



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



KeySwap
\$KEY



28/02/2022



TABLE OF CONTENTS

- 1 DISCLAIMER
- 2 INTRODUCTION
- 3-4 AUDIT OVERVIEW
- 5-7 OWNER PRIVILEGES
- 8 CONCLUSION AND ANALYSIS
- 9 TOKEN DETAILS
- 10 KEYSWAP 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 KeySwap (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x07b1681C082039551952bDee4A505cecC2FF4998

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 28/02/2022



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 exclude an address from transactions.

Contract owner can mint tokens after initial contract deploy

```
function mint(uint256 amount) external onlyOperator returns (bool) {
    _mint(_msgSender(), amount);
    return true;
}

function _mint(address account, uint256 amount) internal {
    require(account != address(0), "ERC20: mint to the zero address");

    _totalSupply = _totalSupply.add(amount);
    _balances[account] = _balances[account].add(amount);
    emit Transfer(address(0), account, amount);
}
```

Contract owner can exclude/include wallet from tax

```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}
```

Contract owner can exclude/include wallet from blacklist

```
function excludeFromBlacklist(address account) public onlyOwner {
    _blacklist[account] = false;
    emit ExcludedFromBlacklist(account);
}

function includeInBlacklist(address account) public onlyOwner {
    _blacklist[account] = true;
    emit IncludedInBlacklist(account);
}
```

Contract owner can exclude/include wallet from AntiWhales limitations

```
function excludeFromAntiWhales(address account) public onlyOwner {
    _isExcludedFromAntiWhales[account] = true;
    emit ExcludedFromAntiWhales(account);
}

function includeInAntiWhales(address account) public onlyOwner {
    _isExcludedFromAntiWhales[account] = false;
    emit IncludedInAntiWhales(account);
}
```

Contract owner can change _marketingWallet address

Current value:

_marketingWallet : 0xfae0c9848538588c2d3cbba16a8ea9d23581ab6e

```
function setMarketingWallet(address payable newMarketingWallet)
    external
    onlyOwner
{
    require(newMarketingWallet != address(0), "ZERO ADDRESS");
    _marketingWallet = newMarketingWallet;
}
```

Contract owner can change the tax up to 10%

```
uint16 public MaxLiquifyFee = 500; // 30% max
uint16 public MaxMarketingFee = 500; // 30% max

function setAllFeePercent(uint16 liquifyFee, uint16 marketingFee)
    external
    onlyOwner
{
    require(liquifyFee <= MaxLiquifyFee, "Liquidity fee overflow");
    require(marketingFee <= MaxMarketingFee, "Buyback fee overflow");
    _liquifyFee = liquifyFee;
    _marketingFee = marketingFee;
}
```

Contract owner can enable/disable tax on sell

```
bool public _applyFeeOnlyOnSell = false; // Fee is applied only when sell tokens or not

function applyFeeOnlyOnSell(bool flag) external onlyOwner {
    _applyFeeOnlyOnSell = flag;
}
```

Contract owner can change wallet/tx limitations (AntiWhales)

```
function setAntiWhalesConfiguration(
    uint256 maxTxAmount,
    uint256 maxWalletAmount
) external onlyOwner {
    require(
        maxTxAmount >= MAX_TX_AMOUNT_MIN_LIMIT,
        "Max tx amount too small"
    );
    require(
        maxWalletAmount >= MAX_WALLET_AMOUNT_MIN_LIMIT,
        "Max wallet amount too small"
    );
    _maxTxAmount = maxTxAmount;
    _maxWalletAmount = maxWalletAmount;
}
```

Contract owner can change swap settings

```
function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {  
    _swapAndLiquifyEnabled = _enabled;  
}
```

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {  
    emit OwnershipTransferred(_owner, address(0));  
    _owner = address(0);  
}
```

Contract owner can transfer ownership

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

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 no issue during the first review.

TOKEN DETAILS

Details

Buy fees:	5%
Sell fees:	5%
Max TX:	100,000
Max Sell:	N/A

Honeypot Risk

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

Rug Pull Risk

Liquidity:	N/A
Holders:	Clean



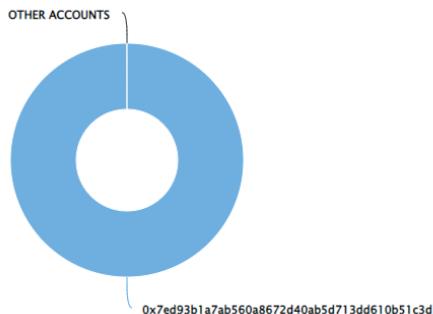
KEYSWAP TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

💡 The top 10 holders collectively own 100.00% (20,000,000.00 Tokens) of KeySwap

💡 Token Total Supply: 20,000,000.00 Token | Total Token Holders: 1

KeySwap Top 10 Token Holders

Source: BscScan.com



(A total of 20,000,000.00 tokens held by the top 10 accounts from the total supply of 20,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x7ed93b1a7ab560a8672d40ab5d713dd610b51c3d	20,000,000	100.0000%

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.

