CERTIK 审计报告

审计日期: 2025/12/18

合约地址: 0xdf3D7f94a179c4d92b5AA261e666bF90B06e1573

所在主网: 币安智能链

官网：https://skynet.certik.com/

一、合约威胁分析

合同源代码已验证。

有利

源代码验证为与智能合约交互的用户提供了透明度。区块浏览器会将编译后的代码与区块链上的代码进行比对。这还使用户有机会审核合约，确保部署的代码符合预期功能，并最大限度地降低恶意或错误合约的风险。

该合约不能发行新的代币，

无影响

铸币功能通常用于生成新的代币，这些代币可以分配到特定地址，例如用户钱包或合约所有者的钱包。此功能广泛应用于各种去中心化金融 (DeFi) 和非同质化代币 (NFT) 项目中，以促进代币的发行和分发。"铸币功能存在性"模块旨在快速识别智能合约中是否存在铸币功能及其实现情况。铸币功能在创建新代币并将其转移到指定用户或所有者的钱包中发挥着至关重要的作用。这一过程显著提高了生态系统内代币的整体流通量。

此合约中的代币不能销毁。

有利

该代币合约包含销毁功能，允许有意减少代币数量，从而降低总供应量。执行此销毁功能有助于在代币生态系统中制造稀缺性，因为代币的整体可用性会降低。

这不是基于代理的可升级合约。

有利

基于代理的可升级合约模块专门用于识别智能合约中是否存在可升级合约或代理模式。利用可升级合约或代理模式，合约所有者无需完全重新部署合约，即可动态更改合约的各个方面，包括功能、代币流通和分发。

所有者不能将代币或用户列入黑名单，

无影响

本模块旨在识别智能合约的所有者是否拥有将特定代币或用户列入黑名单的权限。如果所有者拥有黑名单权限，则所有与被列入黑名单的实体相关的交易都将立即停止。在某些情况下，拥有将代币或用户列入黑名单的权限至关重要，它使所有者能够控制潜在的恶意活动、合规性问题或其他隐患。然而，如果此权限被滥用或误用，则可能导致意想不到的后果和用户不满。

这是 ERC-20 代币，

无影响

代币应符合 ERC-20 代币规范的既定标准，包括包含 ERC-20 标准定义的具有标准化名称和参数的所有必要函数。

这不是一份可暂停的合同。

无影响

可暂停合约是指合约所有者可以主动暂停的合约，从而暂时阻止代币持有者进行买卖活动。这种暂停机制允许合约所有者控制代币的功能，并可出于安全问题、更新或监管合规调整等各种原因暂时中止交易活动。

无影响

合同不能由所有者自行解除，

无影响

SELFDESTRUCT 操作码是以太坊智能合约中的一项关键操作，它允许合约自主终止。调用此操作码后，合约将被释放，从而释放以太坊区块链上的存储和计算资源。值得注意的是，合约中剩余的以太币将被发送到指定的地址，确保资金得到妥善处理。

该合约不存在ERC-20认可的竞争条件漏洞。

无影响

当两个或多个交易同时尝试与同一个 ERC-20 代币合约交互时，就会出现 ERC-20 竞态条件。由于合约中某些操作的非原子性，这种情况可能导致冲突和意外行为。原子性指的是操作不可分割，并且作为一个单一、不可中断的单元执行，

未找到合同持有人。

有利

放弃所有权表明合约真正去中心化，因为所有者已放弃控制权，从而确保合约的功能和规则不会被管理员或任何中央机构更改。

没有一个地址持有的代币总量超过流通代币供应量的5%，

无影响

持有代币余额超过流通代币供应量 5% 的用户需要重点监控，因为他们的行为会对代币价格和生态系统产生重大影响。合理的代币分配有助于维护健康的市场，防止权力集中，促进公平参与，

。

无影响

该合约没有冷却时间条款。

有利

冷却机制是智能合约领域的重要组成部分，用于暂时中止交易活动或其他合约工作流程。该机制引入基于时间的延迟，有效防止用户重复执行交易或频繁买卖代币。冷却机制会在一定时间内暂停交易或其他合约工作流程，从而防止用户重复执行交易或频繁买卖代币。

