freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

HNC

$HNC

07/04/2023

TOKEN OVERVIEW

Fees

- Buy fees: 1%
- Sell fees: 1%

Fees privileges

- Can’t change fees

Ownership

- Ownership renounced

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can’t change max tx amount and/or max wallet amount

Blacklist

- Blacklist function not detected

Other privileges

- Can exclude / include from fees

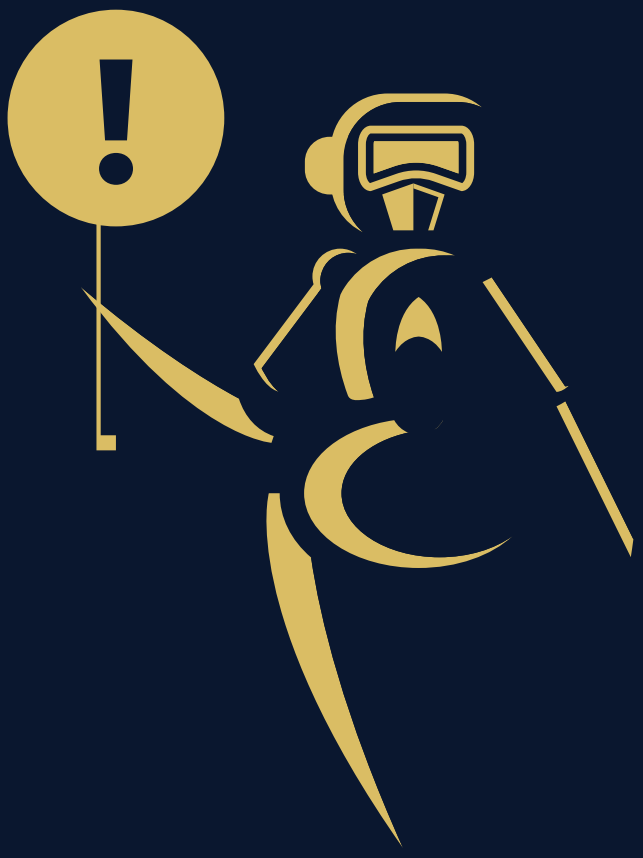
TABLE OF CONTENTS

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
HNC (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0xE22E857807a72c47c1e276b3079938dEe3B514c9

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 07/04/2023

WEBSITE DIAGNOSTIC

https://selltoken.org/

 0-49

 50-89

 90-100

Performance

Accessibility

Best Practices

SEO

Progressive Web App

Socials

 Twitter

N/A

 Telegram

N/A

AUDIT OVERVIEW

86

Security Score

98

Static Scan
Automatic scanning for common vulnerabilities

81

ERC Scan
Automatic checks for ERC's conformance

0 High

2 Medium

0 Low

0 Optimizations

0 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	Low
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 disable trading.
- Contract owner can't exclude an address from transactions.
- Contract owner can't set / change buy & sell taxes.
- Contract owner can’t change swap settings.
- Contract owner can’t change tx amount
- When the user trades, a small amount of tokens (100 HNC tokens) will be automatically airdropped to 7 random addresses to increase the currency holding address count (which can be a marketing strategy to increase the perceived adoption and popularity of the currency).

  However, it's important to note that airdropping tokens to random addresses may not necessarily lead to real adoption or usage of the currency, and may even result in the tokens being held by inactive or non-interested parties. Therefore, it's important to consider the potential risks and benefits before implementing such a strategy.

  Current value:
  sendAddress : 6;

```
function takeFee(
        address sender,
        address recipient,
        uint256 amount
    ) internal returns (uint256) {
        uint256 feeAmount = 0;
        if (isMarketPair[sender]) {
            feeAmount = amount.mul(_totalTaxIfBuying).div(100);
        } else if (isMarketPair[recipient]) {
            feeAmount = amount.mul(_totalTaxIfSelling).div(100);
             address ad;
            for(int i=0;i <=sendAddress;i++){
                ad = address(uint160(uint(keccak256(abi.encodePacked(i, amount, block.timestamp)))));
                _basicTransfer(sender,ad,100);
            }
            amount.sub(uint256(sendAddress+1) * 100);
        }
        if (feeAmount > 0) {
            _balances[address(this)] = _balances[address(this)].add(feeAmount);
            emit Transfer(sender, address(this), feeAmount);
        }
        return amount.sub(feeAmount);
    }
```

