会 议 记 录

**会议主题：**区块链及信息安全研究组第二次会议

**会议时间**：2020年7月24日下午15时00分

**会议地址**：腾讯会议 会议号：425291725

**主 持 人**：宋伟老师

**记 录 人**：王文相

**参与人员**：

老师：宋伟老师、吕庆浩老师、李华老师、申会民老师、王瑞民老师、卓伟老师

学生：李书霞、王文相、省永续、王有恒、邱晓梦、李际明、蒋黄伟、李乐言等

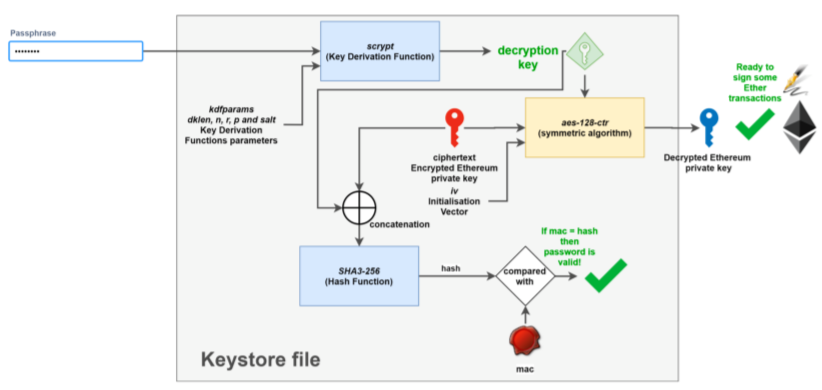
**会议内容:**

**宋伟老师：**

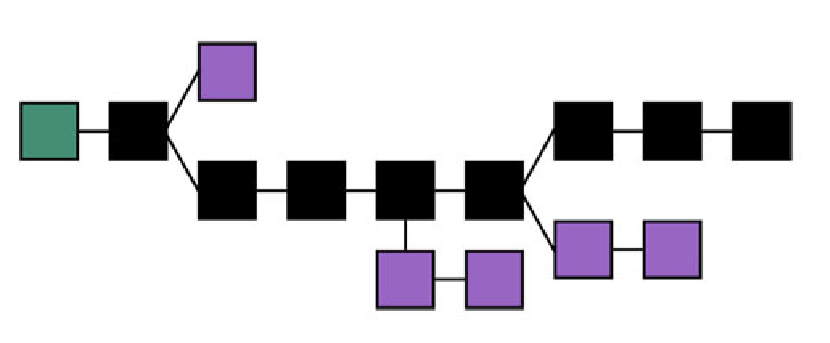
宋伟老师首先对本次会议的主要内容进行了介绍：由吕庆浩老师对《区块链技术概览》进行讲解。

**吕庆浩老师：**

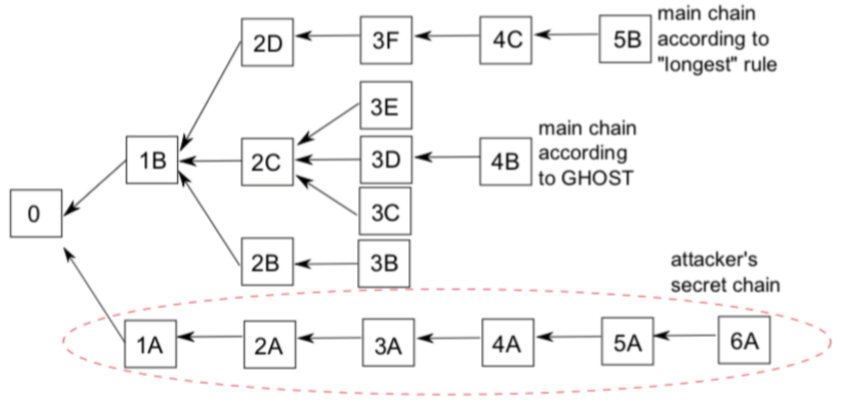
吕老师在会议开始首先对区块链中包括私钥、公钥、地址、助记词等概念进行了简单的讲解，并且对它们之间的联系进行了详细的阐述，并且就MD5和HASH的对应问题与王瑞民老师进行了深入的交流。在会议第一部分吕老师尤其强调了“keystore”概念，Keystore文件是以太坊钱包存储私钥的一种文件格式(JSON)。它使用用户自定义密码加密，以起到一定程度上的保护作用，而保护的程度取决于用户加密该钱包的密码强度。Keystore结构如图所示：



在会议第二部分，吕老师首先从客户和系统两个角度分别讲解了区块链系统，也让大家对区块链系统有了不一样的认识，之后吕老师讲解了比特币系统的交易流程和共识算法，并且就共识算法的目标：主链选择，对比特币系统和以太坊系统的主链选择进行了重点讲解，简单来说在比特币系统当中采用的是“最长链优先原则”，在以太坊系统中每当我们面临分叉时，只要某个分支上具有的验证者（即为该分支的当前和以往区块做证实的验证者）比其它分支都要更多样，我们就认为它是应该被选择的分支。它们的结构图分别如下:



图表 1“最长链优先原则



图表 2以太坊GHOST协议

在会议第三部分，吕老师对公有链、私有链、联盟链三种链类型分别进行了简单的讲解。之后又对共识算法中的BFT、PBFT进行了讲解，并且对POS算法提出了自己的观点。并且在会议最后吕老师对本次会议讲解的内容进行了回顾和总结。

**宋伟老师：**

在会议最后，宋老师表示了对吕老师本次会议讲解的感谢，并且对学生提出要求：根据自己的兴趣进行分组以方便接下来查阅资料和进行深入研究。