01 审计摘要与适用范围

内部 AI 审计 · 公开阅读版 · 2026-09-25

> 本轮未确认新的高危或中危 V7 候选合约漏洞。网站发现的 2 项中危、2 项低危问题已修复，补丁发布于站点 v48。新增 29 组检查和 2 套浏览器验收通过。

本报告由内部 AI 复核与可复现测试形成，不是独立第三方审计、认证、投资建议或安全保证。“未确认漏洞”仅描述本次已检查范围，不能推导为不存在漏洞或不会发生损失。

三条复核路径

- V7 池账务：计息、供应/债务份额、舍入、清算、坏账、储备守恒与全损后的代际重置。
- V7 依赖边界：预言机、奖励分配和领取、原生 BNB 包装、权限及不可替换依赖。
- 现有网站：BSC 钱包发送、交易回执、未知发送状态恢复，以及 V5 → V6 迁移记录和继续流程。

先区分三个版本边界

对象	本报告对应状态
线上 V5/V6 合约	不可升级的既有部署，存在真实借款。第 2 页所列已知问题仍然存在。
V7 候选合约	本地/测试网候选，保留链 ID 31337/97 限制；候选整改没有修改既有部署。
网站 v48	发送、回执与迁移界面的安全补丁；它不是 V7 合约部署或 V7 迁移上线。

本报告冻结于下列源码提交。之后新增的 BSC 主网包装合约、部署参数、角色、地址、奖励配置及迁移实现，必须由单独的生产变更报告覆盖；不得直接沿用本报告宣称已审计。

```
97a422c254cac36ba47e8bf520539c0bae4dd5b9
```

02 当前线上 V5/V6 的已知风险

> 以下是已部署合约的已知行为，V7 候选中的修复不会自动生效。用户应结合自己实际使用的池地址判断风险。

已知行为	对使用者的影响
计息调用频率影响债务	相同初始状态和时长，仅改变计息频率即可改变债务。本地满利用率示例：1000 单位借款一年一次计息为 1900，分 12 次约为 2381.779599。这是规则复现，不是收益承诺。
暂停/上限可阻止补抵押	暂停时供给式补仓被拒绝，而清算仍可能发生；还款仍可执行。
无关资产喂价故障可阻塞风险计算	只持有部分资产也可能因其他喂价过期无法借款、减少抵押或清算；全额还款及无债务退出仍可执行。
全损后的无价值份额阻碍恢复	若旧持有人不销毁无价值份额，储备可能无法恢复新供应；补充风险准备金不等于恢复供应净值。
清算所得可能无法即时兑现	所得为抵押份额；储备现金不足时无法立即提现，且旧清算入口没有最小所得保护。
最后一次部分提现可遗留尘埃	特定舍入边界可烧完份额并留下 1 wei 无主资产，由下一存款继承。

迁移与退出同样受条件约束

现有 V5 → V6 路径要求无债务且旧池有足够现金。新版本也不能自动消除旧债务或创造退出流动性。旧池不能通过管理员直接转移所有用户仓位；每位用户保留自己的资产与奖励领取权。

线上奖励控制器没有未用预算回收机制。角色、预言机和代码不可替换；配置变更延时不等于合约升级。请勿把新池发布理解为旧仓位已经自动迁出。

本报告识别的线上池（BSC，chain ID 56）

`V5 0xa6dfA661EF760E7F81bD6aA9b23B8933bD9027A4`

`V6 0xD905b5e057cd0313b519D47e81609Ccfd58Bcf89`

来源：audit/current/SCOPE.md、audit/current/REMEDIATION.md、audit/current/STATUS.zh-CN.md。历史状态文档用于证明旧部署行为，不作为最新审计进度或对外联系状态的依据。

