



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



House of the Dragon
\$HOTD

14/04/2024



TOKEN OVERVIEW

Fees

- Buy fees: 4%
- Sell fees: 4%

Fees privileges

- Can change fees up to 25%

Ownership

- Owned

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

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

Blacklist

- Blacklist function not detected

Other privileges

- Can exclude / include from fees
-

TABLE OF CONTENTS

1

DISCLAIMER

2

INTRODUCTION

3

WEBSITE + SOCIALS

4-5

AUDIT OVERVIEW

6-8

OWNER PRIVILEGES

9

CONCLUSION AND ANALYSIS

10

TOKEN DETAILS

11

HOTD TOKEN ANALYTICS &
TOP 10 TOKEN HOLDERS

12

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 **House of the Dragon** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x30605912092F18E4f60dA5AE71Ed1BD92Ea9Cd5A

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 **14/04/2024**



WEBSITE DIAGNOSTIC

<http://houseofthedragontoken.com>



0-49



50-89



90-100



Performance



Accessibility



Best
Practices



SEO



Progressive
Web App

Socials



Twitter

<https://twitter.com/HOTDragonToken>



Telegram

<https://t.me/HotDragonToken>

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(s) from tax**

```
function excludeFromFees(address account) external onlyOwner {
    require(
        !_isExcludedFromFees[account],
        "BABYTOKEN: Account is already excluded"
    );
    _isExcludedFromFees[account] = true;

    emit ExcludeFromFees(account);
}

function excludeMultipleAccountsFromFees(address[] calldata accounts)
    external
    onlyOwner
{
    for (uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromFees[accounts[i]] = true;
    }

    emit ExcludeMultipleAccountsFromFees(accounts);
}
```

- **Contract owner can exclude/include wallet from dividends**

```
function excludeFromDividends(address account) external onlyOwner {
    require(!excludedFromDividends[account]);
    excludedFromDividends[account] = true;

    _setBalance(account, 0);
    tokenHoldersMap.remove(account);

    emit ExcludeFromDividends(account);
}
```

- **Contract owner can change swap settings**

```
function setSwapTokensAtAmount(uint256 amount) external onlyOwner {
    require(
        amount > totalSupply() / 10**5,
        "BABYTOKEN: Amount must be greater than 0.001% of total supply"
    );
    swapTokensAtAmount = amount;
}
```

● Contract owner can change fees up to 25%

```
function setTokenRewardsFee(uint256 value) external onlyOwner {
    tokenRewardsFee = value;
    totalFees = tokenRewardsFee.add(liquidityFee).add(marketingFee);
    require(totalFees <= 25, "Total fee is over 25%");
}

function setLiquidityFee(uint256 value) external onlyOwner {
    liquidityFee = value;
    totalFees = tokenRewardsFee.add(liquidityFee).add(marketingFee);
    require(totalFees <= 25, "Total fee is over 25%");
}

function setMarketingFee(uint256 value) external onlyOwner {
    marketingFee = value;
    totalFees = tokenRewardsFee.add(liquidityFee).add(marketingFee);
    require(totalFees <= 25, "Total fee is over 25%");
}
```

● Contract owner can change `_marketingWalletAddress` address

Current value:

`_marketingWalletAddress`: `0xF76C084FfFf4B2BE2b21d71AC7C06829d02DE1F5`

```
function setMarketingWallet(address payable wallet) external onlyOwner {
    require(
        wallet != address(0),
        "BABYTOKEN: The marketing wallet cannot be the value of zero"
    );
    require(!wallet.isContract(), "Marketing wallet cannot be a contract");
    _marketingWalletAddress = wallet;
}
```

● Contract owner can transfer ownership

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

function _setOwner(address newOwner) private {
    address oldOwner = _owner;
    _owner = newOwner;
    emit OwnershipTransferred(oldOwner, newOwner);
}
```

● Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
    _setOwner(address(0));
}
```

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 no HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees: 4%

Sell fees: 4%

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: 100% unlocked tokens



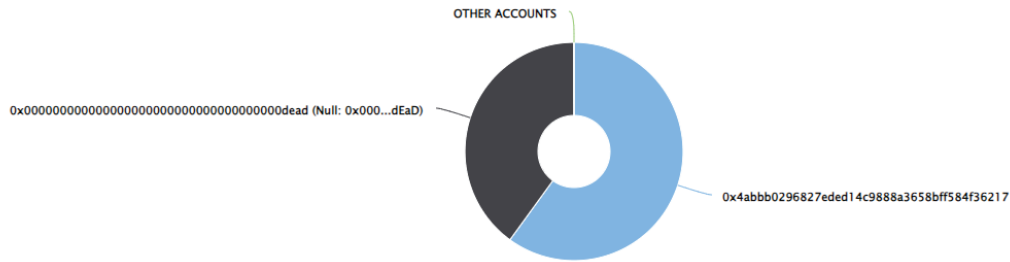
HOTD TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00%
(100,000,000,000,000.00 Tokens) of House of the Dragon

Token Total Supply: 100,000,000,000,000.00 Token | Total Token Holders: 2

House of the Dragon Top 10 Token Holders

Source: BscScan.com



(A total of 100,000,000,000,000.00 tokens held by the top 10 accounts from the total supply of 100,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x4abBB029...584f36217	60,000,000,000,000	60.0000%
2	Null: 0x000...dEaD	40,000,000,000,000	40.0000%

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.

