



智能合约安全审计报告



审计编号: 202008191810

审计合约名称:

CocosGateway

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

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	编译器版本安全审计	通过
		弃用项审计	通过
		冗余代码审计	通过
		require/assert 使用审计	通过
		gas 消耗审计	通过
2	通用漏洞审计	整型溢出审计	通过
		重入攻击审计	通过
		伪随机数生成审计	通过
		交易顺序依赖审计	通过
		拒绝服务攻击审计	通过
		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
		tx.origin 使用安全审计	通过
		重放攻击审计	通过
		变量覆盖审计	通过
3	业务审计	业务逻辑审计	通过
		业务实现审计	通过

备注：审计意见及建议请见代码注释。

免责声明：本次审计仅针对本报告载明的审计类型及结果表中给定的审计类型范围进行审计，其他未知安全漏洞不在本次审计责任范围之内。成都链安科技仅根据本报告出具前已经存在或发生的攻击或漏洞出具本报告，对于出具以后存在或发生的新的攻击或漏洞，成都链安科技无法判断其对智能合约安全状况可能的影响，亦不对此承担责任。本报告所作的安全审计分析及其他内容，仅基于合约提供者在本报告出具前已向成都链安科技提供的文件和资料，且该部分文件和资料不存在任何缺失、被篡改、删减或隐瞒的前提下作出的；如提供的文件和资料存在信息缺失、被篡改、删减、隐瞒或反映的情况与实际情况不符等情况或提供文件和资料在本报告出具后发生任何变动的，成都链安科技对由此而导致的损失和不利影响不承担任何责任。成都链安科技出具的本审计报告系根据合约提供者提供的文件和资料依靠成都链安科技现掌握的技术而作出的，由于任何机构均存在技术的局限性，成都链安科技作出的本审计报告仍存在无法完整检测出全部风险的可能性，成都链安科技对由此产生的损失不承担任何责任。

本声明最终解释权归成都链安科技所有。

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CocosGateway项目智能合约代码规范性、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，CocosGateway项目智能合约通过所有检测项，合约审计结果为通过。**以下为本合约详细审计信息。

代码规范审计

1. 编译器版本安全审计

老版本的编译器可能会导致各种已知安全问题，建议开发者在代码中指定合约代码采用最新的编译器版本，并消除编译器告警。

- 安全建议：无
- 审计结果：通过

2. 弃用项审计

Solidity智能合约开发语言处于快速迭代中，部分关键字已被新版本的编译器弃用，如throw、years等，为了消除其可能导致的隐患，合约开发者不应该使用当前编译器版本已弃用的关键字。

- 安全建议：无
- 审计结果：通过

3. 冗余代码审计

智能合约中的冗余代码会降低代码可读性，并可能需要消耗更多的gas用于合约部署，建议消除冗余代码。

- 安全建议：无
- 审计结果：通过

4. require/assert 使用审计

Solidity使用状态恢复异常来处理错误。这种机制将会撤消对当前调用(及其所有子调用)中的状态所做的所有更改，并向调用者标记错误。函数assert和require可用于检查条件并在条件不满足时抛出异常。assert函数只能用于测试内部错误，并检查非变量。require函数用于确认条件有效性，例如输入变量，或合约状态变量是否满足条件，或验证外部合约调用的返回值。

- 安全建议：无
- 审计结果：通过

5. gas 消耗审计

以太坊虚拟机执行合约代码需要消耗gas，当gas不足时，代码执行会抛出out of gas异常，并撤销所有状态变更。合约开发者需要控制代码的gas消耗，避免因gas不足导致函数执行一直失败。

- 安全建议：无
- 审计结果：通过

通用漏洞审计

1. 整型溢出审计

整型溢出是很多语言都存在的安全问题，它们在智能合约中尤其危险。Solidity最多能处理256位的数字($2^{256}-1$)，最大数字增加1会溢出得到0。同样，当数字为uint类型时，0减去1会下溢得到最大数字值。溢出情况会导致不正确的结果，特别是如果其可能的结果未被预期，可能会影响程序的可靠性和安全性。

