北京链安
Chains Guard Technology

SPADE FINANCE
智能合约审计

北京链安安全评测中心

二〇二一年

■ 文档说明

文档名称	SPADE FINANCE 智能合约审计		
文档管理编号	CG-YMSJ-20210417		
保密级别	公开	文档版本号	V1
制作人	北京链安安全技术中心	制作日期	2021-04-17
扩散范围	限北京链安和授权方		

■ 适用范围

本次安全评估是由授权方授权，由北京链安网络科技有限公司（以下简称“北京链安”）对 SPADE FINANCE 智能合约进行的安全风险深度评估，根据评估结果所提交的技术报告，用于对该智能合约的安全状况做出安全评估和加固建议，仅限于“北京链安”、授权方内部人员传阅。

■ 版本变更记录

修改日期	版本	说明	修改人
2021-04-17	V1.0	文档创建	Berry

目录

免责申明

本次审计为服务于授权方的技术安全性审计，其目的在于向授权方提供进行其业务安全评估和优化的参考依据，不会对代码的实用性、代码的安全性、商业模式的适用性、商业模式的监管制度或任何其他有关应用适用性的说明以及应用在无错状态的行为作出声明或担保。本报告不能作为证明这些被测试过的相关系统和代码已经绝对安全且不存在其他安全风险的证明依据。

本次审计仅针对授权方指定版本的代码、安装包及其它授权方提供的素材展开，其结论仅对相应版本的应用适用，一旦相关代码、配置、运营环境等发生变化，相应结论将不再适用。

技术在不断更新，我们永远保持一颗敬畏之心！

1 项目审计说明

1.1 概述

智能合约的部署和应用越来越广泛，安全问题也越来越受重视。由于智能合约的特殊性，智能合约的不规范编码可能导致代币溢出、交易异常、隐私泄漏、拒绝服务等安全问题。目前已经发生多起因为智能合约安全问题，导致的巨大资产损失事件。北京链安公司提供的智能合约安全审计用于评估当前智能合约风险状态并提供解决方案。

本次审计工作由北京链安安全攻防团队根据智能合约可能出现的所有攻击面，对需测评智能合约进行全面的审计并提供解决方案。

1.2 审计时间

评估测试时间	
起始时间	2021 年 04 月 01 日
结束时间	2021 年 04 月 17 日

1.3 审计单位

单位名称	北京链安网络科技有限公司
单位网址	https://www.chainsguard.com/

1.4 审计对象

名称	合约地址	部署版本
SPADE FINANCE	https://github.com/spadefiannce/SpadeFinance commit： 71732a8a66a33f88589319e13e59e3284edfacc7	V1

1.5 审计方式

虽然我们可以利用各种工具来完成一些自动化的检测工作，但是任何工具都不能替代手工测试，因为工具局限性很强，存在很多的漏报和误报，需要人工结合实际环境手动测试，工具只是一种辅助检测手段，我们侧重于手工检查分析漏洞。所提交的报告，都是经过北京链安安全专家的严格审核。

2 安全审计摘要

2.1 漏洞统计表

漏洞数量	高危	中危	低危
0	0	0	0

【注】危害程度的分级方式简要说明如下

高危：直接导致系统被控制或数据被破坏，一旦发生，就是严重的安全事件。

中危：可能导致重要信息的泄漏或有可能导致系统被控制。

低危：非重要信息泄漏或轻微安全问题，一般不会导致严重的安全事件。

2.2 安全审计

攻击面	检查项目	状态	描述
重入攻击	跨合约交互	通过	不受保护的敏感函数调用外部合约
	OKT 转移	通过	未限制 Gas 转移 OKT 存在重入隐患
越权访问	构造函数不匹配	通过	低版本中合约名称和构造函数是否不匹配
	特权功能暴露	通过	不正确的鉴权方式导致的特权功能暴露
	tx.origin 变量滥用	通过	合约是否使用 tx.origin 进行身份鉴权
	访问控制缺陷	通过	函数及状态变量可见性不合理的设置
数值溢出	上溢和下溢	通过	合约是否具有普遍的上溢或下溢漏洞
条件竞争	交易顺序依赖	通过	合约的最终状态是否取决于交易的顺序
拒绝服务	非预期的交易回滚	通过	合约是否容易受到 revert 而拒绝服务
	手续费超限	通过	过大循环造成的手续费超限
call 注入	call 函数滥用	通过	合约接收外部输入作为 call 函数的参数
假充值攻击	充值结果检查	通过	合约是否不正确的检查充值结果
假币攻击	假币标识检查	通过	合约是否检查代币标识如地址
矿工特权隐患	时间戳依赖	通过	合约是否依赖时间戳完成主要功能
业务安全	业务逻辑审查	通过	审查业务逻辑是否存在明显缺陷
	功能正确性审查	通过	审查功能是否符合业务需求
	伪随机数依赖	通过	合约是否依赖伪随机数完成主要功能
	前端合约集成	通过	审查前端是否正确集成路由合约接口
	预言机安全	通过	审查预言机是否不正确的实现和使用
	数字资产托管	通过	审查数字资产托管是否存在缺陷
特殊检查项	外部输入检查	通过	合约是否校验外部输入的合法性
	使用不受信任的库	通过	合约是否使用了不受信任（不安全）的库
	敏感信息泄露	通过	合约是否存在泄露敏感信息的隐患
	黑洞	通过	合约是否无限期锁定 OKT 或代币
	合约后门	通过	合约是否存在可由项目方控制的后门

