freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

SNAIL COIN V2

$SNAIL V2

SNAIL v2

FROM MEME, TO FUTURE.

24/07/2022

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
SNAIL COIN V2 (Customer) to conduct a Smart Contract Code Review and
Security Analysis.

0x7b89778d911a01570327b0FC1EA6096440998F2b

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 24/07/2022

AUDIT OVERVIEW

98

Security Score

98 Static Scan
Automatic scanning for
common vulnerabilities

98 ERC Scan
Automatic checks for
ERC's conformance

0 High

0 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	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

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

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

Contract owner can renounce ownership

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

Contract owner can transfer ownership

```solidity
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:	6%
Sell fees:	6%
Max TX:	20,000,000,000
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

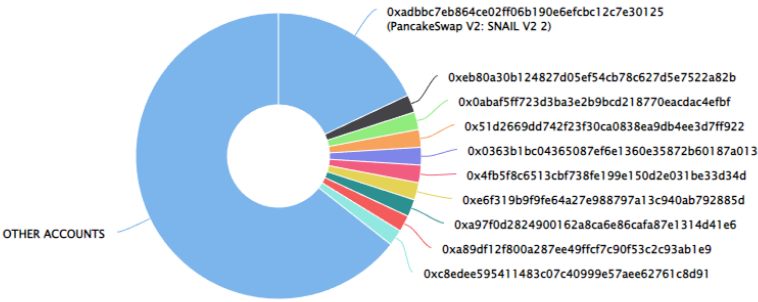|	
Liquidity:	N/A
Holders:	Clean

SNAIL COIN V2 TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 35.61% (356,087,423,470.89 Tokens) of SNAIL COIN V2 | Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 418

SNAIL COIN V2 Top 10 Token Holders
Source: BscScan.com

0xadbbc7eb864ce02ff06b190e6efcbc12c7e30125
(PancakeSwap V2: SNAIL V2 2)

0xeb80a30b124827d05ef54cb78c627d5e7522a82b

0x0abaf5ff723d3ba3e2b9bcd218770eacdac4efbf

0x51d2669dd742f23f30ca0838ea9db4ee3d7ff922

0x0363b1bc04365087ef6e1360e35872b60187a013

0x4fb5f8c6513cbf738fe199e150d2e031be33d34d

0xe6f319b9f9fe64a27e988797a13c940ab792885d

0xa97f0d2824900162a8ca6e86cafa87e1314d41e6

0xa89df12f800a287ee49ffcf7c90f53c2c93ab1e9

0xc8edee595411483c07c40999e57aee62761c8d91

OTHER ACCOUNTS

(A total of 356,087,423,470.89 tokens held by the top 10 accounts from the total supply of 1,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	📄 PancakeSwap V2: SNAIL V2 2	180,268,578,460.151955795	18.0269%
2	0xeb80a30b124827d05ef54cb78c627d5e7522a82b	20,000,000,000	2.0000%
3	0x0abaf5ff723d3ba3e2b9bcd218770eacdac4efbf	19,999,986,520.998720125	2.0000%
4	0x51d2669dd742f23f30ca0838ea9db4ee3d7ff922	19,997,212,745.54836551	1.9997%
5	0x0363b1bc04365087ef6e1360e35872b60187a013	19,951,007,965.88	1.9951%
6	0x4fb5f8c6513cbf738fe199e150d2e031be33d34d	19,928,000,000	1.9928%
7	0xe6f319b9f9fe64a27e988797a13c940ab792885d	19,562,485,617.540737117	1.9562%
8	0xa97f0d2824900162a8ca6e86cafa87e1314d41e6	19,520,774,378.080298743	1.9521%
9	0xa89df12f800a287ee49ffcf7c90f53c2c93ab1e9	18,538,447,250.289482296	1.8538%
10	0xc8edee595411483c07c40999e57aee62761c8d91	18,320,930,532.400760966	1.8321%

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.