- 安全建议：无
- 审计结果：通过

2. 重入攻击审计

重入漏洞是最典型的以太坊智能合约漏洞，曾导致了The DAO被攻击。该漏洞原因是Solidity中的`call.value()`函数在被用来发送Ether的时候会消耗它接收到的所有gas，当调用`call.value()`函数发送Ether的逻辑顺序存在错误时，就会存在重入攻击的风险。

- 安全建议：无
- 审计结果：通过

3. 伪随机数生成审计

智能合约中可能会使用到随机数，在solidity下常见的是用block区块信息作为随机因子生成，但是这样使用是不安全的，区块信息是可以被矿工控制或被攻击者在交易时获取到，这类随机数在一定程度上是可预测或可碰撞的，比较典型的例子就是fomo3d的airdrop随机数可以被碰撞。

- 安全建议：无
- 审计结果：通过

4. 交易顺序依赖审计

在以太坊的交易打包执行过程中，面对相同难度的交易时，矿工往往会选择gas费用高的优先打包，因此用户可以指定更高的gas费用，使自己的交易优先被打包执行。

- 安全建议：无
- 审计结果：通过

5. 拒绝服务攻击审计

拒绝服务攻击，即Denial of Service，可以使目标无法提供正常的服务。在以太坊智能合约中也会存在此类问题，由于智能合约的不可更改性，该类攻击可能使得合约永远无法恢复正常工作状态。导致智能合约拒绝服务的原因有很多种，包括在作为交易接收方时的恶意revert、代码设计缺陷导致gas耗尽等等。

- 安全建议：无
- 审计结果：通过

6. 函数调用权限审计

智能合约如果存在高权限功能，如：铸币、自毁、change owner等，需要对函数调用做权限限制，避免权限泄露导致的安全问题。

- 安全建议：无
- 审计结果：通过

7. call/delegatecall安全审计

Solidity中提供了call/delegatecall函数来进行函数调用，如果使用不当，会造成call注入漏洞，例如call的参数如果可控，则可以控制本合约进行越权操作或调用其他合约的危险函数。

- 安全建议：无

- 审计结果：通过

8. 返回值安全审计

在Solidity中存在transfer()、send()、call.value()等方法中，transfer转账失败交易会回滚，而send和call.value转账失败会return false，如果未对返回做正确判断，则可能会执行到未预期的逻辑；另外在ERC20 Token的transfer/transferFrom功能实现中，也要避免转账失败return false的情况，以免造成假充值漏洞。

- 安全建议：无
- 审计结果：通过

9. tx.origin使用安全审计

在以太坊智能合约的复杂调用中，tx.origin表示交易的初始创建者地址，如果使用tx.origin进行权限判断，可能会出现错误；另外，如果合约需要判断调用方是否为合约地址时则需要使用tx.origin，不能使用extcodesize。

- 安全建议：无
- 审计结果：通过

10. 重放攻击审计

重放攻击是指如果两份合约使用了相同的代码实现，并且身份鉴权在传参中，当用户在向一份合约中执行一笔交易，交易信息可以被复制并且向另一份合约重放执行该笔交易。

- 安全建议：无
- 审计结果：通过

11. 变量覆盖审计

以太坊存在着复杂的变量类型，例如结构体、动态数组等，如果使用不当，对其赋值后，可能导致覆盖已有状态变量的值，造成合约执行逻辑异常。

- 安全建议：无
- 审计结果：通过

业务审计

1. 交换dCOCOS代币（COCOS → dCOCOS）

- **业务描述：**合约实现了swapDCOCOS函数用于将COCOS代币一比一兑换为dCOCOS代币，用户（COCOS代币持有者）向该合约地址预授权，通过调用COCOS合约中的transferFrom函数，合约地址代理用户将指定数量的COCOS代币转至本合约地址，然后通过调用dCOCOS合约中的transfer函数，合约地址将对应数量的dCOCOS代币转至函数调用者（用户）地址；该函数功能可被暂停，当合约全局暂停状态为true时函数无法被成功调用。

➤ **相关函数：** swapDCOCOS、transferFrom (COCOS合约)、transfer (dCOCOS合约)

➤ **安全建议：** 无

➤ **审计结果：** 通过

2. 交换COCOS代币 (dCOCOS -> COCOS)