3 测试的攻击面

针对智能合约源码审计，我们着重检测了如下一些安全点：

3.1 重入攻击

合约之间的相互调用会产生可供攻击者控制的中间态，不严格的合约调用方式会导致执行流程被攻击者控制，执行非预期的逻辑处理流程。

审计结果：**通过**

3.2 越权访问

合约变量及函数错误的访问域设置，会致使原本应受到访问调用限制的函数可被任何其他账户访问并调用，这通常是因为编码不严谨导致的。

审计结果：**通过**

3.3 数值溢出

合约中的数值处理需要严格检查算术溢出问题，常规的加减算数处理容易引起整数上溢或者下溢，尤其是类似代币在处理账户金额时，更需要严格判断账户金额前后的大小。通常数值运算推荐使用 OpenZeppelin 开源库 SafeMath 模块进行处理。

审计结果：**通过**

3.4 条件竞争

每一笔交易和每一次合约调用最终都需要矿工挖矿来进行确认，不同函数共享一个状态会可能会因为执行顺序的变化而造成不一样的处理结果。

审计结果：**通过**

3.5 拒绝服务

不可恢复的恶意操作或者可控制的无限资源消耗都能称作为智能合约中的拒绝服务，攻击者通过构造恶意参数进行合约函数调用可能导致已部署合约无法恢复的逻辑处理问题，被拒绝服务的合约通常会让整个代码逻辑无法继续执行而“停止服务”。

审计结果：**通过**

3.6 call 注入

智能合约中使用底层接口 call 进行合约交互时，接口使用不当时，攻击者可以控制 call 接口的参数、方法选择器或者执行字节内容，进行越权转币、增发、销毁代币等危险操作。

审计结果：**通过**

3.7 假充值攻击

智能合约是否采用不正确的方式检查充值结果，调用充值函数时应检查函数返回值是否成功和资金是否到账来判断充值是否成功。

审计结果：**通过**

3.8 矿工特权隐患

智能合约中的 block.timestamp、block.number 等数值本身可预测，当合约中涉及到随机数生成时，切勿使用易被获取的变量或参数来作为种子生成随机数，较好的方法是使用外部服务 Provable API 来进行随机数的生成和处理。

审计结果：**通过**

3.9 业务安全

审查去中心化金融（Decentralized finance）业务逻辑是否存在明显缺陷，功能是否符合业务需求，数字资产托管是否存在安全隐患以及预言机实现和使用安全。

审计结果：**通过**

3.10 敏感信息泄露

智能合约代码需要对存储的用户隐私信息进行加密保护，任何人都能通过查询链上数据获取合约存储的相关信息，若隐私信息未进行加密或加密不严格，则很容易导致隐私泄露。

审计结果：**通过**

3.11 合约后门

在区块链生态里有些项目方本身不具备智能合约开发能力，通常会选择一些智能合约自动化生成工具进行一键生成并自动部署到链上，这就给黑客向智能合约插入后门代码带来了机会。智能合约一旦被插入后门代码，黑客便可利用其后门任意操纵合约行为这将给项目方带来致命危害。或者合约存在可由项目方控制的后门。

审计结果：**通过**

4 安全审计总结

本次智能合约审计未发现可利用的安全漏洞，总体评估安全状态为：**良好状态**

本次智能合约审计结果仅作为授权方制定相应的安全措施与解决方案提供实际的依据。

附录 A. 安全风险状况等级说明

安全风险状况说明	
1	**良好状态** 智能合约处于良好运行状态，没有发现或只存在零星的低风险安全问题，此时只要保持现有安全策略就满足了本系统的安全等级要求。
2	**预警状态** 智能合约中存在一些漏洞或安全隐患，未开始大规模使用，此时需根据评估中发现的问题对进行有针对性的加固或改进，重新部署。
3	**严重状态** 智能合约已经大规模使用，智能合约中发现存在严重漏洞或可能严重威胁到合约正常运行的安全问题，此时需要立刻采取措施，重新部署加固后的智能合约。
4	**紧急状态** 智能合约相关代币已开放交易，智能合约中发现严重漏洞或可能严重威胁到合约正常运行的安全问题，可能对经济利益造成严重损害。此时，应立刻停止合约相关的代币交易，立即采取措施，重新部署加固后的智能合约。