所有者无法将代币或用户列入白名单。

无影响

这使得合约所有者能够有选择地授予用户特权，例如免除费用或访问独特的合约功能。

业主无法在合同中设定或更新费用。

无影响

在智能合约中，费用是至关重要的组成部分，它可能与各种功能相关联，例如交易、代币转移或其他特定操作。在需要根据市场状况、监管要求或项目特定因素调整费用的情况下，所有者设置或更新费用的能力尤为重要。"所有者可设置或更新费用"模块旨在明确智能合约中所有者设置或修改费用的功能。此功能使合约所有者能够控制合约内的费用结构，从而提供灵活性和适应性，以应对不断变化的情况。

未找到硬编码地址。

无影响

在智能合约中包含固定或硬编码的地址，未来可能会带来重大挑战，尤其是在合约的适应性和可升级性方面。这种对地址的静态引用可能会阻碍合约更新或修改的无缝实施，从而限制其根据不断变化的需求进行演进的能力。随着时间的推移，这种僵化可能会导致在尝试增强或更改智能合约功能时出现各种复杂情况和障碍。

该合约没有任何所有者可控制的修改代币余额的功能。

无影响

"所有者更新代币余额"模块旨在识别智能合约中所有者控制的功能，这些功能允许所有者更新其他用户或合约自身的代币余额。如果合约允许所有者操纵代币余额，则可能对用户持有的代币数量和合约的整体完整性产生重大影响。在某些情况下，合约可能为所有者提供手动调整代币余额的功能。虽然此功能在特定用例（例如代币分发或奖励）中可能合法，但也引入了潜在风险。允许所有者随意更新代币余额可能会导致漏洞、操纵或对代币生态系统造成意外更改。

所有者的钱包中含有 0 个代币，不到流通代币供应量的 5%。

无影响

检查所有者的钱包余额是否超过特定代币数量，可能表明存在中心化风险，即所有者可能对代币供应拥有不成比例的控制权，从而可能导致操纵或滥用。

未找到获取所有权的此类函数。

无影响

"检索所有权"模块旨在快速高效地检索智能合约中的所有权相关信息。对于希望无缝访问和管理所有权数据的项目而言，此功能至关重要。借助此模块，开发人员可以简化获取所有权详情的流程，从而有助于在生态系统中有效管理所有权相关功能。

可用

›

不存在恶意定型。

无影响

恶意类型转换，特别是将 uint160 值转换为地址，是诈骗分子经常使用的策略，用于创建可以绕过标准检测机制的欺骗性地址，从而实施欺诈活动，

未找到具有 totalSupply 函数更新功能的函数。

无影响

当代币价值与稀缺性挂钩，或者需要精确控制通货膨胀或通货紧缩时，固定供应量至关重要。如果没有固定供应量，合约可能会引入意外通货膨胀，导致代币贬值，或削弱人们对代币稳定性的信任。

没有此类通过恶意铸币滥用气体的功能。

无影响

Gas滥用是指智能合约中存在操纵gas消耗、不必要地增加用户交易成本的模式。这种滥用可以通过各种机制实现，这些机制旨在利用gas的低效性或人为抬高gas使用量，从而在用户不知情的情况下将经济负担转嫁给用户。

有效的令牌名称或符号。

无影响

令牌名称或符号包含潜在有害内容，例如 HTML 标签或 JavaScript 代码。如果这些未经处理的字符串显示在用户界面上，它们可能会在用户的浏览器中执行脚本，从而构成跨站脚本攻击 (XSS) 的重大风险，

未检测到隐藏所有者

有利

隐藏所有者检查用于识别合同中是否存在任何隐藏的所有者角色。隐藏的所有权可能导致未经授权的访问和控制，从而对用户和利益相关者构成风险。

没有此类具有特殊访问权限的地址的功能。

无影响

授予非所有者地址的特殊权限允许它们以更高的访问权限执行特定功能。这可能会带来安全风险，因为这些特权地址可能会执行影响合约状态或用户资金的关键操作。如果管理或监控不当，这些权限可能导致未经授权或恶意行为，从而损害合约的完整性。

