



# **Smart contract security audit report**



**Audit Number:** 202101121113

**Report Query Name:** FC-BlackHold

**Smart Contract Info:**

Smart Contract Name	Smart Contract Address	Smart Contract Address Link
BlackHold	TWJQjqQw7Y5qtL2VVHADPEKy WGvcQFiBQz	<a href="https://tronscan.io/#/contract/TWJQjqQw7Y5qtL2VVHADPEKyWGvcQFiBQz/code">https://tronscan.io/#/contract/TWJQjqQw7Y5qtL2VVHADPEKyWGvcQFiBQz/code</a>

**Start Date:** 2021.01.08

**Completion Date:** 2021.01.12

**Overall Result:** Pass

**Audit Team:** Beosin (Chengdu LianAn) Technology Co. Ltd.

### Audit Categories and Results:

No.	Categories	Subitems	Results
1	Coding Conventions	Compiler Version Security	Pass
		Deprecated Items	Pass
		Redundant Code	Pass
		SafeMath Features	Pass
		require/assert Usage	Pass
		Gas Consumption	Pass
		Visibility Specifiers	Pass
2	General Vulnerability	Fallback Usage	Pass
		Integer Overflow/Underflow	Pass
		Reentrancy	Pass
		Pseudo-random Number Generator (PRNG)	Pass

		Transaction-Ordering Dependence	Pass
		DoS (Denial of Service)	Pass
		Access Control of Owner	Pass
		Low-level Function (call/delegatecall) Security	Pass
		Returned Value Security	Pass
		tx.origin Usage	Pass
		Replay Attack	Pass
		Overriding Variables	Pass
3	Business Security	Business Logics	Pass
		Business Implementations	Pass

Note: Audit results and suggestions in code comments

Disclaimer: This audit is only applied to the type of auditing specified in this report and the scope of given in the results table. Other unknown security vulnerabilities are beyond auditing responsibility. Beosin (Chengdu LianAn) Technology only issues this report based on the attacks or vulnerabilities that already existed or occurred before the issuance of this report. For the emergence of new attacks or vulnerabilities that exist or occur in the future, Beosin (Chengdu LianAn) Technology lacks the capability to judge its possible impact on the security status of smart contracts, thus taking no responsibility for them. The security audit analysis and other contents of this report are based solely on the documents and materials that the contract provider has provided to Beosin (Chengdu LianAn) Technology before the issuance of this report, and the contract provider warrants that there are no missing, tampered, deleted; if the documents and materials provided by the contract provider are missing, tampered, deleted, concealed or reflected in a situation that is inconsistent with the actual situation, or if the documents and materials provided are changed after the issuance of this report, Beosin (Chengdu LianAn) Technology assumes no responsibility for the resulting loss or adverse effects. The audit report issued by Beosin (Chengdu LianAn) Technology is based on the documents and materials provided by the contract provider, and relies on the technology currently possessed by Beosin (Chengdu LianAn). Due to the technical limitations of any organization, this report conducted by Beosin (Chengdu LianAn) still has the possibility that the entire risk cannot be completely detected. Beosin (Chengdu LianAn) disclaims any liability for the resulting losses.

The final interpretation of this statement belongs to Beosin (Chengdu LianAn).

## Audit Results Explained:

Beosin (Chengdu LianAn) Technology has used several methods including Formal Verification, Static Analysis, Typical Case Testing and Manual Review to audit three major aspects of smart contracts project FC-BlackHold, including Coding Standards, Security, and Business Logic. **The FC-BlackHold project passed all audit items. The overall result is Pass (Distinction). The smart contract is able to function properly.** Immediate update is required to mitigate security risks. The smart contract is able to function properly only the possible operations mentioned above should be noticed.

## Audit Contents:

### 1. Coding Conventions

Check the code style that does not conform to Solidity code style.

