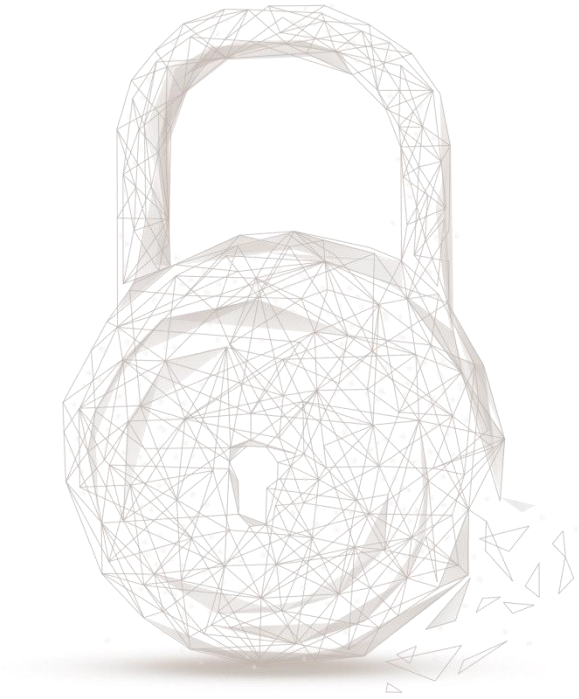
成都链安
BEOSIN

Smart contract security audit report



Audit Number：202008191939

Smart Contract Name：

dcocos.finance (dCOCOS)

Smart Contract Address Link：

https://github.com/dcocos-finance/dCocosToken.git

Commit Hash：

0688ff7462bdd72499467eb5fcfbf54102b87c0c

Start Date：2020.08.13

Completion Date：2020.08.19

Overall Result：Pass（Distinction）

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

Audit Categories and Results:

No.	Categories	Subitems	Results
1	Coding Conventions	ERC20 Token Standards	Pass
		Compiler Version Security	Pass
		Visibility Specifiers	Pass
		Gas Consumption	Pass
		SafeMath Features	Pass
		Fallback Usage	Pass
		tx.origin Usage	Pass
		Deprecated Items	Pass
		Redundant Code	Pass
		Overriding Variables	Pass
2	Function Call Audit	Authorization of Function Call	Pass
		Low-level Function (call/delegatecall) Security	Pass
		Returned Value Security	Pass
		selfdestruct Function Security	Pass

3	Business Security	Access Control of Owner	Pass
		Business Logics	Pass
		Business Implementations	Pass
4	Integer Overflow/Underflow	-	Pass
5	Reentrancy	-	Pass
6	Exceptional Reachable State	-	Pass
7	Transaction-Ordering Dependence	-	Pass
8	Block Properties Dependence	-	Pass
9	Pseudo-random Number Generator (PRNG)	-	Pass
10	DoS (Denial of Service)	-	Pass
11	Token Vesting Implementation	-	**Missing**
12	Fake Deposit	-	Pass
13	event security	-	Pass

Note: Audit results and suggestions in code comments

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 contract dCOCOS, including Coding Standards, Security, and Business Logic. **dCOCOS contract passed all audit items. The overall result is Pass (Distinction). The smart contract is able to function properly.** Please find below the basic information of the smart contract:

1、Basic Token Information

Token name	dcocos.finance
Token symbol	dCOCOS
decimals	18
totalSupply	Initial supply is 0 (Mintable without cap; corresponding contract CocosGateway set a changeable cap is 2.4 billion)
Token type	ERC20

Table 1 – Basic Token Information

2、Token Vesting Information

Missing

Audited Source Code with Comments:

```
pragma solidity ^0.5.0; // Beosin (Chengdu LianAn) // Fixing compiler version is recommended.

import '@openzeppelin/contracts/token/ERC20/ERC20.sol';
import '@openzeppelin/contracts/token/ERC20/ERC20Detailed.sol';

/// @title dCocosToken Contract
/// For more information about this token please visit https://dcocos.finance
/// @author reedhong



contract dCOCOS is ERC20, ERC20Detailed {

  address public governance; // Beosin (Chengdu LianAn) // Declare the variable 'governance' for storing governance address.
  mapping (address => bool) public minters; // Beosin (Chengdu LianAn) // Declare the mapping variable 'minters' for storing minter role of corresponding address.
  // Beosin (Chengdu LianAn) // Constructor, initialize token basic information and governance address.
  constructor () public ERC20Detailed("dcocos.finance", "dCOCOS", 18) {
      governance = tx.origin;
  }
  // Beosin (Chengdu LianAn) // The function 'mint' for mint tokens.
  function mint(address account, uint256 amount) public {
      require(minters[msg.sender], "!minter"); // Beosin (Chengdu LianAn) // Require the caller has the minter role.
      _mint(account, amount); // Beosin (Chengdu LianAn) // Call internal '_mint' to mint tokens.
  }
  // Beosin (Chengdu LianAn) // The function 'setGovernance' for setting governance address.
  function setGovernance(address _governance) public {
```

```
    require(msg.sender == governance, "!governance");
    governance = _governance;
  }
  // Beosin (Chengdu LianAn) // The function 'addMinter' for adding a new minter.
  function addMinter(address _minter) public {
    require(msg.sender == governance, "!governance"); // Beosin (Chengdu LianAn) // Requiire The caller must be governance address.
    minters[_minter] = true; // Beosin (Chengdu LianAn) // Add minter role to '_minter'.
  }
  // Beosin (Chengdu LianAn) // The function 'renounceMinter' for removing the specified minter.
  function removeMinter(address _minter) public {
    require(msg.sender == governance, "!governance"); // Beosin (Chengdu LianAn) // Require the caller must be governance address.
    minters[_minter] = false; // Beosin (Chengdu LianAn) // Remove minter role to '_minter'.
  }
}
```

成都链安

BEOSIN

Official Website

https://lianantech.com

E-mail

vaas@lianantech.com

Twitter

https://twitter.com/LianAnTech