

ORA 项目投研尽职调查报告

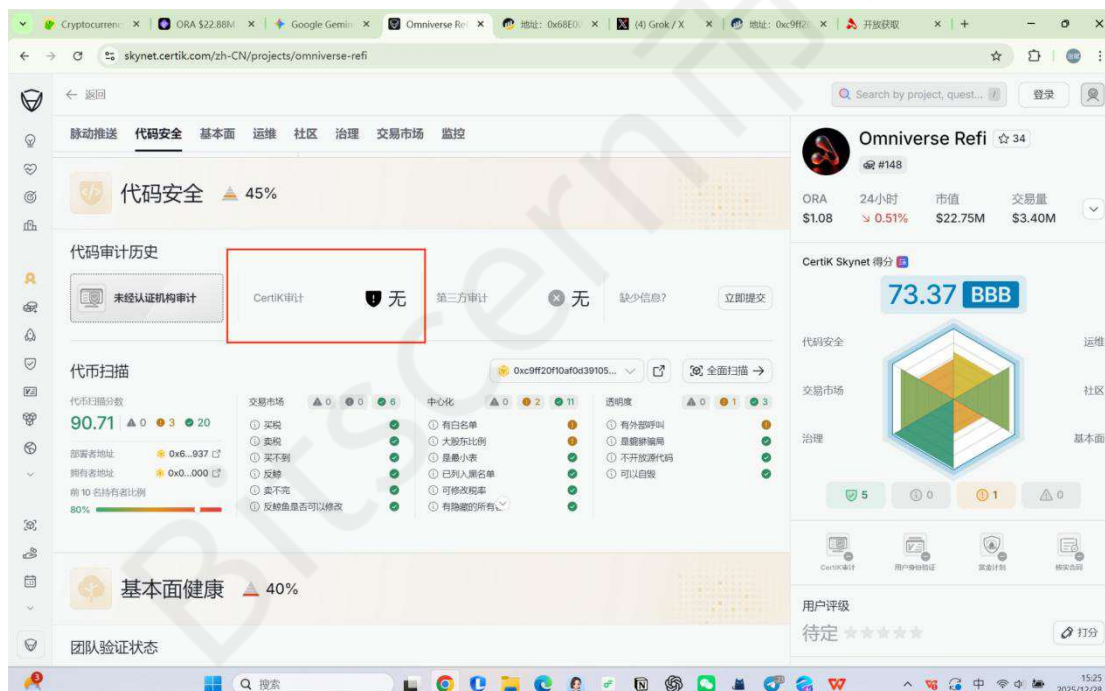
最新更新日期：12/28/2025

1. 安全审计合规性核查

宣发与事实的差异：项目方公开宣传已通过 CertiK 审计，但经交叉验证，CertiK 官方数据库中未收录该项目的任何审计记录。

风险提示：项目方提供的审计状态与事实严重不符，存在虚假宣传嫌疑。缺乏权威第三方的代码审计意味着项目存在未知的安全漏洞，极易遭受黑客攻击。

certik 链接：<https://skynet.certik.com/zh-CN/projects/omniverse-refi>