#### 1.1 Compiler Version Security

- Description: Check whether the code implementation of current contract contains the exposed solidity compiler bug.
- Result: Pass

#### 1.2 Deprecated Items

- Description: Check whether the current contract has the deprecated items.
- Result: Pass

#### 1.3 Redundant Code

- Description: Check whether the contract code has redundant codes.
- Result: Pass

#### 1.4 SafeMath Features

- Description: Check whether the SafeMath has been used. Or prevents the integer overflow/underflow in mathematical operation.
- Result: Pass

#### 1.5 require/assert Usage

- Description: Check the use reasonability of 'require' and 'assert' in the contract.
- Result: Pass

#### 1.6 Gas Consumption

- Description: Check whether the gas consumption exceeds the block gas limitation.
- Result: Pass



### 1.7 Visibility Specifiers

- Description: Check whether the visibility conforms to design requirement.
- Result: Pass

### 1.8 Fallback Usage

- Description: Check whether the Fallback function has been used correctly in the current contract.
- Result: Pass

## 2. General Vulnerability

Check whether the general vulnerabilities exist in the contract.

### 2.1 Integer Overflow/Underflow

- Description: Check whether there is an integer overflow/underflow in the contract and the calculation result is abnormal.
- Result: Pass

### 2.2 Reentrancy

- Description: An issue when code can call back into your contract and change state, such as withdrawing ETH.
- Result: Pass

### 2.3 Pseudo-random Number Generator (PRNG)

- Description: Whether the results of random numbers can be predicted.
- Result: Pass

### 2.4 Transaction-Ordering Dependence

- Description: Whether the final state of the contract depends on the order of the transactions.
- Result: Pass

### 2.5 DoS (Denial of Service)

- Description: Whether exist DoS attack in the contract which is vulnerable because of unexpected reason.
- Result: Pass

### 2.6 Access Control of Owner

- Description: Whether the owner has excessive permissions, such as malicious issue, modifying the balance of others.
- Result: Pass

### 2.7 Low-level Function (call/delegatecall) Security



- Description: Check whether the usage of low-level functions like call/delegatecall have vulnerabilities.

- Result: Pass

## 2.8 Returned Value Security

- Description: Check whether the function checks the return value and responds to it accordingly.

- Result: Pass

## 2.9 tx.origin Usage

- Description: Check the use secure risk of 'tx.origin' in the contract. In this project, the contract

- Result: Pass

## 2.10 Replay Attack

- Description: Check the weather the implement possibility of Replay Attack exists in the contract.

- Result: Pass

## 2.11 Overriding Variables

- Description: Check whether the variables have been overridden and lead to wrong code execution.

- Result: Pass

# 3. Business Security

## 3.1 Business analysis of Contract BlackHold

### (1) Query the balance of specified TRC20 tokens function

- Description: As shown in the figure below, the contract implements the *balanceOf* function to query the number of tokens destroyed to the address of this contract. After the tokens are sent to this contract, they cannot be transferred out and are regarded as destroyed. Users can query the number of specified tokens sent to this contract for destruction.

```
C: > Users > deft > Desktop > fc_trxpool(1) > BlackHold.sol
1  pragma solidity ^0.5.8;
2
3  interface ITRC20 {
4      function balanceOf(address account) external view returns (uint256);
5  }
6  contract BlackHold {
7      function balanceOf(address tokenAddr) public view returns (uint256) {
8          return ITRC20(tokenAddr).balanceOf(address(this));
9      }
10 }
```

Figure 13 source code of *balanceOf*

- Result: Pass

#### 4. Conclusion

Beosin(ChengduLianAn) conducted a detailed audit on the design and code implementation of the smart contracts project FC-BlackHold. The problems found by the audit team during the audit process have been notified to the project party and fixed, the overall audit result of the FC-BlackHold project's smart contract is **Pass**.



# BEOSIN

Blockchain Security

## **Official Website**

<https://lianantech.com>

## **E-mail**

[vaas@lianantech.com](mailto:vaas@lianantech.com)

## **Twitter**

[https://twitter.com/Beosin\\_com](https://twitter.com/Beosin_com)