北京链安
Chains Guard Technology

# BHC
# 智能合约审计报告

北京链安安全评测中心

二〇二〇年十月

## □ 文档说明

| | | | |
|---|---|---|---|
| 文档名称 | BHC 智能合约审计报告 | | |
| 文档管理编号 | CG-YMSJ-ZH-202010032 | | |
| 保密级别 | 商密 | 文档版本号 | V1.0 |
| 制作人 | 北京链安安全技术中心 | 制作日期 | 2020-10-13 |
| 扩散范围 | 限北京链安和授权方 | | |

## □ 适用范围

本次安全评估是由项目方授权，由北京链安网络科技有限公司（以下简称“北京链安”）对 BHC 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，仅限于北京链安和项目方内部人员传阅。

## □ 版本变更记录

| 修改日期 | 版本 | 说明 | 修改人 |
|---|---|---|---|
| 2020-10-13 | V1.0 | 文档创建 | 张峰 |

# 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。

本次审计仅限于对该智能合约的技术安全审计，调用该智能合约的其它程序、应用、前端页面等技术模块的技术安全并不在审计范围内。同时，涉及该智能合约实际使用产生的道德风险、经营风险、市场风险等非技术风险也与本次智能合约的技术审计结果无关。

技术在不断更新，我们永远保持一颗敬畏之心！

# 1 项目测试说明

## 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、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** | 2020 年 10 月 13 日 |
| **结束时间** | 2020 年 10 月 14 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

bhc_opt.sol SHA256：4f50c6a37a28f01653df67e72e341401edb558972cf666a7578127acadc09986

## 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**：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**：可能导致重要信息的泄漏或有可能导致系统被控制。

**低**：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 安全审计项

针对该智能合约的审计，我们着重检查如下安全点：

| 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不可信外部合约 |
| | ETH 转移 | 通过 | 未限制 Gas 转移 ETH 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波场地址 |
| 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 |
| | 伪随机数依赖 | 通过 | 合约是否依赖伪随机数完成主要功能 |
| 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 安全审计结果

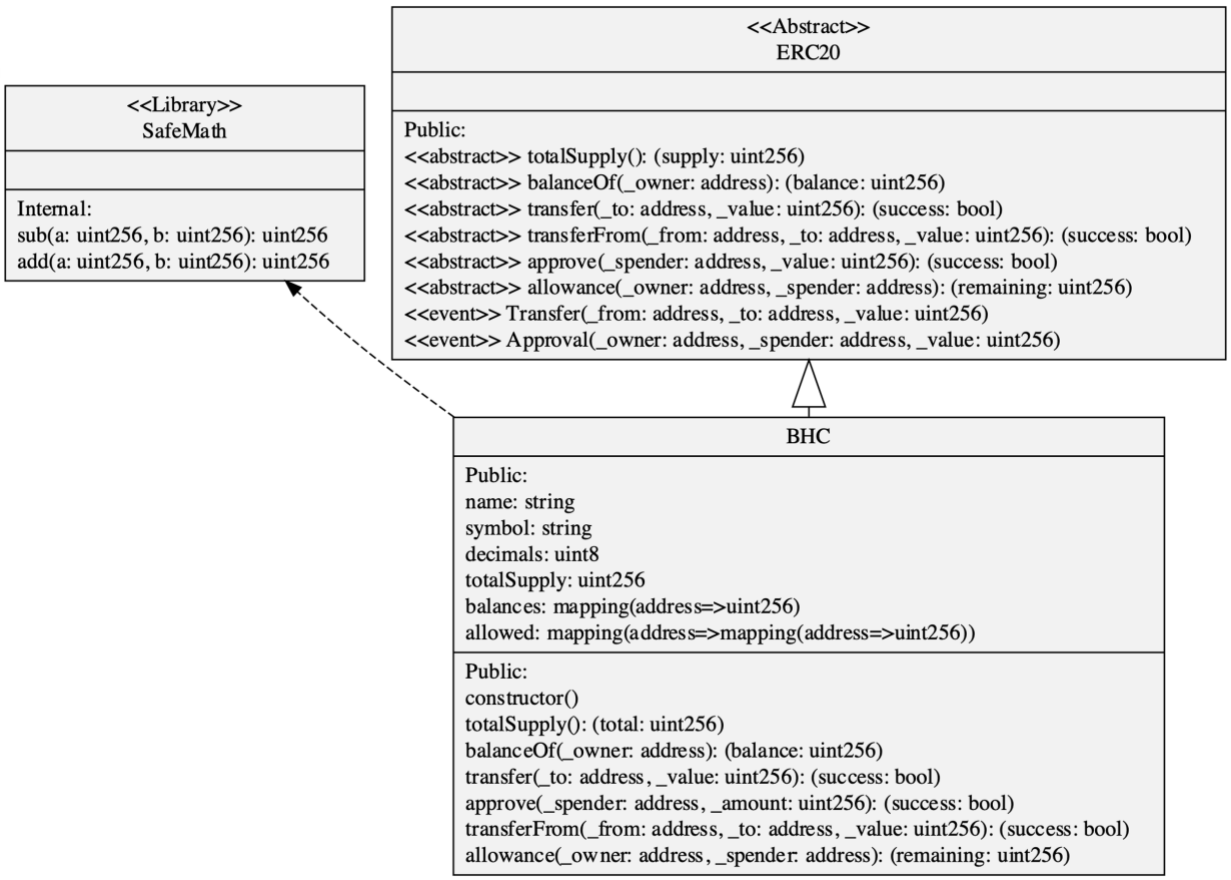
经本次审计，以及过程中项目方与审计方的配合，各合约均已处于无已知问题状态。

# 4 安全审计总结

本次审计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。

# 5 合约结构


<<Abstract>>
ERC20
Public:
<<abstract>> totalSupply(): (supply: uint256)
<<abstract>> balanceOf(_owner: address): (balance: uint256)
<<abstract>> transfer(_to: address, _value: uint256): (success: bool)
<<abstract>> transferFrom(_from: address, _to: address, _value: uint256): (success: bool)
<<abstract>> approve(_spender: address, _value: uint256): (success: bool)
<<abstract>> allowance(_owner: address, _spender: address): (remaining: uint256)
<<event>> Transfer(_from: address, _to: address, _value: uint256)
<<event>> Approval(_owner: address, _spender: address, _value: uint256)
<<Library>>
SafeMath
Internal:
sub(a: uint256, b: uint256): uint256
add(a: uint256, b: uint256): uint256
BHC
Public:
name: string
symbol: string
decimals: uint8
totalSupply: uint256
balances: mapping(address=>uint256)
allowed: mapping(address=>mapping(address=>uint256))
Public:
constructor()
totalSupply(): (total: uint256)
balanceOf(_owner: address): (balance: uint256)
transfer(_to: address, _value: uint256): (success: bool)
approve(_spender: address, _amount: uint256): (success: bool)
transferFrom(_from: address, _to: address, _value: uint256): (success: bool)
allowance(_owner: address, _spender: address): (remaining: uint256)

# 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**<br>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**<br>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**<br>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**<br>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。 |