

01 生产增量与实际发布状态

内部 AI 复核补充 · 公开阅读版 · 2026-09-25

V7 主网交易尚未签名。公开清单为 not-deployed，没有 V7 主网地址或部署回执。网页发布不等于链上池已部署，也不等于用户资金已迁移。

本材料补充此前冻结的 V7 候选与网站整改报告，单独记录主网包装器、固定参数和迁移界面的新增内容。它是内部 AI 复核，不是第三方审计、认证或资金安全保证。原候选报告及其哈希保持不变。

部署与开放需要五笔钱包交易

步骤	作用与签名边界
1. 部署预言机	创建固定 BSC 五资产喂价配置的 V7 主网预言机。
2. 部署池	创建初始暂停的 V7 池，构造时核验预言机代码、配置和价格缩放。
3. 部署奖励控制器	创建未注资的 V7 奖励控制器；不铸币、不划拨新奖励预算。
4. 绑定控制器	由治理钱包执行一次性绑定；绑定后不可替换。
5. 首次开放池	由治理钱包执行首次 unpause，开始借贷与 30 天集中迁移窗口。

每笔等待规范区块及至少三次确认。页面在绑定前核对精确创建代码、参数、签名者、CREATE 地址、运行码与不可变身份；异常或未知发送状态保留记录并停止。链上身份、钱包和浏览器材料的最终验收另见单列网页增量复核。

公开部署身份以链上核验为准

只有经链上回执核验并正式发布的清单才可称为公共 V7 部署。浏览器本地清单用于核对，不能替代公开发布。部署与开放不会替用户搬走旧池资产；用户迁移仍需原钱包逐笔签名。

与前一份报告的关系

此前审计源码提交：

97a422c254cac36ba47e8bf520539c0bae4dd5b9

本补充报告以第 5 页列明的最终生产源码及证据哈希为边界，不把早先候选审查自动扩展到后续任何代码。

02 合约增量、修复与测试

生成主网核心与冻结候选池逐字比较，仅替换抽象合约声明/名称和构造链约束，并增加生成说明。会计、计息、清算、补抵押、原生资产转账及权限函数体保持不变。Oracle 和 Rewards 通过继承复用。

固定生产边界

仅允许 BSC chain ID 56；固定 WBNB、USDT、BTCB、ETH、USDC 五种 18 位资产、治理和守护角色、现有 ORBIT、金库、喂价及初始风控。紧急补抵押上限为初始普通存款上限的两倍，且仅有债务账户可使用。

PV7-01 / 中危 / 已修复

仅比较运行码不能证明预言机的构造存储正确。恶意构造代码可产生相同运行码，却写入不同公开配置或隐藏缩放值。最终池构造同时核验运行码、五组完整配置，以及独立读取固定 feed 后按 $\text{answer} \times 1e10$ 得到的归一化价格。

回归实际部署两种相同运行码克隆：错误有效期和仅修改私有 scale。两者自身均能返回价格，后者的全部公开配置也相同；最终池构造均拒绝。问题在主网部署前闭环。

独立复核和测试结果

- 另一内部 AI 复核任务独立编译三个标准输入；创建码、运行码、ABI、元数据与归一化后的不可变字段偏移完全一致。
- 9 组生产合约本地检查通过，覆盖固定配置、错误依赖、恶意预言机克隆、角色与参数、绑定/开放权限、无新奖励的存借还提、真实暂停补抵押和错误链拒绝。
- 最终产物在 BSC 区块 123938837 的本地分叉通过五种真实资产/喂价配置检查，以及实际 WBNB 存入、借出、还款退款、完整退出和会计守恒。其余四种资产在本轮未逐一执行真实转账循环。

0xb27b7d0a5a58c098845661ffc4f4085964906be89619c7a0130dfe825364c443

公共链发送交易数为 0。分叉中的角色模拟不是主网签名；现有 ORBIT 代码存在性得到核验，但本轮不注资、不转移 ORBIT，也未新增真实 ORBIT 发奖兼容性证明。

完整配置与原始证据见审计页的固定参数 JSON 和主网适配增量复核材料。通过测试不等于不存在漏洞。

03 30 天迁移与零新增奖励

窗口如何计算

集中迁移窗口为 30 天：从 V7 首次已核验 unpause 区块时间开始，到该时间加 2,592,000 秒结束。后续恢复开放不能重置窗口。没有真实开放回执时显示“尚未开始”。

到期后继续保留旧池还款、退出、领奖和手动迁移入口。期限不创造自动代迁权限，不强制转移资产，也不保证旧池具备足够流动性。

每次迁移由原钱包决定

- 用户可拒绝迁移并保留旧仓位，也可只提现退出。旧 V5/V6 没有 keeper 授权或管理员转移用户仓位的能力。
- 流程为旧池提现、精确授权 V7、存入 V7，由原钱包逐笔确认。迁移仅使用这笔提现回执的实际数量，不包括钱包已有余额。WBNB 作为 ERC20 处理，不混用钱包 BNB。
- 旧债务需先偿还；旧池现金不足、新池额度不足或健康检查失败时停止。提现后若中断，资产可能已到用户钱包，应恢复原进度后继续。
- V5/V6 → V7 使用按来源隔离的新记录键。原 V5 → V6 恢复入口及原记录保留，未知发送不能当作“未发生”而自动重试。
- 迁入沿用源仓位的抵押开关；这会影响 V7 中该资产的整个仓位。已有 V7 债务时尤其应核对抵押状态，合约健康检查仍生效。