➤ **业务描述：** 合约实现了swapCOCOS函数用于将dCOCOS代币一比一兑换为COCOS代币，用户 (dCOCOS代币持有者) 向该合约地址预授权，通过调用dCOCOS合约中的transferFrom函数，合约地址代理用户将指定数量的dCOCOS代币转至本合约地址，然后通过调用COCOS合约中的transfer函数，合约地址将对应数量的COCOS代币转至函数调用者 (用户) 地址；该函数功能可被暂停，当合约全局暂停状态为true时函数无法被成功调用。

➤ **相关函数：** swapCOCOS、transferFrom (dCOCOS合约)、transfer (COCOS合约)

➤ **安全建议：** 无

➤ **审计结果：** 通过

3. dCOCOS铸币

➤ **业务描述：** 合约实现了内部函数_mintDCOCOS用于在本合约内调用dCOCOS合约的mint函数进行铸币操作 (有上限，但原dCOCOS的铸币功能可无上限铸币)，该合约内设置的铸币上限值可通过addDCOCOSSupply函数进行修改。

➤ **相关函数：** _mintDCOCOS、mint (dCOCOS合约)、addDCOCOSSupply

➤ **安全建议：** 无

➤ **审计结果：** 通过

4. 治理设置

➤ **业务描述：** 合约实现了setGovernance函数用于设置治理管理员地址。

➤ **相关函数：** setGovernance

➤ **安全建议：** 无

➤ **审计结果：** 通过

合约源代码审计注释：

```
// 成都链安 // 合约文件: CocosGateway.sol
/// @title CocosGateway
/// swap COCOS<->dCOCOS 1:1
/// For more information about this token please visit https://dcocos.finance
/// @author reedhong
pragma solidity ^0.5.0; // 成都链安 // 建议固定编译器版本

import '@openzeppelin/contracts/lifecycle/Pausable.sol';
```

```
import './IERC20.sol';
import './SafeERC20.sol';

contract CocosGateway is Pausable {
    using SafeERC20 for IERC20; // 成都链安 //引入 SafeERC20 库，其内部函数用于安全外部
ERC20 合约转账相关操作
    using SafeMath for uint256; // 成都链安 // 引入 SafeMath 安全数学运算库，避免数学运算整
型溢出

    address public governance;

    IERC20 public cocos = IERC20(0x60626db611a9957C1ae4Ac5b7eDE69e24A3B76c5); // 成都链安
// 声明外部 COCOS Token 合约实例
    IERC20 public dcocos = IERC20(0x16cAC1403377978644e78769Daa49d8f6B6CF565); // 成都链安
// 声明外部 dCOCOS Token 合约实例

    uint256 public dcocosTotalSupply = 0; // 成都链安 // 声明变量 dcocosTotalSupply，存储
本合约内记录的 dCOCOS 代币总量
    uint256 public dcocosMaxSupply = 24000000000*1e18; // 成都链安 // 声明变量
dcocosMaxSupply，存储 dCOCOS 代币在本合约的铸币上限（原 dCOCOS 代币可无上限铸币）

    event MintDCOCOS(uint256 amount); // 成都链安 // 声明 dCOCOS 铸币事件
    event SwapDCOCOS(address indexed user, uint256 amount); // 成都链安 // 声明交换 dCOCOS
代币事件
    event SwapCOCOS(address indexed user, uint256 amount); // 成都链安 // 声明交换 COCOS 代
币事件
    // 成都链安 // 构造函数，初始化代币暂停状态与治理管理员地址
    constructor () public {
        pause();
        governance = tx.origin;
    }
    // 成都链安 // 设置治理管理员地址函数
    // 成都链安 // 建议在合约中声明相关事件并在本函数触发，以记录治理管理员地址变化
    function setGovernance(address _governance) public {
        require(msg.sender == governance, "!governance"); // 成都链安 // 调用者权限检查，
要求调用者必须为当前治理管理员地址
        governance = _governance; // 成都链安 // 更新治理管理员地址
    }
    // 成都链安 // 增加 dCOCOS 代币本合约铸币上限值函数
    function addDCOCOSSupply(uint256 supply)
    public
    {
        require(msg.sender == governance, "!governance"); // 成都链安 // 调用者权限检查，
要求调用者必须为当前治理管理员地址
