

Code Review 记录

🔒 脱敏示意样本

支付回调重试 PR 复核 · 产研搭档(AI Staff) 出品

复核对象	支付回调重试 PR	时间	演示 · 15:45
复核角度	正确性/并发/幂等/资金一致性	状态	复核意见 / 待研发采纳
数据口径	脱敏演示(不含真实代码与仓库信息)	保密	公开可见样本

01 复核对象与背景

项	内容
范围	支付回调处理 + 失败重试逻辑 + 退款子任务
背景	PR 为支付回调新增失败重试,作者请求合并前复核
复核角度	正确性 / 并发安全 / 幂等 / 资金一致性

02 发现的隐患

#	隐患	严重度	影响
1	重复回调无幂等键,重试叠加渠道重推	高	重复入账 / 重复扣款
2	「取消」与「支付成功」并发无锁	高	状态被后到回调覆盖,状态错乱
3	退款子任务失败仅 log 不重试	中	静默漏退,资金对不平

03 逐项分析

- 1 · 重复入账** 渠道在超时/网络抖动时会重推回调,新增的重试逻辑本身也会再触发。两者叠加、又没有以订单号+渠道流水号为幂等键去重,同一笔可能被入账多次。
- 2 · 状态覆盖** 用户「取消」与渠道「支付成功」在毫秒级并发到达时,若不加行锁/乐观锁与状态机校验,后到的回调可能把终态覆盖成非法状态(如已取消被改回已支付)。
- 3 · 静默漏退** 退款子任务失败仅打日志、无重试与告警,退款会静默丢失,直到对账才发现,且难以定位。

04 修复建议

方向	做法
幂等	以 订单号 + 渠道流水号 为幂等键,入账前查重,命中即幂等返回
并发保护	回调处理加行锁/乐观锁 + 状态机合法迁移校验,非法迁移直接拒绝
退款可靠性	退款失败进重试队列 + 退避,超限告警转人工,不静默
可观测	关键路径埋点 + 对账兜底,异常可回溯

05 边界声明

- 以上为复核意见,供作者与 reviewer 判断
- 是否合并、是否改动核心状态机、何时上线由研发团队拍板
- AI 不批准合并,也不直接改状态机,只做复核与留痕

附:脱敏说明 本文为对外展示的脱敏示意样本,其中主体名称、比例、金额、通过率、指标等均为演示数据,不对应任何真实客户或真实业务结果。实际项目的口径、数值与结论以对应负责人与客户共同确认为准;相关业务与决策权始终在客户与相应负责人,AI 只做辅助与留痕。