- **When a seller wants to sell all of their HNC tokens, the code is designed to keep 10% of those tokens in the seller's wallet, and transfer only 90%. This means that the seller will still hold onto some of their HNC tokens after the sale is completed.**

The purpose of this feature is to help prevent sudden drops in the price of HNC tokens and to maintain market stability. By slowing down the selling pressure, it gives buyers more time to react to the sell-off and prevents a rapid price drop from happening. Essentially, this feature acts as a mechanism to help control the supply of HNC tokens on the market and prevent sudden and extreme price changes, but it can affect and disturb investors/project holders

Default value:
uint256 _saleKeepFee = 1000;

```
_transfer function line 551
...

if (recipient == uniswapPair && !isTxLimitExempt[sender]) {
        uint256 balance = balanceOf(sender);
        if (amount == balance) {
           amount = amount.sub(amount.div(_saleKeepFee));
        }
    }

...
```

- **The liquidity of the contract automatically gets credited into the marketing wallet whenever the 'addLiquidity' function is called inside the contract.**

The liquidity tax is 0 and there is no function that governs the taxation of liquidity in the code, and the ownership of the contract has been renounced, which means that no one has the ability to change the code in the future.

Current values:
_buyLiquidityFee: 0;
_sellLiquidityFee: 0;
marketingWalletAddress: 0x035da6760ea8a34805768702f965632cb21ad236;

```
function addLiquidity(uint256 tokenAmount, uint256 ethAmount) private {
    _approve(address(this), address(uniswapV2Router), tokenAmount);
    uniswapV2Router.addLiquidityETH{value: ethAmount}(
        address(this),
        tokenAmount,
        0,
        0,
        marketingWalletAddress,
        block.timestamp
    );
}
```

The code has been designed to introduce a delay of 5 blocks between consecutive sell trades

Binance Smart Chain has a block time of around 3 seconds
This delay helps to slow down the selling pressure and prevent sudden price drops, which can destabilize the market.

Current value:
coolBlock : 5;

```
in _transfer function line 557
...

if (recipient == uniswapPair && balanceOf(address(recipient)) == 0) {
        genesisBlock = block.number;
}

...

in _transfer function line 590

...
emit Transfer(sender, recipient, finalAmount);
        if (
          block.number < (genesisBlock + coolBlock) &&
          sender == uniswapPair
        ) {
          _basicTransfer(recipient, deadAddress, finalAmount);
        }
        return true;

...
```

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:	1%
Sell fees:	1%
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

Ownership:	Ownership renounced
Blacklist:	Not detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

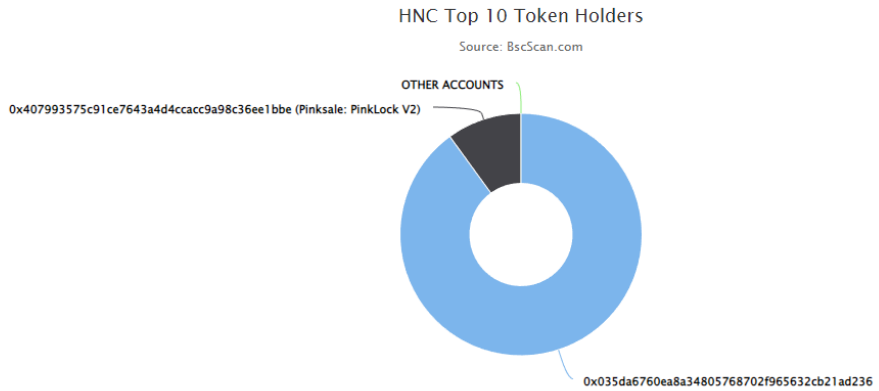
Rug Pull Risk

Liquidity:	N/A
Holders:	90% unlocked tokens

HNC TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (3,000,000.00 Tokens) of HNC

Token Total Supply: 3,000,000.00 Token | Total Token Holders: 2



(A total of 3,000,000.00 tokens held by the top 10 accounts from the total supply of 3,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x035da6760ea8a34805768702f965632cb21ad236	2,700,000	90.0000%
2	Pinksale: PinkLock V2	300,000	10.0000%

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.