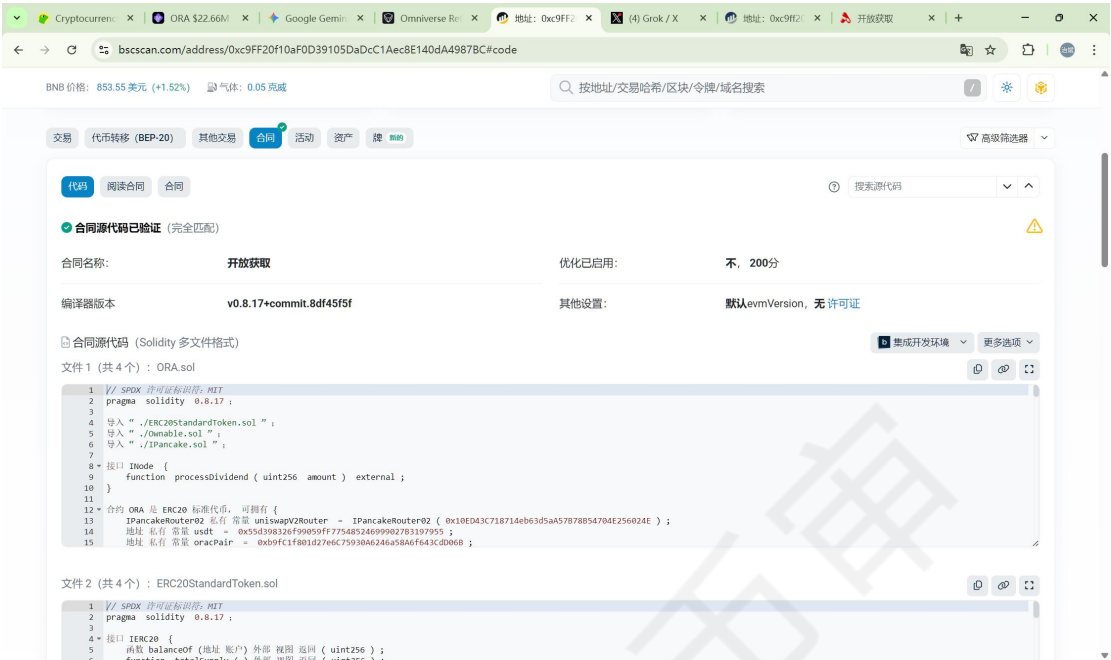


2. 代码库与架构分析

代码溯源：代码库呈现出明显的“拼凑”特征，大量逻辑疑似复用自其他短周期的土狗项目，缺乏原创性开发痕迹。

开发特征：代码风格及注释习惯具有显著的中文开发者特征，推测开发团队大概率位于中国地区。

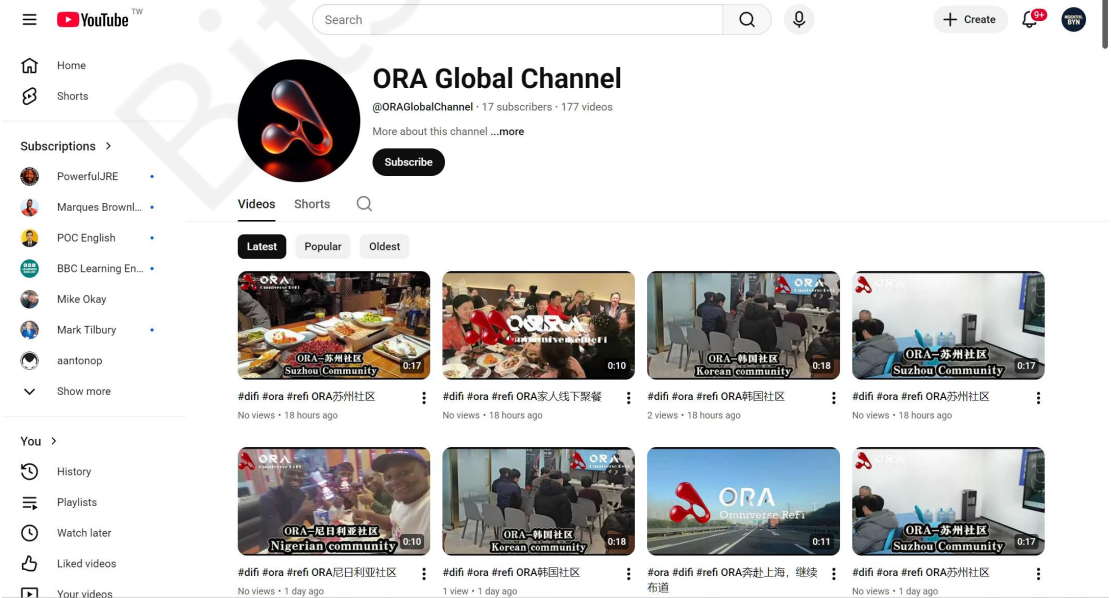
安全性评估：核心合约代码虽已在区块浏览器开源，但由于 **未经过专业审计机构的代码审计**，无法排除逻辑漏洞或溢出风险。