该代币并非伪造代币。

无影响

经查，该合约使用的代币符号与官方代币完全相同，因此属于伪造代币。这些伪造代币会误导用户，让他们误以为自己正在使用合法、知名的加密货币，从而可能导致经济损失并损害官方代币的声誉。

关键功能中不存在外部呼叫风险。

无影响

此检查旨在识别关键函数中外部调用相关的风险。外部调用可能会引入漏洞，例如意外的状态变更或对外部合约的依赖，从而损害函数执行的完整性和可靠性。

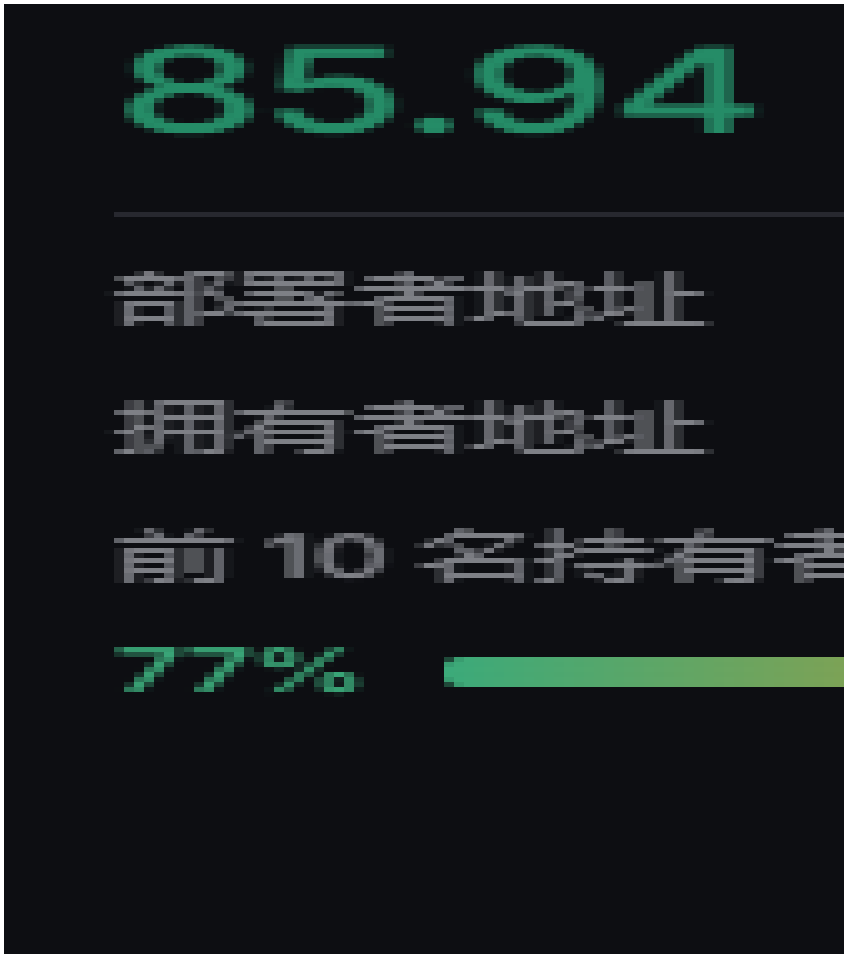
这份合同并非诱饵合同。

无影响

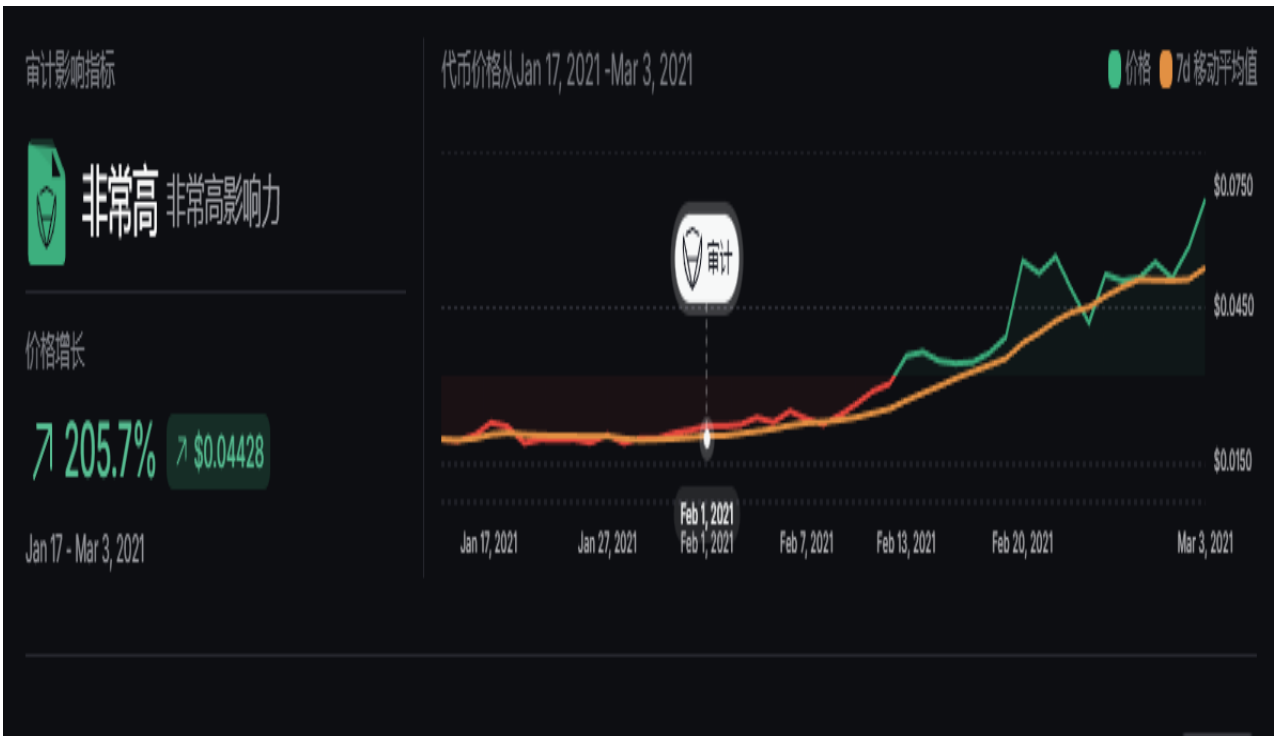
当一种代币具备旨在诱捕投资者资金并阻止其获利的典型特征时，它就被称为"蜜罐代币"。常见的特征包括：购买后无法出售代币、智能合约中编码了限制性的转让功能、交易税过高或存在隐性税收，或者仅允许合约所有者执行出售操作。

