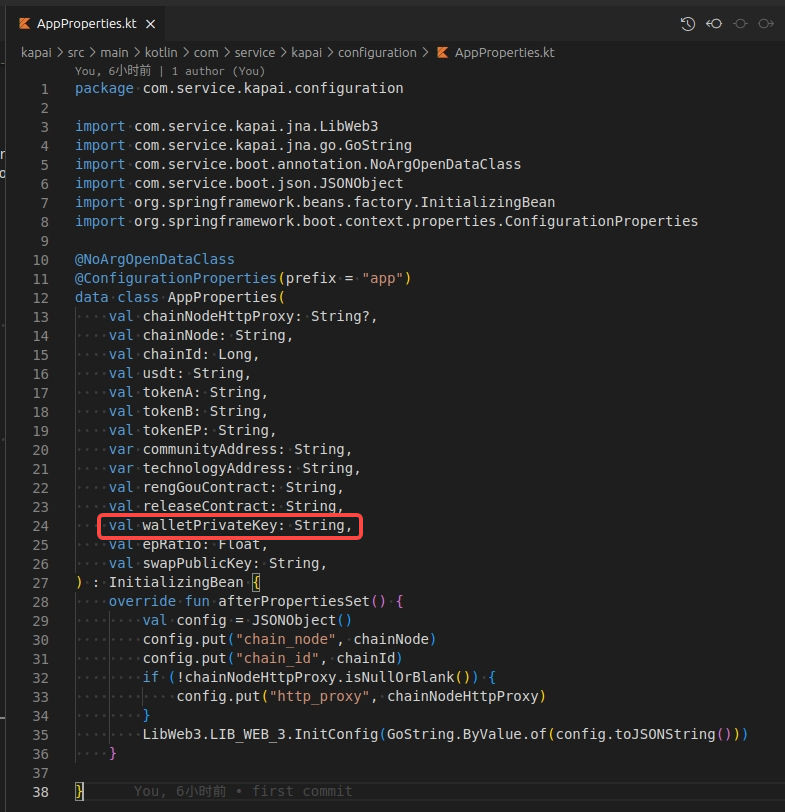
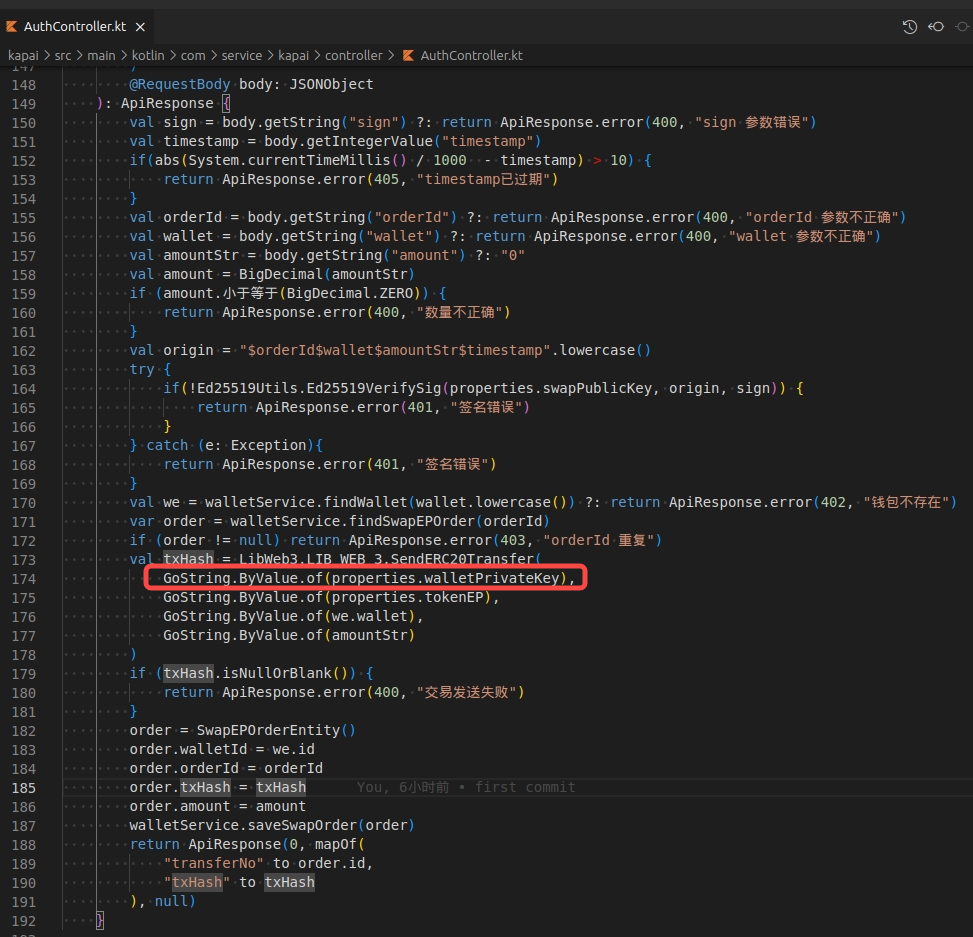