3. 团队背景与社区画像

匿名性风险：项目团队处于完全匿名状态，公开渠道无法检索到任何核心成员的履历信息。

社区构成：尽管项目名为 Global Channel，但 **社群参与者与链上交互地址高度集中于中国地区**，这与代码风格分析结果一致。此类“国人盘”特征通常伴随着较高的运营不确定性。

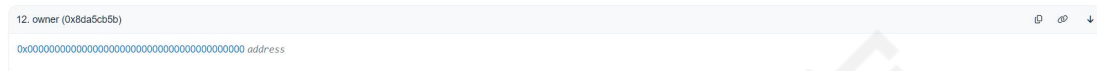


4. 权限与治理结构审计

链上数据确权显示，项目方放弃了部分控制权，但仍保留了关键的运营权限。

已放弃的权限：

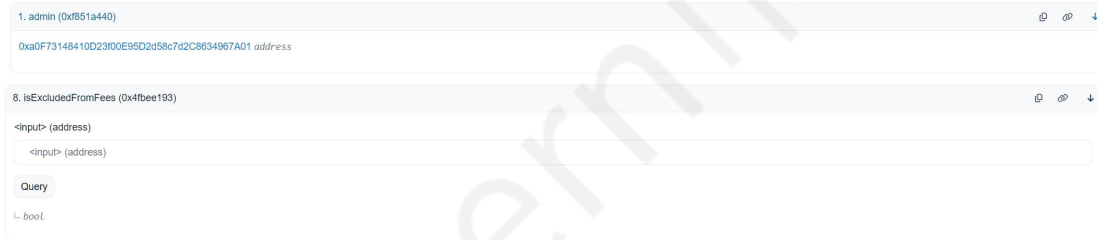
Token Owner: 主代币合约的所有权已移交至黑洞地址（0x00...000），无法再进行增发或修改核心参数。



Stake & Node Contracts: 交互合约与节点分红合约的所有权均已确认放弃。

未放弃的风险权限：

Admin Role: 核心的管理员权限（Admin）仍由普通外部账户（EOA: 0xa0F7...7A01）控制。



白名单机制 (Whitelisting): Admin 账户有权设置免税白名单（ExcludedFromFees）。这意味着项目方可以指定特定地址进行零手续费交易，存在利用该特权进行无损套利或“老鼠仓”出货的风险。

5. 经济模型与可持续性

庞氏结构：项目缺乏外部造血能力（即无真实业务收入），其收益来源完全依赖于后续资金的流入以支付前期用户的利息。这是典型的庞氏（Ponzi）资金盘逻辑。

不可持续性：一旦新进资金流量（TVL Inflow）无法覆盖旧用户的提现需求，流动性将迅速枯竭导致崩盘。该模型不具备长期持有的基本面支撑。

6. 潜在风险研判

市场操纵风险：虽然并未发现直接转移所有用户资金的“硬后门”，但当前的代币分配机制极其有利于早期参与者。项目方极可能在早期埋伏了多个隐形地址囤积大量低成本代币，待价格推高后集中抛售，导致散户资产归零。

综合总结

基于链上数据分析与定性调研，对 ORA 项目的综合评级为 极高风险。

信任基础缺失：项目方宣称的 CertiK 审计被证实为虚假信息，且团队完全匿名，这种不透明性是投资的重大红旗。

伪去中心化：尽管项目方放弃了 Owner 权限以营造“去中心化”假象，但仍通过 Admin 权限掌控着费率白名单等核心利益输送通道，并未实现真正的社区自治。

博弈本质：该项目的本质是一个代码拼凑、面向特定地区（主要为中国社区）收割的庞氏资金盘。目前未发现直接盗币代码，但存在极高的**“控盘收割”**风险。

结论：该标的缺乏真实价值支撑，且存在明显的操纵风险与合规瑕疵，强烈建议规避，不适合任何长线投资策略。

免责声明 本报告基于公开的链上数据及第三方审计结果客观撰写，仅供参考，不构成任何投资建议。区块链项目具有高度动态性，存在代码漏洞、权限变更及市场波动等不可预见风险。请投资者务必独立判断，自负盈亏。报告撰写方不对因信赖本报告而导致的任何资金损失承担法律责任。