03 V7 候选合约整改

下面的整改仅适用于本报告列明哈希的候选源码。三份候选合约在本轮追加 AI 审计中未改变，原测试按完全相同的源码身份沿用，另执行针对性的新增边界检查。

问题方向	候选实现与验证重点
计息频率	按固定利率周期起点计算累计复利；公开计息不重置周期。年/月/不规则计息序列对齐。
救援补仓	有债务账户可使用单独、有明确额度上限的补抵押入口；测试暂停、上限、无债务拒绝和已持有抵押的喂价故障。
预言机依赖	仅计算账户实际暴露的正值抵押与债务；相关暴露故障时保守拒绝，不能以猜测价格替代。
全损与代际隔离	零净值且无债务储备可开启新一代；旧无价值份额不能捕获新存款，旧奖励停止状态保留。
清算结果	加入最小份额/资产所得、截止时间和可选原子底层资产支付；现金不足时整体回滚。
最后份额尘埃	拒绝烧掉最后全局份额但仍遗留账面资产的部分提现；使用完整退出路径。
奖励预算	新控制器保护所有已分配奖励，仅在活动结束后按规则把未分配排放退回固定金库；旧控制器不因此改变。

此前候选复核中发现并闭环的问题

• C-01（中危）：注入新的陈旧喂价抵押可阻塞清算。最终供应/开启抵押检查依据实际底层索取权，而不只看份额是否为零；新增正值暴露要求有效价格。

• C-02（中危）：坏账结算接收者聚合零值份额后可能形成未核价的正值抵押。最终结算检查该边界；陈旧价格导致完整回滚，并验证余额/债务不变。

保留并披露的合约限制

C-03：极长时间后的债务可能超出 uint256。已验证 150 年边界下故障储备与无关储备操作隔离，不承诺无限运行年限。C-04 / AC-01：经济事件丢弃不足一个最小原始单位的利息；低精度资产可产生明显偏差。本次范围仅为核验地址的 WBNB、USDT、BTCB、ETH、USDC 五种 18 位资产，扩展精度必须重新设计并复审。

来源：audit/v7/FINDINGS.md、audit/v7/SPECIFICATION.md、audit/ai-current/POOL-REVIEW.md。

04 网站整改与验证证据

编号 / 级别	已发布于 v48 的整改
WEB-01 / 中危	回执核对 BSC 链身份、所在高度的规范区块哈希和至少 3 次确认。迁移继续前重新核对已完成步骤；异常时保留记录并停止。
WEB-02 / 中危	意图和发送请求显式绑定 chain ID 56，在实际交给钱包的边界复核账户/网络。只有本地可证明未提交的阻断可释放新意图；不确定发送保留恢复记录。
WEB-03 / 低危	导出同时保留原始计划、待确认和批量记录及解析诊断；损坏或截断 JSON 不再丢失原文。
WEB-04 / 低危	明确标注 V5 → V6，显示核验的源池/目标池地址，并明确当前页面不提供 V7 迁移。

本轮新增检查：29 组 + 2 套浏览器验收

检查类型	通过数量
池账务边界	4 组
奖励、包装币和不可替换依赖边界	3 组
网站不利条件与 RPC/记录恢复	13 组
独立历史迁移兼容性	6 组
钱包错误来源与未知发送保留	3 组
浏览器市场操作与迁移流程	2 套（另计）

浏览器验收使用无头 Edge、隔离内存 Ganache 和模拟钱包，拦截公共网络请求；不是实际浏览器扩展和真实资金交易。测试过程中未发送主网交易。至少三次确认降低短重组风险，但不等于绝对最终性，仍依赖诚实、一致的 RPC 数据和正确钱包实现。

沿用且绑定相同源码的既有证据

池测试 9 个定向场景及 180 次确定性操作（120 次成功、60 次预期拒绝）；预言机 37 项；奖励 7 组，包含 80 步、3 用户、10 奖励桶的独立模型；陈旧抵押回归 7 项。另有 4 组真实 BSC 资产本地分叉检查，奖励代币为本地测试替身。静态分析保留 149 条原始告警并逐类判断，原始级别不等于确认漏洞数量。

来源：audit/ai-current/WEB-CLOSURE-REVIEW.md、outputs/ai-review/*-results.json、audit/v7/FINDINGS.md、audit/v7/STATIC-ANALYSIS.md。通过测试不能证明所有路径安全。

05 剩余风险与用户自主决定

尚未消除的依赖和操作风险

• 奖励控制器一经绑定不可替换。错误或可变的控制器可能阻塞本金操作；生产部署必须核对确切字节码、角色、资金与参数，不能只检查 pool() 返回值。

• 前端 integration 依赖审计记录为 0 项已知公告；本地合约开发/构建依赖仍有 29 项，其中 27 项位于 Ganache 测试依赖，另 2 项涉及 solc/tmp。这些工具链风险没有被宣称已修复，也不直接等同于链上漏洞。