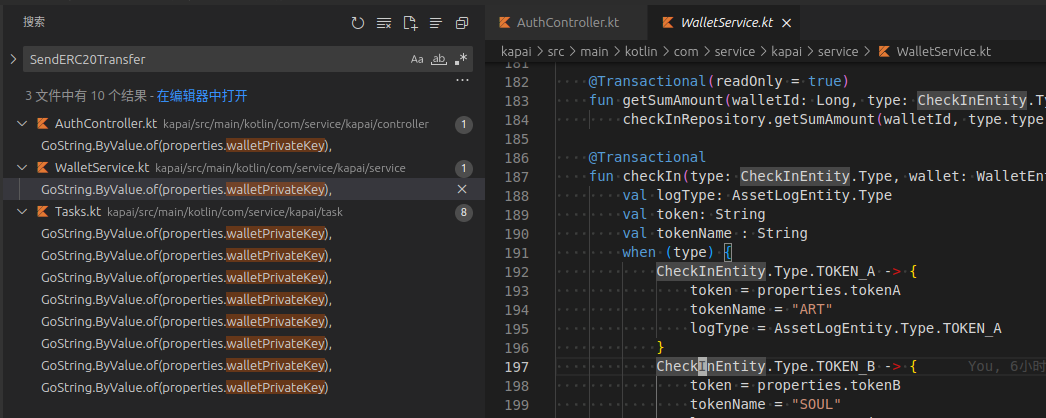
## 问题1：钱包私钥以明文格式写在配置文件中

