

5-7

OWNER PRIVILEGES

8

CONCLUSION AND ANALYSIS

9

TOKEN DETAILS

10

**BICONOMIC TOKEN ANALYTICS &
TOP 10 TOKEN HOLDERS**

11

TECHNICAL DISCLAIMER



DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website <https://freshcoins.io>

FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy (RUG or Honeypot etc)



INTRODUCTION

FreshCoins (Consultant) was contracted by **Biconomic** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0xFCaC04229D2b552fd77075E5bCae27C2D6E5b035

Network: **Binance Smart Chain (BSC)**

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on **09/01/2023**



AUDIT OVERVIEW



Security Score



Static Scan

Automatic scanning for common vulnerabilities



ERC Scan

Automatic checks for ERC's conformance



High



Medium



Low



Optimizations



Informational



| No. | Issue description | Checking Status |
|-----|--------------------------------|-----------------|
| 1 | Compiler Errors / Warnings | Passed |
| 2 | Reentrancy and Cross-function | Passed |
| 3 | Front running | Passed |
| 4 | Timestamp dependence | Passed |
| 5 | Integer Overflow and Underflow | Passed |
| 6 | Reverted DoS | Passed |
| 7 | DoS with block gas limit | Passed |
| 8 | Methods execution permissions | Passed |
| 9 | Exchange rate impact | Passed |
| 10 | Malicious Event | Passed |
| 11 | Scoping and Declarations | Passed |
| 12 | Uninitialized storage pointers | Passed |
| 13 | Design Logic | Passed |
| 14 | Safe Zeppelin module | Passed |

OWNER PRIVILEGES

- **Contract owner can't mint tokens after initial contract deploy**
- **Contract owner can't exclude an address from transactions**
- **Contract owner can exclude/include wallet from tax**

```
function setIsWhitelisted(address account, bool value) external onlyOwner {
    isWhitelisted[account] = value;
    emit SetWhitelisted(account, value);
}
```

- **Contract owner can burn tokens**

```
function burn (uint256 amount_) public onlyOwner {
    _burn (msg.sender, amount_);
}
```

- **Contract owner can send tokens in multiple wallets**

```
function doAirDrop(address[] memory _address, uint256 _amount) onlyOwner public returns (bool) {
    uint256 count = _address.length;

    for (uint256 i = 0; i < count; i++)
    {
        BEP20._transfer(msg.sender, _address [i], _amount);
        emit AirDrop (_address[i], _amount);
    }
    return true;
}
```

- **Contract owner can change taxes wallet recipient**

If the status of the recipient's wallet is true, the prize amount will be sent to that wallet, if not, it will be sent to the token contract address

```
function setRewardWalletOn (bool srwallet) public onlyOwner {
    rewardWalletOn = srwallet;
}
```

- **Contract owner can set wallet as CEX**

```
function setIsCEX(address account, bool value) external onlyOwner {
    isCEX[account] = value;
    emit SetCEX(account, value);
}
```


● Contract owner can set wallet as MM (MarketMaker)

```
function setIsMarketMaker(address account, bool value) external onlyOwner {
    require(account != pair, "Can't modify pair");
    isMarketMaker[account] = value;
    emit SetMarketMaker(account, value);
}
```

● Contract owner can change buy fees up to 49%, sell fees up to 49% and transfer fees up to 49%

```
function setTaxes(uint256 newBuyTax, uint256 newSellTax, uint256 newTransferTax) external onlyOwner {
    require(newBuyTax <= 49 && newSellTax <= 49 && newTransferTax <= 49, "Too high taxes");
    buyTax = newBuyTax;
    sellTax = newSellTax;
    transferTax = newTransferTax;
    emit SetTaxes(buyTax, sellTax, transferTax);
}
```

● Contract owner can change rewardWallet and marketingWallet addresses

Current values:

rewardWallet : 0x6d865fc7cfd8eeec2ecb778a40a64cf98a25d38d

marketingWallet : 0x62f9d9919d3d9e4a778646c6e9d3f0a723a70c2e

```
function setRewardWallet(address newAddress) external onlyOwner {
    require(newAddress != address(0), "New reward pool is the zero address");
    emit SetRewardWallet(newAddress, rewardWallet);
    rewardWallet = newAddress;
}

function setMarketingWallet(address newWallet) external onlyOwner {
    require(newWallet != address(0), "New marketing wallet is the zero address");
    emit SetMarketingWallet(newWallet, marketingWallet);
    marketingWallet = newWallet;
}
```