CertiK Skynet 得分：

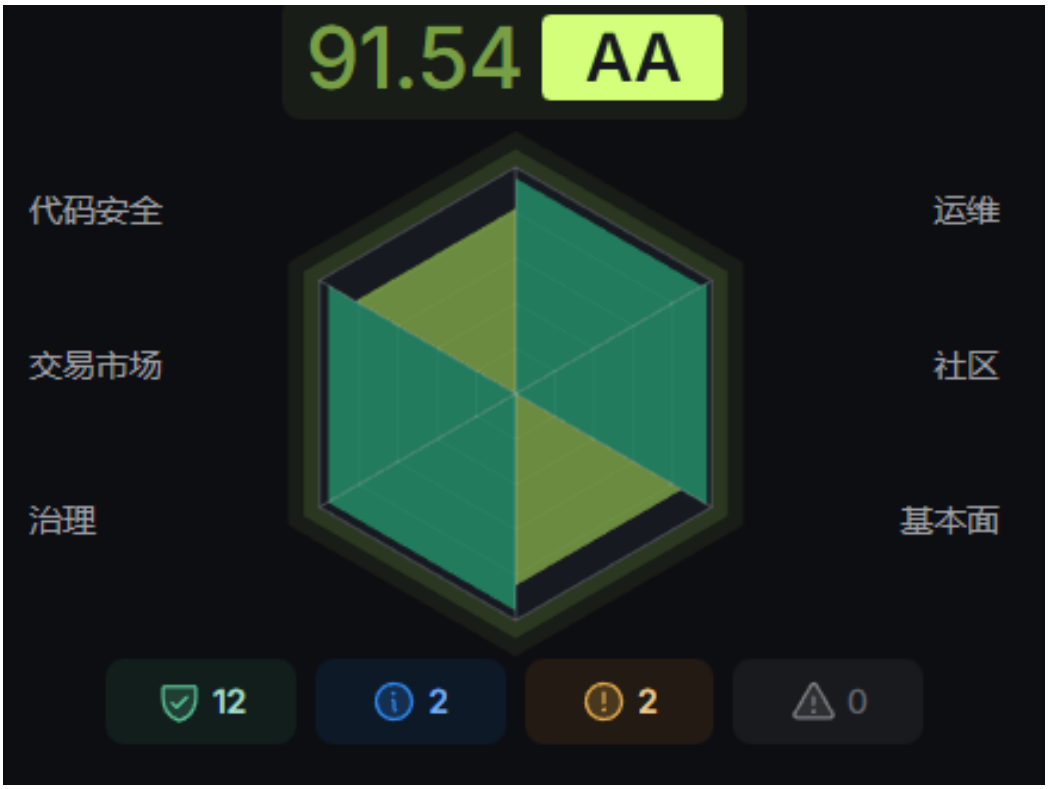
合约扫描代码:



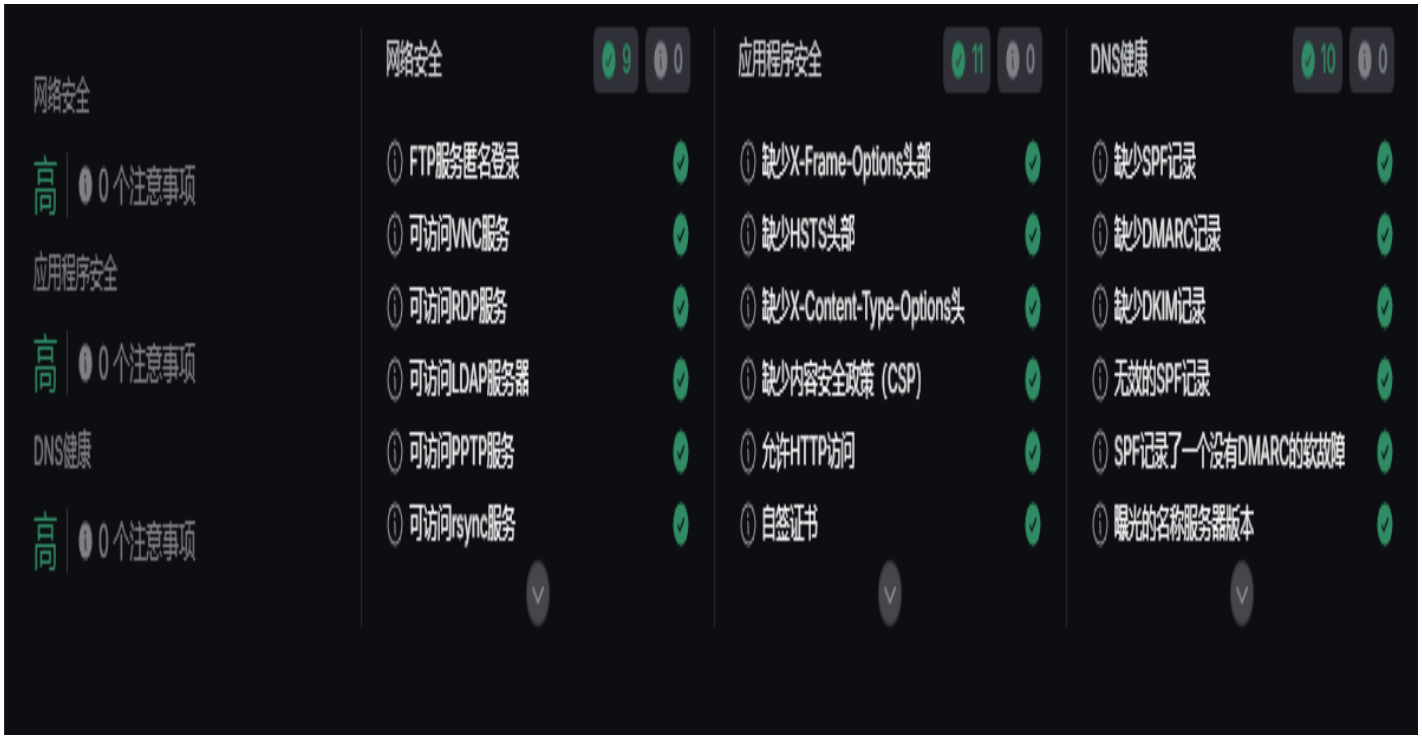
审计安全度:


审计影响指标
非常高 非常高影响力
价格增长
205.7%
$0.04428
Jan 17 - Mar 3, 2021
代币价格从Jan 17, 2021 -Mar 3, 2021
价格
7d 移动平均值
$0.0750
$0.0450
$0.0150
审计
Feb 1, 2021
Jan 17, 2021
Jan 27, 2021
Feb 1, 2021
Feb 7, 2021
Feb 13, 2021
Feb 20, 2021
Mar 3, 2021

代码安全:



网站安全度：


网络安全
高
0 个注意事项
应用程序安全
高
0 个注意事项
DNS健康
高
0 个注意事项
网络安全
9
0
FTP服务匿名登录
可访问VNC服务
可访问RDP服务
可访问LDAP服务器
可访问PPTP服务
可访问rsync服务
应用程序安全
11
0
缺少X-Frame-Options头部
缺少HSTS头部
缺少X-Content-Type-Options头
缺少内容安全政策 (CSP)
允许HTTP访问
自签证书
DNS健康
10
0
缺少SPF记录
缺少DMARC记录
缺少DKIM记录
无效的SPF记录
SPF记录了一个没有DMARC的软故障
暴光的名称服务器版本

社区信任度：


推特监测
推特 活动指标
高
非常
活跃
推特粉丝 (24小时)
516,313 -53
推特账户年龄
11年 6 mo
推特总数 (24小时)
14,612 +2
追随者增长
519K
517K
515K
11/07
11/11
11/15
11/19
11/24
11/29
12/04
12/09
12/14
12/19
Telegram 监控
@chiliz_io
Telegram 活动指标
高
非常
活跃
总用户数 (24小时)
15,350 +0
每日活跃用户 & 消息
432
318
188
11/27
11/29
12/02
12/04
12/07
12/10
12/13
12/16
12/19
每日活跃用户 (24小时)
355 +0
每日信息 (24小时)
14 +6

以上数据来自CERTIK审计报告，安全度100%，可以放心理财，便于链上监控

官网：https://skynet.certik.com/

免责声明

The content on this website or hyperlinked sites is provided for informational purposes only on an “as is” basis at user's sole risk. This information does not constitute financial or investment advice, legal advice, or any other form of advice meant for a user’s specific reliance for any purpose. Past performance is not indicative of future results. Users are solely responsible for their investment decisions and should consult with a financial advisor as needed. Investing in any type of cryptocurrency or other digital asset involves significant risks, including the potential loss of principal. CertiK makes no warranties or guarantees of any kind as to the accurateness, quality, or completeness of the information and CertiK shall not be responsible or liable for any errors, omissions, or inaccuracies in the information or for any user’s reliance on the information. Users are solely responsible for verifying the information as being appropriate for user’s personal use. No content on our website or hyperlinked sites is meant to be a solicitation or offer of any kind.

我们始终建议进行独立的手动审计，包括手动审计和公共漏洞赏金计划，以确保智能合约的安全。