**二次密钥方案讨论**

大体方案说明：

1. 抵押账户A0（主账号）每次发抵押交易时带上A1（子账号）
2. A1可以发送委托交易，形式为A2【账户（签名账户），高度】

故需对签名服务和验签服务提供接口（孙春风）

1. 签名相关
   1. 根据高度获取签名账户
      1. （郑贺提供接口查询）若获取成功，去配置中拿签名账户的密码，拿到密码则返回签名账户和密码，拿不到返回异常，
      2. 若获取失败，去配置里拿A1的密码，拿到密码则返回签名账户和密码，拿不到则返回异常
2. 验签相关
   1. 根据高度和签名账户，返回抵押账户
      1. 根据高度和签名账户，查找该账户是哪个抵押账户的子账户发的抵押交易

在此基础上需要网络层支持（郑贺支持）

1. 根据高度获取签名账户
   1. 若存在委托交易，则返回委托交易里高度对应的签名账户
   2. 若不存在委托交易，返回空账户
2. 根据签名账户和高度，返回抵押账户
   1. 若签名账户和高度匹配，查找其子账户，再根据其子账户返回签名账户
   2. 若不匹配，返回空账户