毕业设计答辩问答记录

题 目：基于秘密共享的多方协作撮合服务系统设计
答辩人：廖添

Q1. 秘密分割与秘密共享是什么关系？

秘密共享是指通过某种方式将秘密拆分成若干碎片，使得参与者都拥有一部分碎片，这些碎片会在达到还原条件时可以被还原为拆分前的秘密。因此，秘密分割是完成秘密共享当中的一个关键过程，另外一个是秘密还原过程。

Q2. 使用到了哪些密码学方法？

对称加密算法有 AES，非对称加密算法有 RSA、ECC。其中，RSA 和 ECC 主要用于对 AES 的密钥交换的过程进行加密，通过 AES 对数据内容进行加密。

Q3. 区块链技术用在毕业设计的什么方面？

为了实现整个系统的去中心化模式，同时也保留用户账户模式所能带来的优势，将系统中所有的身份认证工作全部托管给 BaaS 认证平台，该认证平台使用了区块链技术对数据控制进去中心化，从而保证了整个系统的去中心化程度。