freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

planetcryptos

$PLC

21/02/2023

TOKEN OVERVIEW

Fees

- Buy fees: N/A
- Sell fees: N/A

Fees privileges

- Can’t change / set fees

Ownership

- Owned

Minting

- Mint function detected

Max Tx Amount / Max Wallet Amount

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

Blacklist

- No blacklist function detected

Other privileges

- N/A

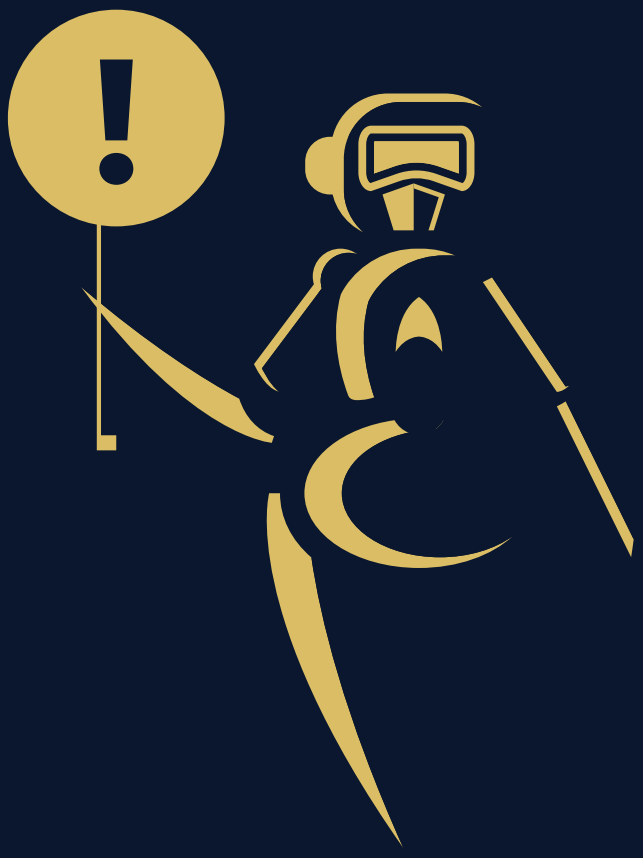
TABLE OF CONTENTS

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

0xd2EcdcA39bBd8B4DD456780A542a4f9DE575313C

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 21/02/2023

AUDIT OVERVIEW

72

Security Score

93

Static Scan

Automatic scanning for common vulnerabilities

88

ERC Scan

Automatic checks for ERC's conformance

2 High

1 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 mint tokens after initial contract deploy

```
function _mint(address account, uint256 amount) internal override onlyOwner {
    super._mint(account, amount);
}

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

    _beforeTokenTransfer(address(0), account, amount);

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

Contract owner can burn tokens from any wallet

```
function burn(uint256 amount) public virtual {
    _burn(_msgSender(), amount);
}

function burnFrom(address account, uint256 amount) public virtual {
    uint256 currentAllowance = allowance(account, _msgSender());
    require(currentAllowance >= amount, "ERC20: burn amount exceeds allowance");
    _approve(account, _msgSender(), currentAllowance - amount);
    _burn(account, amount);
}
```

Contract owner can withdraw stuck tokens from smart contract

```
function recoverToken(address tokenAddress, uint256 tokenAmount) public virtual onlyOwner {
    IERC20(tokenAddress).transfer(owner(), tokenAmount);
}
```

Contract owner can transfer ownership

```
function transferOwnership(address newOwner) public virtual onlyOwner {
    require(newOwner != address(0), "ERC20Ownable: new owner is the zero address");
    emit OwnershipTransferred(_owner, newOwner);
    _owner = newOwner;
}
```

Contract owner can renounce ownership

```
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = 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 2 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	N/A
Sell fees:	N/A
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

Others

Liquidity:	N/A
Holders:	Clean

PLC TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00%
(99,999,999,857,114,000,000,000.00 Tokens) of planetcryptos

Token Total Supply: 100,000,000,000,000,000,000,000.00 Token | Total Token Holders: 1,416

(A total of 99,999,999,857,114,000,000,000.00 tokens held by the top 10 accounts from the total supply of 100,000,000,000,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	99,745,452,021,863,949,305,105.73487457535011081	99.7455%
2	0x74f3a9b5c67562ab988c23ea0c177f0238914bd4	254,444,446,090,000,004,997	0.2544%
3	0x3be0c5d31958dd4c96a600dab767e5b42939c178	50,051,279,730,858,493.510310206811191171	0.0001%
4	0x78b7a0cd46149619c3e4f4353954d7a204c5fffc	50,000,000,000,000,000	0.0001%
5	0x3223cc0e772fc268254609fbac1f5645ca92a542	1,896,477,967,580,000	0.0000%
6	0x2af715e1743fd7de940c14bddfbcfb28aa4ee4e0	1,010,010,010,000,000	0.0000%
7	0x59ad938a507b45b8ada6b40de744fb377d7f7c0b	173,647,398,958,410.503801512103335342	0.0000%
8	PancakeSwap V2: PLC 30	127,987,447,931,503.054098614837901301	0.0000%
9	0xd6571da7e930404751fe5614853145080231a937	93,424,284,202,493.400527807334081933	0.0000%
10	0x70f8117b822a3ea1a269f5cb2ec3ebc2a7f958b3	36,333,257,280,627.306570274548363431	0.0000%

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.