        dcocosMaxSupply = dcocosMaxSupply.add(supply); // 成都链安 // 更新 dCOCOS 代币在本
合约的铸币上限
    }
}
```



```
// 成都链安 // 内部函数，用于向本合约地址铸币一定数量的 dCOCOS 代币
function _mintDCOCOS(uint256 amount) internal{
    uint256 supply = dcocosTotalSupply.add(amount); // 成都链安 // 声明局部变量
    supply, 记录铸币后 dCOCOS 代币总量
    require(supply <= dcocosMaxSupply, "supply is too large"); // 成都链安 // 本合约内
    铸币上限检查，要求铸币后代币总量不超过 dCOCOS 代币在本合约的铸币上限
    dcocos.mint(address(this), amount); // 成都链安 // 调用 dCOCOS 代币的 mint 函数向本合
    约地址进行铸币
    dcocosTotalSupply = supply; // 成都链安 // 更新本合约内记录的 dCOCOS 代币总量
    emit MintDCOCOS(amount); // 成都链安 // 触发 MintDCOCOS 事件
}

// 成都链安 // 交换 dCOCOS 代币函数
// COCOS->dCOCOS
function swapDCOCOS(uint256 amount)
    public
    whenNotPaused // 成都链安 // 该函数功能可被暂停，当合约全局暂停状态为 true 时函数无
    法被成功调用
    returns (bool)
{
    uint256 dcocosBalance = dcocos.balanceOf(address(this)); // 成都链安 // 声明局部
    变量 dcocosBalance，记录该合约下 dCOCOS 代币余额
    if( dcocosBalance < amount){
        _mintDCOCOS(amount.sub(dcocosBalance)); // 成都链安 // 当代币余额不足时，调用
        内部函数 _mintDCOCOS 进行铸币，补足代币余额
    }

    cocos.safeTransferFrom(msg.sender, address(this), amount); // 成都链安 // 通过
    IERC20 合约实体所引用的 SafeERC20 库中 safeTransferFrom 函数发起指定函数调用，调用指定 COCOS
    代币合约的 transferFrom 函数，代理当前函数调用者转出其指定数量的 COCOS 代币至本合约地址
    dcocos.safeTransfer(msg.sender, amount); // 成都链安 // 通过 IERC20 合约实体所引用
    的 SafeERC20 库中 safeTransfer 函数发起指定函数调用，调用指定 dCOCOS 代币合约的 transfer 函
    数，转出对应数量的 dCOCOS 代币至当前函数调用者

    emit SwapDCOCOS(msg.sender, amount); // 成都链安 // 触发 SwapDCOCOS 事件

    return true;
}

// 成都链安 // 交换 COCOS 代币函数
// dCOCOS->COCOS
function swapCOCOS(uint256 amount)
    public
    whenNotPaused // 成都链安 // 该函数功能可被暂停，当合约全局暂停状态为 true 时函数无
    法被成功调用
    returns (bool)
{
    uint256 cocosBalance = cocos.balanceOf(address(this)); // 成都链安 // 声明局部变
    量 cocosBalance，记录该合约下 COCOS 代币余额
```

```
require(cocosBalance >= amount, "amount is too large"); // 成都链安 // 代币余额检查，要求交换代币数量 amount 不大于该合约下 COCOS 代币余额
```

```
dcocos.safeTransferFrom(msg.sender, address(this), amount); // 成都链安 // 通过 IERC20 合约实体所引用的 SafeERC20 库中 safeTransferFrom 函数发起指定函数调用，调用指定 dCOCOS 代币合约的 transferFrom 函数，代理当前函数调用者转出其指定数量的 dCOCOS 代币至本合约地址
```

```
cocos.safeTransfer(msg.sender, amount); // 成都链安 // 通过 IERC20 合约实体所引用的 SafeERC20 库中 safeTransfer 函数发起指定函数调用，调用指定 COCOS 代币合约的 transfer 函数，转出对应数量的 COCOS 代币至当前函数调用者
```

```
emit SwapCOCOS(msg.sender, amount); // 成都链安 // 触发 SwapCOCOS 事件
```

```
return true;
```

```
}
```

```
}
```



成都链安
BEOSIN

官方网址

<https://lianantech.com>

电子邮箱

vaas@lianantech.com

微信公众号