本次开放不新增 ORBIT 奖励

不发行代币、不注入新奖励预算。旧奖励仍由原钱包在旧控制器领取，旧控制器剩余预算不能迁走。V7 保留未来经治理启动奖励的代码能力，不能把本次“无新增奖励”理解为永久删除 fund 能力；本次没有执行该资金划拨。

遗失私钥不属于补抵押救援

提款和领奖权属于原钱包。若私钥、助记词及全部有效恢复方式丢失，Orbit 不能代该地址提款、领奖或迁移；身份证明和转账截图不能替代签名。借贷、计息和清算仍按链上规则执行。rescueCollateral 仅指借款人补充自己的抵押，不提供私钥找回或管理员代提。

04 网页保护与尚存限制

补充保护检查：27 项通过

新页面沿用显式 chain ID 56、签名前账户/网络复核、规范链三次确认、精确交易内容与提现回执金额核验。新增 V7 跨页面活动锁和持久化未知交易的跨流程阻断。27 项补充检查覆盖持久记录隔离、回执排列和 30 天窗口语义。

V7 清算界面使用八参数入口，把最小所得份额/资产、收款方式和截止时间写入交易。授权后可只读试算，填入 0.5% 所得容差及十分钟截止时间，用户可调整。静态试算不是发送交易或收益保证；直接领取底层代币时现金不足则整笔回滚。

借款报价按相关资产读取价格；借款 APR 为名义利率，债务按秒复利。参考年成本假设全年利率不变，不构成固定成本承诺。

最终浏览器及迁移验收由单列“网页增量复核”记录，可在审计页下载。本补充 PDF 不把尚未纳入的最终浏览器结果宣称通过。隔离链和模拟钱包测试不能覆盖全部真实扩展、网络故障、跨设备状态或攻击路径。

治理与依赖边界仍然存在

- 奖励控制器一次性绑定且不可替换。链上入口只强制控制器有代码并指向本池；合法治理钱包误绑其他控制器可能阻断本金操作，网页核验无法阻止管理员绕过网页直接签名。
- 角色不可轮换，喂价不可由本池管理员替换。治理密钥丢失或滥用、喂价故障/升级、桥接资产脱锚、清算、坏账及流动性不足均可能造成损失。
- 旧 V5/V6 的已知问题继续存在。V7 不会自动修复旧债务、创造提现现金或接管旧奖励。此次生产增量复核也没有重新执行此前每一项性质测试或所有经济路径。

自主决定与签名

请阅读报告并核对网络、池地址、合约版本、授权与金额后，自主决定是否使用，并承担相应交易和持仓风险，包括本金损失。阅读或下载不产生授权、签名或迁移。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。

05 附录：生产源码与制品身份

下列 Solidity 文件相对 contracts/release-v7/; SHA-256 绑定本次最终生产适配源码。文件或编译设置改变后，应重新绑定验证证据。

OrbitV7MainnetCore.sol
fb8889636993393109e291dad01a4ad621933d66e50942655343d55798116f60

OrbitV7MainnetConfig.sol
09053068613ac3f0904bf9c8ced0f5815ecec771b0b284926cbc0db72eefbdcb

OrbitV7MainnetOracle.sol
fe79adb15c2247e859b7b914996079753f009410783f28af4137e1f4cb7972d6

OrbitV7MainnetPool.sol
43a46bddf3d993d188224ccc9dc83f72ba1e9596b9af0ae137d125129eab69dd

OrbitV7MainnetRewards.sol
8f019025c38e98258eb4b826aec6cddb25c9f3cf9168c3f94b3883792718bea0

创建代码 Keccak-256（不含构造参数）

OrbitV7MainnetOracle · Runtime 1,738 字节
0x8b30772bf611ea6cd895a45e215dda8ba1a35dc6991368d4eb22912341b6079c

OrbitV7MainnetPool · Runtime 21,572 字节
0x5ce5dfffc1c8777a57d662f5a0942f2a26e6a53a8221147fe1009e152cc1225a

OrbitV7MainnetRewards · Runtime 5,462 字节
0xebcb953d0b0ad540c3a51301c7156d09049a6ca9ec5af6c27110d736906b0e06

固定初始配置身份

0x909a6e74b587a0872ce4eafe9070b6f3fa656cf474b69a104e4873f60b7d9cc7

initialConfigurationHash 覆盖供应/借款上限、风控参数和补抵押上限。完整参数应与审计页 v7-parameters.json 一并核对。编译：solc 0.8.30、optimizer 200、vialR、Paris、literal source metadata。

来源与下载材料

integration/audit-public/v7-production-review.md
audit/production-v7/INDEPENDENT-DELTA-REVIEW.md
outputs/production-v7/build.json
outputs/production-v7/local-test-results.json
outputs/production-v7/fork-preflight.json

审计页另提供主网适配复核、固定参数 JSON 和网页增量复核。此 PDF 仅是公开补充摘要，文件 SHA-256 用于核对下载完整性，不是第三方认证。本报告不包含私人联络资料、本机路径或任何私钥。