● Contract owner can withdraw BNB and stuck tokens from smart contract

```
function recoverBNB() external onlyOwner {
    uint256 amount = address(this).balance;
    (bool sent,) = payable(rewardWallet).call{value: amount, gas: transferGas}("");
    require(sent, "Tx failed");
    emit RecoverBNB(amount);
}

function recoverBEP20(IBEP20 token, address recipient) external onlyOwner {
    require(address(token) != address(this), "Can't withdraw Step");
    uint256 amount = token.balanceOf(address(this));
    token.transfer(recipient, amount);
    emit RecoverBEP20(address(token), amount);
}
```

● Contract owner can transfer ownership

```
function transferOwnership(address newOwner) public onlyOwner {  
    require(newOwner != address(0), "Ownable: new owner is the zero address");  
    emit OwnershipTransferred(_owner, newOwner);  
    _owner = newOwner;  
}
```

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. The risk can be prevented by temporarily locking the contract or renouncing ownership.



CONCLUSION AND ANALYSIS



Smart Contracts within the scope were manually reviewed and analyzed with static tools.



Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.



Found 1 HIGH issue during the first review.

TOKEN DETAILS

Details

| | |
|----------------|-----|
| Buy fees: | 2% |
| Sell fees: | 3% |
| Transfer fees: | 5% |
| Max TX: | N/A |
| Max Sell: | N/A |

Honeypot Risk

| | |
|------------------|--------------|
| Ownership: | Owned |
| Blacklist: | Not detected |
| Modify Max TX: | Not detected |
| Modify Max Sell: | Not detected |
| Disable Trading: | Not detected |

Rug Pull Risk

| | |
|------------|-------|
| Liquidity: | N/A |
| Holders: | Clean |



BICONOMIC TOKEN ANALYTICS

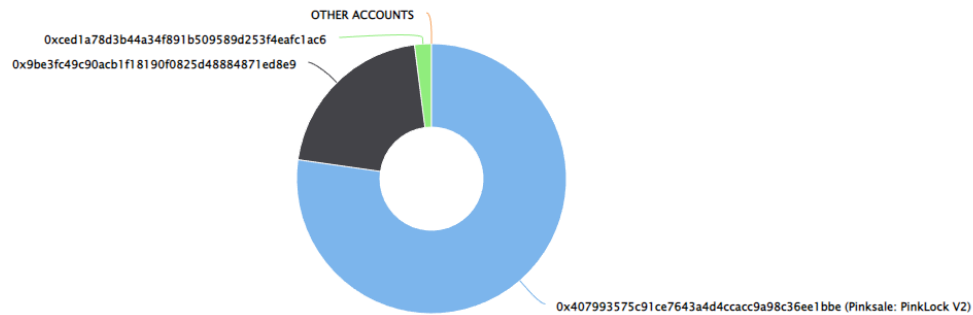
& TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (1,000,000,000.00 Tokens) of Biconomic

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 3

Biconomic Top 10 Token Holders

Source: BscScan.com



(A total of 1,000,000,000.00 tokens held by the top 10 accounts from the total supply of 1,000,000,000.00 token)

| Rank | Address | Quantity (Token) | Percentage |
|------|--|------------------|------------|
| 1 | Pinksale: PinkLock V2 | 772,500,000 | 77.2500% |
| 2 | 0x9be3fc49c90acb1f18190f0825d48884871ed8e9 | 207,354,800 | 20.7355% |
| 3 | 0xcd1a78d3b44a34f891b509589d253f4eafc1ac6 | 20,145,200 | 2.0145% |

0x407993575c91ce7643a4d4ccacc9a98c36ee1bbe
77.25% tokens locked with Pinksale

Lock records

| Wallet | Amount | Cycle(d) | Cycle Release(%) | TGE(%) | Unlock time(UTC) | |
|-------------------------------|-------------|----------|------------------|--------|------------------|----------------------|
| 0x62F9...0C2e | 150,000,000 | 30 | 8 | 4 | 2023.02.14 12:00 | View |
| 0x9Be3...d8E9 | 30,000,000 | - | - | - | 2023.02.20 12:00 | View |
| 0x6d86...d38d | 200,000,000 | - | - | - | 2023.03.14 12:00 | View |
| 0x9Be3...d8E9 | 142,500,000 | 30 | 4 | 4 | 2023.07.14 13:00 | View |
| 0x9Be3...d8E9 | 50,000,000 | - | - | - | 2023.08.14 13:00 | View |
| 0xfa3E...72Dd | 50,000,000 | 30 | 8 | 8 | 2023.09.14 13:00 | View |
| 0x8934...ef2f | 150,000,000 | 30 | 8 | 8 | 2023.12.14 12:00 | View |

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.