kapai/src/main/kotlin/com/service/kapai/configuration/AppProperties.kt



kapai/src/main/kotlin/com/service/kapai/controller/AuthController.kt

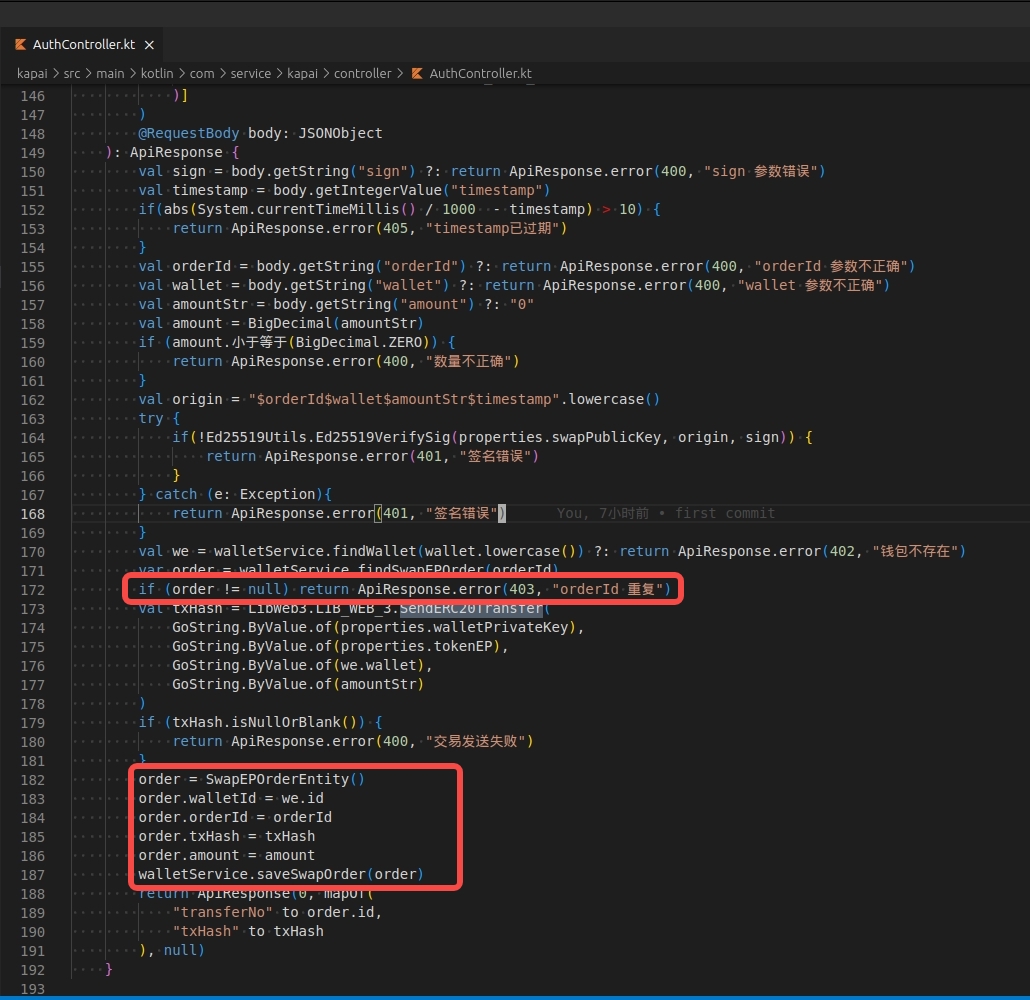




修改建议：

