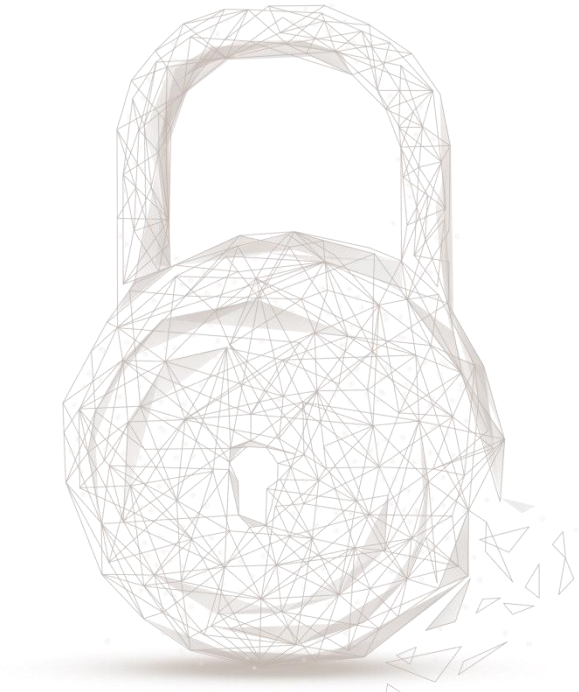
成都链安
BEOSIN

智能合约安全审计报告



审计编号：202008191935

审计合约名称：

dcocos.finance (dCOCOS)

审计合约链接地址：

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

Commit Hash：

0688ff7462bdd72499467eb5fcfbf54102b87c0c

合约审计开始日期：2020.08.13

合约审计完成日期：2020.08.19

审计结果：通过（优）

审计团队：成都链安科技有限公司

审计类型及结果：

序号	审计类型	审计子项	审计结果
1	代码规范审计	ERC20 Token 标准规范审计	通过
		编译器版本安全审计	通过
		可见性规范审计	通过
		gas 消耗审计	通过
		SafeMath 功能审计	通过
		fallback 函数使用审计	通过
		tx.origin 使用审计	通过
		弃用项审计	通过
		冗余代码审计	通过
		变量覆盖审计	通过
2	函数调用审计	函数调用权限审计	通过
		call/delegatecall 安全审计	通过
		返回值安全审计	通过
		自毁函数安全审计	通过
3	业务安全审计	owner 权限审计	通过
		业务逻辑审计	通过
		业务实现审计	通过
4	整型溢出审计	-	通过
5	可重入攻击审计	-	通过
6	异常可达状态审计	-	通过
7	交易顺序依赖审计	-	通过
8	块参数依赖审计	-	通过
9	伪随机数生成审计	-	通过

10	拒绝服务攻击审计	-	通过
11	代币锁仓审计	-	无锁仓
12	假充值审计	-	通过
13	event 安全审计	-	通过

备注：审计意见及建议请见代码注释。

审计结果说明：

本公司采用形式化验证、静态分析、动态分析、典型案例测试和人工审核的方式对智能合约dCOCOS的代码规范性、安全性以及业务逻辑三个方面进行多维度全面的安全审计。**经审计，dCOCOS合约通过所有检测项，合约审计结果为通过(优)，合约可正常使用。**以下为本合约基本信息。

1、代币基本信息

Token name	dcocos.finance
Token symbol	dCOCOS
decimals	18
totalSupply	初始为0(可铸币，无代币上限；对应CocosGateway合约设置可修改的铸币上限值为24亿)
Token type	ERC20

表1 代币基本信息

2、代币锁仓信息

无锁仓

合约源代码审计注释：

```
pragma solidity ^0.5.0; // 成都链安 // 建议固定编译器版本

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; // 成都链安 // 声明变量 governance，存储 governance 地址
  mapping (address => bool) public minters; // 成都链安 // 声明 mapping 变量 minters，存储指定地址的铸币者权限
  // 成都链安 // 构造函数，初始化代币基本信息和设置 governance 地址
  constructor () public ERC20Detailed("dcocos.finance", "dCOCOS", 18) {
      governance = tx.origin;
  }
  // 成都链安 // 铸币函数，调用者调用该函数向指定地址铸一定数量的代币
  function mint(address account, uint256 amount) public {
      require(minters[msg.sender], "!minter");  // 成都链安 // 要求调用者必须是铸币者
      _mint(account, amount);
  }
  // 成都链安 // 设置 governance 地址函数
  function setGovernance(address _governance) public {
      require(msg.sender == governance, "!governance"); // 成都链安 // 要求调用者必须是governance 地址
      governance = _governance; // 成都链安 // 设置 governance 地址为_governance
  }
  // 成都链安 // 添加铸币者函数，添加指定地址_minter 为铸币者
  function addMinter(address _minter) public {
      require(msg.sender == governance, "!governance"); // 成都链安 // 要求调用者必须是governance 地址
      minters[_minter] = true; // 成都链安 // 设置指定地址_minter 为铸币者
  }
  // 成都链安 // 移除铸币者函数，移除指定地址_minter 铸币者权限
  function removeMinter(address _minter) public {
      require(msg.sender == governance, "!governance"); // 成都链安 // 要求调用者必须是governance 地址
      minters[_minter] = false; // 成都链安 // 取消指定地址_minter 铸币权限
  }
}
```

成都链安
BEOSIN

官方网址

https://lianantech.com

电子邮箱

vaas@lianantech.com

微信公众号