• Solidity 0.8.30 后续披露并修复的 7 项编译器问题，已按源码及编译设置逐项核对，未找到触发条件。工具链升级会形成新制品，仍需重新编译、核验及测试。

• 代币和桥接资产风险、价格偏离、喂价故障、流动性短缺、清算、坏账、网络拥堵与交易费用可能造成损失。已核验的地址和测试时点不能消除未来外部依赖变化。

不属于本次完整证明范围

普通市场的真实跨标签页钱包竞态、钱包扩展内部实现、托管基础设施与域名控制、所有潜在 MEV/经济攻击，以及冻结提交之后的 V7 主网包装、部署与迁移。复核覆盖有限场景，未执行无限时间、所有状态和所有对手行为的数学证明。

使用前请自行核对

请阅读本报告，核对正在交互的网络、池地址、合约版本、授权对象和金额；理解债务、清算、流动性及不可逆链上交易风险后，自主决定是否使用。使用者需自行承担其交易和持仓风险，包括本金损失；不能把“AI 审计”理解为保本、保收益、保险或机构背书。

> 阅读或下载本报告不触发钱包授权、交易或迁移，也不代表用户已经同意迁移。每笔链上操作仍应由相应钱包持有人核对并签名。风险提示不构成免除项目责任的承诺，也不限制用户依法享有的权利。

后续生产变更应另外披露

实际 V7 主网地址和代码身份、角色及风险参数、迁移窗口与退出/拒绝方式、债务和现金不足处理、旧奖励领取方式，以及生产变更后的复验结果。后续补充材料应有独立版本与哈希；本冻结报告不应被改写成对未来代码的审计结论。

来源：audit/ai-current/DEPENDENCIES-REVIEW.md、TOOLCHAIN-REVIEW.md、REPORT.zh-CN.md 及 audit/v7/RELEASE-GATES.md。

06 附录：冻结标识与复核来源

本次审计源码提交

`97a422c254cac36ba47e8bf520539c0bae4dd5b9`

候选初始冻结基线如下；本轮三份候选合约保持相同源码字节。

`d34b545eabb666aecb0cc6987e137975b984898d`

候选 Solidity 源文件 SHA-256

contracts/candidate/OrbitV7Pool.sol

`372cb8f72af9ed1bf57deb0a65e8e0101549900f773748d4f67690a788edda5c`

contracts/candidate/OrbitV7Oracle.sol

`4d50921366127a5208f135c6a0875be864e5999216b029b8be7b43d02905c5c7`

contracts/candidate/OrbitV7Rewards.sol

`3d20df3d28a25990a2f34607b6888b38796e6843ff17b16a395ac441f94425c3`

编译与分叉标识

Solidity 0.8.30；优化器 200 次；viaIR；EVM Paris；OpenZeppelin Contracts 5.4.0。原分叉证据固定在 BSC 区块 123922439；所有写操作发生于本地链 31337，未向主网发送交易。

`0xf7e55d94373cd79108b57edc3a42f7ada265488465f8518d3e83f12633c84974`

主要来源（仓库相对路径）

audit/ai-current/REPORT.zh-CN.md
audit/ai-current/POOL-REVIEW.md
audit/ai-current/DEPENDENCIES-REVIEW.md
audit/ai-current/WEB-MIGRATION-REVIEW.md
audit/ai-current/WEB-CLOSURE-REVIEW.md
audit/ai-current/TOOLCHAIN-REVIEW.md
audit/v7/FINDINGS.md、SPECIFICATION.md、STATIC-ANALYSIS.md
audit/current/SCOPE.md、REMEDIATION.md、STATUS.zh-CN.md
outputs/ai-review/accounting-results.json、boundaries-results.json
outputs/ai-review/web-safety-results.json、web-history-closure.json
outputs/ai-review/web-local-handoff-provenance.json、browser-results.json
outputs/v7/fork-results.json

本公开阅读版根据冻结材料编写，清除私人联络及本机目录信息；它是风险和证据摘要。源码哈希用于识别审计对象，随附 SHA-256 文件用于核对下载文件完整性；文件哈希本身不是审计认证。