对私钥进行加密处理，并将加密后的密文私钥放在环境变量中，程序从环境变量中读取加密格式的钱包私钥，然后解密

## 问题2： EP兑换订单处理

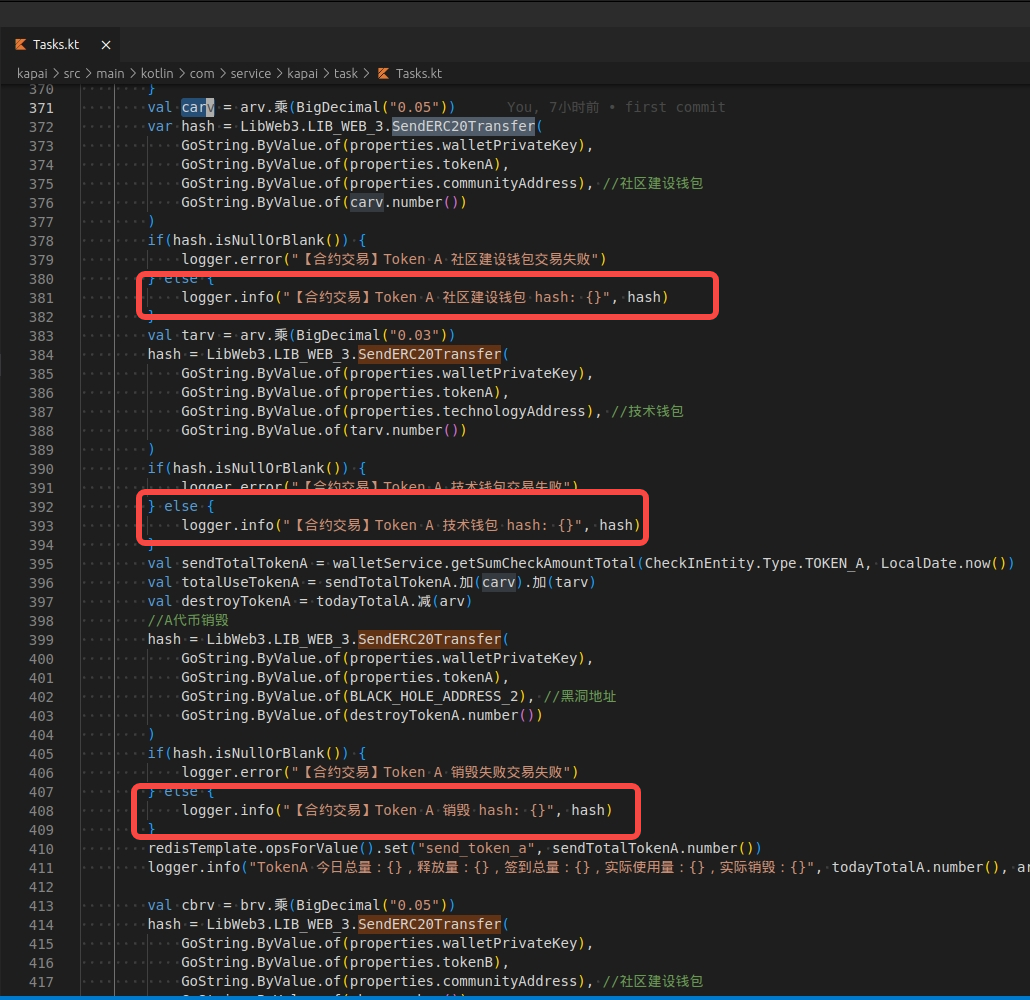


修改建议：

1. 签名验证通过之后，应该先存订单信息，然后再处理兑换订单并发送兑换交易

## 问题3： 分红失败，没有进行重试

kapai/src/main/kotlin/com/service/kapai/task/Tasks.kt

