听《Foundational Aspects of Blockchain Protocols》有感

2018年11月19日报告会邀请了德克萨斯州农工大学著名教授Juan Garay关于区块链协议基本的思想展开分享，报告共一小时，对于没太多接触过该技术的我来说，受益匪浅。

Juan Garay教授绝对称得上是安全、加密领域的大牛，他于宾夕法尼亚州立大学计算机科学与技术专业博士毕业，在魏茨曼科学研究学院攻读博士后，同时，他在IBM的研究总部——湯瑪士·Ｊ·華生研究中心、贝尔实验室、美国最大的固网电话服务供应商AT&T、雅虎公司等均做过研究。2017年秋，他成为德克萨斯州农工大学全职教授。他的研究领域涵盖了加密与信息安全的理论基础以及上层应用，在加密、网络安全、分布式计算等等领域内发表了大量高水平论文。同时，他也参与了多个安全系统的设计、分析以及实现，拥有24项专利。Garay教授还是多个会议的成员，包括2013年-2014年出任顶级会议Crypto的联合主席。最近，他成为国际密码学研究组织（IACR）的成员之一。

在报告中，Juan Garay教授讲述了区块链协议的几个基本性质，包括公共前缀、区块链的质量以及区块链的增长方式。同时向我们详细阐述了如何利用区块链协议构建如一致性保证等上层应用，并且着重说明了此技术是基于“对手的哈希计算能力远远低于比特币体系”。这项技术是现代密码学——基于复杂性理论的密码学理论的成功应用。

具体来说，区块链是一套去中心化的分布式认证机制，它利用了哈希算法以及共识机制，以比特币举例来说，他的大体流程是第一步：每一笔交易为了让全网承认有效，必须广播给每个节点（node：也就是矿工）；第二步：每个矿工节点要正确无误的给这十分钟的每一笔交易盖上时间戳并记入那个区块（block）；第三步：每个矿工节点要通过解SHA256难题去竞争这个十分钟区块的合法记账权，并争取得到二十五个比特币的奖励（头四年是每十分钟五十个比特币，每四年递减一半）；第四步：如果一个矿工节点解开了这十分钟的SHA256难题，将向全网公布ta这十分钟区块记录的所有盖时间戳交易，并由全网其他矿工节点核对；第五步：全网其他矿工节点核对该区块记账的正确性（因为他们同时也在盖时间戳记账，只是没有竞争到合法区块记账权，因此无奖励），没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块单链，也就是比特币支付系统的总账--区块链。一般来说，每一笔交易，必须经过六次区块确认，也就是六个十分钟记账，才能最终在区块链上被承认合法交易。

基于此，区块链着重需要解决“双花”以及“拜占庭将军”问题，在现用算法基础上，需要制造假账（即人为构建区块）需要控制控制全球 51% 的算力，正是这个苛刻的难度保证了比特币体系的正常运行。