Smart Contract
Security Audit Report

The SlowMist Security Team received the Chainbase Network team's application for smart contract security audit of the Chainbase OFT on 2025.06.24. The following are the details and results of this smart contract security audit:

Token Name :

Chainbase OFT

The contract address :

ChainbaseOFT:

https://bscscan.com/address/0xc32cc70741c3a8433dcbcb5ade071c299b55ffc8

ChainbaseOFTAdapter:

https://basescan.org/address/0x3ade69d08ac3c7c0cc3654eeedbe899f109f7181

The audit items and results :

(Other unknown security vulnerabilities are not included in the audit responsibility scope)

NO.	Audit Items	Result
1	Replay Vulnerability	Passed
2	Denial of Service Vulnerability	Passed
3	Race Conditions Vulnerability	Passed
4	Authority Control Vulnerability Audit	Passed
5	Integer Overflow and Underflow Vulnerability	Passed
6	Gas Optimization Audit	Passed
7	Design Logic Audit	Passed
8	Uninitialized Storage Pointers Vulnerability	Passed
9	Arithmetic Accuracy Deviation Vulnerability	Passed
10	"False top-up" Vulnerability	Passed
11	Malicious Event Log Audit	Passed
12	Scoping and Declarations Audit	Passed

NO.	Audit Items	Result
13	Safety Design Audit	Passed
14	Non-privacy/Non-dark Coin Audit	Passed

Audit Result : Passed

Audit Number : 0X002506250002

Audit Date : 2025.06.24 - 2025.06.25

Audit Team : SlowMist Security Team

Summary conclusion : This is an OFT contract and an OFTAdapter contract that does not contain the dark coin functions. The total amount of contract tokens remains unchanged in the ChainbaseOFTAdapter contract. The contract does not have the Overflow and the Race Conditions issue.

The source code:

ChainbaseOFT.sol

```solidity
// SPDX-License-Identifier: UNLICENSED
//SlowMist// The contract does not have the Overflow and the Race Conditions issue
pragma solidity ^0.8.22;

import { OFT } from "@layerzerolabs/oft-evm/contracts/OFT.sol";
import { Ownable } from "@openzeppelin/contracts/access/Ownable.sol";

contract ChainbaseOFT is OFT {
    constructor(
        string memory _name,
        string memory _symbol,
        address _lzEndpoint,
        address _delegate
    ) OFT(_name, _symbol, _lzEndpoint, _delegate) Ownable(_delegate) {}
}
```

ChainbaseOFTAdapter.sol

```solidity
// SPDX-License-Identifier: UNLICENSED
//SlowMist// The contract does not have the Overflow and the Race Conditions issue
pragma solidity ^0.8.22;
```

```solidity
import { OFTAdapter } from "@layerzerolabs/oft-evm/contracts/OFTAdapter.sol";
import { Ownable } from "@openzeppelin/contracts/access/Ownable.sol";

contract ChainbaseOFTAdapter is OFTAdapter {
    constructor(
        address _token,
        address _lzEndpoint,
        address _owner
    ) OFTAdapter(_token, _lzEndpoint, _owner) Ownable(_owner) {}
}
```

Statement

SlowMist issues this report with reference to the facts that have occurred or existed before the issuance of this report, and only assumes corresponding responsibility based on these.

For the facts that occurred or existed after the issuance, SlowMist is not able to judge the security status of this project, and is not responsible for them. The security audit analysis and other contents of this report are based on the documents and materials provided to SlowMist by the information provider till the date of the insurance report (referred to as "provided information"). SlowMist assumes: The information provided is not missing, tampered with, deleted or concealed. If the information provided is missing, tampered with, deleted, concealed, or inconsistent with the actual situation, the SlowMist shall not be liable for any loss or adverse effect resulting therefrom. SlowMist only conducts the agreed security audit on the security situation of the project and issues this report. SlowMist is not responsible for the background and other conditions of the project.

SLOWMIST

Official Website

www.slowmist.com

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

Github

https://github.com/slowmist