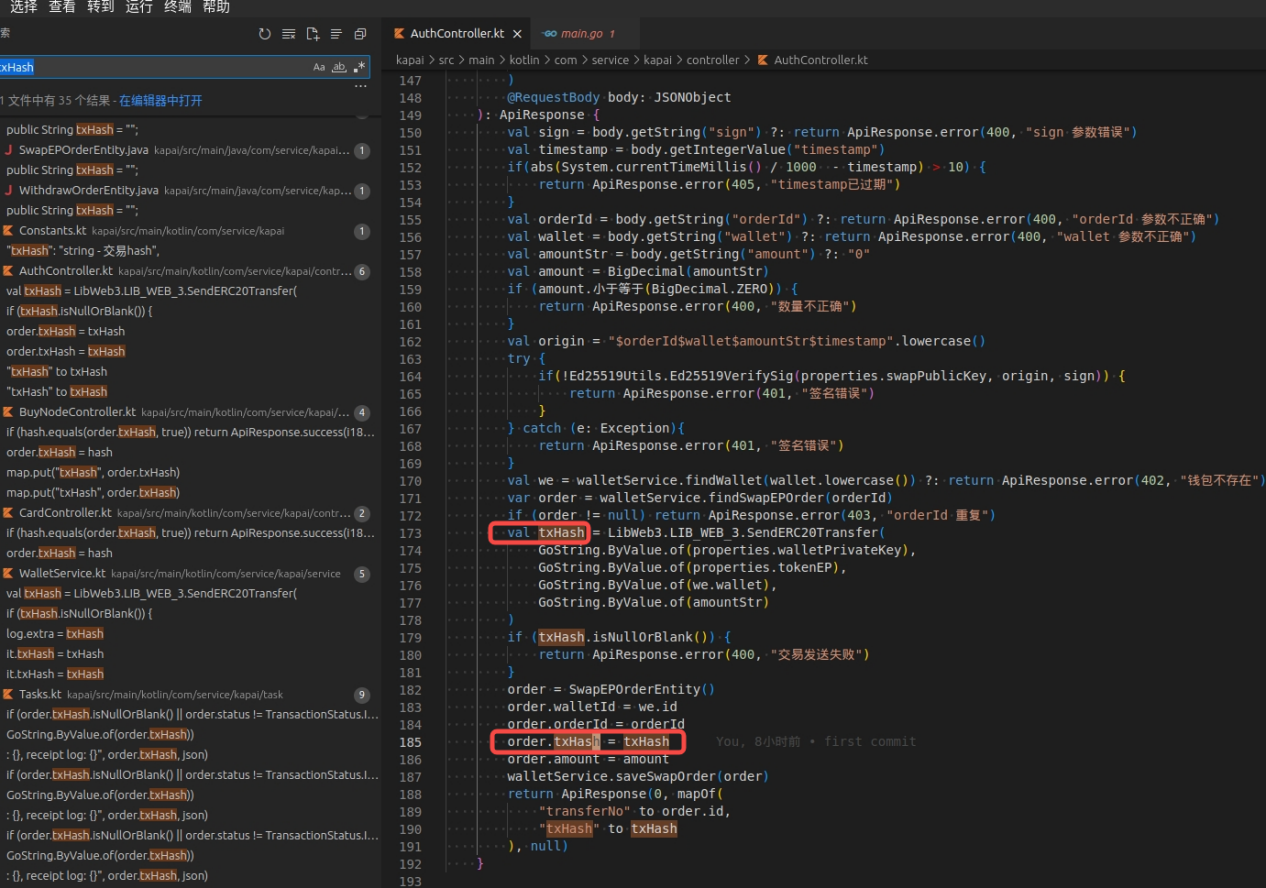


修改建议：

对分红失败的交易进行重试，同时要避免重复发送交易

## 问题4： 交易发出后，没有对交易状态进行跟踪

BSC链上，交易发出到交易最终被确认，需要1～6s的时间，交易可能会失败

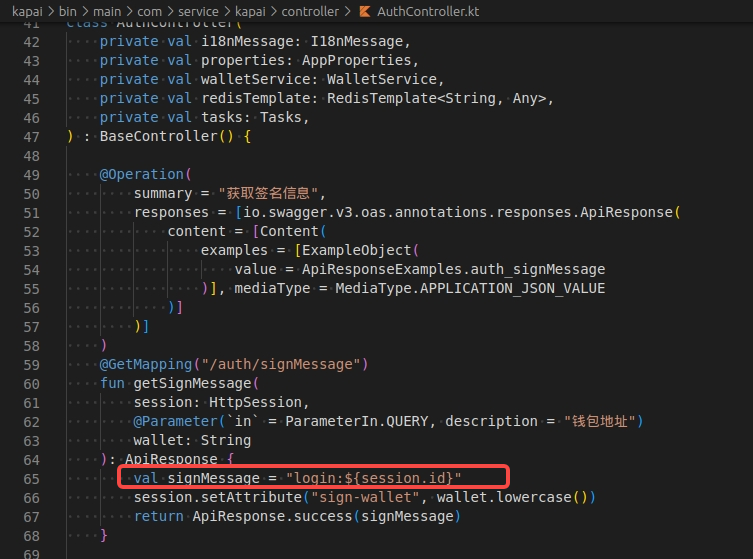


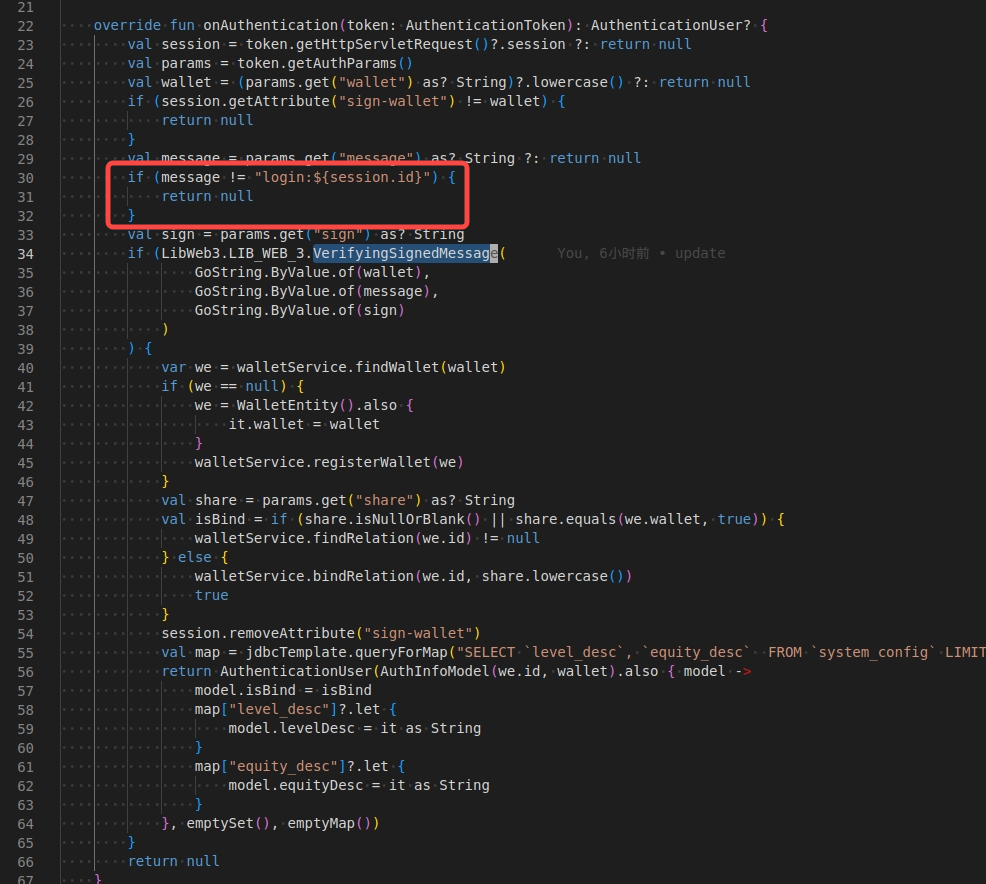
修改建议：

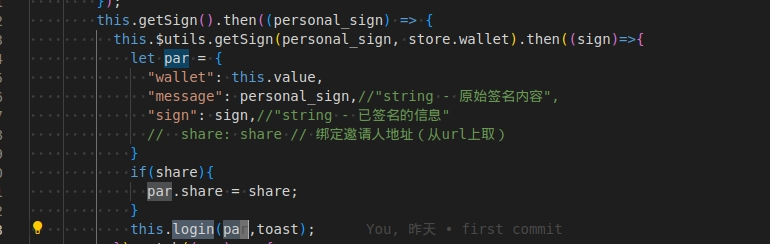
异步跟踪交易状态，只有当交易发送成功后才能将订单设置为成功

## 问题5： **登录签名消息存在安全风险**

目前签名消息**仅仅依赖**sessionId ，安全性不够高，因为存在**会话劫持**和**会话固定**的攻击







修改建议：

* 在签名消息增加：一个大随机数，一个当前时间戳，钱包地址，