freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

ClanBit

$ClanBit

01/07/2025

AUDIT REPORT

TOKEN OVERVIEW

Fees

- Buy fees: 0%
- Sell fees: 0%

Fees privileges

- Can’t change fees

Ownership

- N/A

Minting

- Mint function not detected

Max Tx Amount / Max Wallet Amount

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

Blacklist

- Blacklist function not detected

Other privileges

- N/A

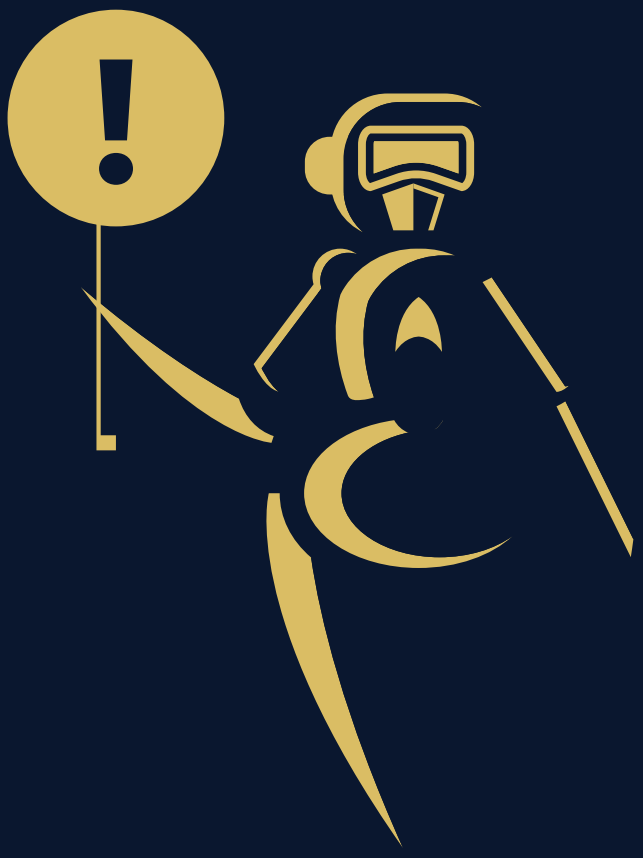
TABLE OF CONTENTS

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

0x830fC5915D6aD75BB7C975fbE26050B3EE1F78ac

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 01/07/2025

WEBSITE DIAGNOSTIC

https://clanbit.xyz

0-49 50-89 90-100

Performance Accessibility Best Practices SEO Progressive Web App

Socials

X (Twitter)

https://x.com/clanbitx

Telegram

https://t.me/clanbitgame

AUDIT OVERVIEW

92

Security Score

94

Static Scan
Automatic scanning for common vulnerabilities

90

ERC Scan
Automatic checks for ERC's conformance

0 High

2 Medium

1 Low

2 Optimizations

0 Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Low
3	Front running	Low
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 & FINDINGS

Missing increaseAllowance / decreaseAllowance Methods

The contract does not implement increaseAllowance and decreaseAllowance functions, which are commonly used to safely manage allowances and prevent potential issues caused by setting allowances manually.

Approve Front-Running Vulnerability

The standard approve() function can be exploited in a front-running attack, where a spender could quickly use the old allowance before the new one is applied, leading to unexpected fund transfers. Use the pattern:

```
require(allowance[msg.sender][spender] == 0 || value == 0, "Set to zero first");
```

No Ownership or Access Control

The contract lacks an ownership or access control mechanism. This is not a direct vulnerability for a simple ERC-20, but can limit extensibility (e.g., if upgrades or admin controls are later needed).

No EIP-2612 permit() Support

The contract does not support permit() from EIP-2612, which allows gasless approvals using signatures (common in DeFi).

Missing SafeMath

The contract does not use SafeMath. While Solidity 0.8+ has built-in overflow checks, using SafeMath can still improve code readability and safety perceptions.

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:	0%
Sell fees:	0%
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

Ownership:	N/A
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

CLANBIT TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 100.00% (21,000,000.00 Tokens) of ClanBit

Token Total Supply: 21,000,000.00 Token | Total Token Holders: 1

(A total of 21,000,000.00 tokens held by the top 10 accounts from the total supply of 21,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xE144b27E...b247d8Cc8	21,000,000	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.