**活动回顾--『协议学院·上海·技术沙龙』第三期**

（内附大量插图）

2019.6.15日上海浦东新区，由协议学院（ProtoSchool）上海分院主办，**IPFS原力区承办**的「技术沙龙·第三期」与众多技术大咖齐聚松林路97弄海怡别墅41号。该活动是一个非营利的社区学习活动，面向开发者和技术人员，分享和传授DWeb相关的数据结构、协议、算法以及工具等知识。

本期沙龙现场从【IPFS的Web开发】、【区块链的椭圆曲线密码学】，以及【Filecoin的预期共识（EC）】等多主题进行深度交流、探讨与互动答疑。



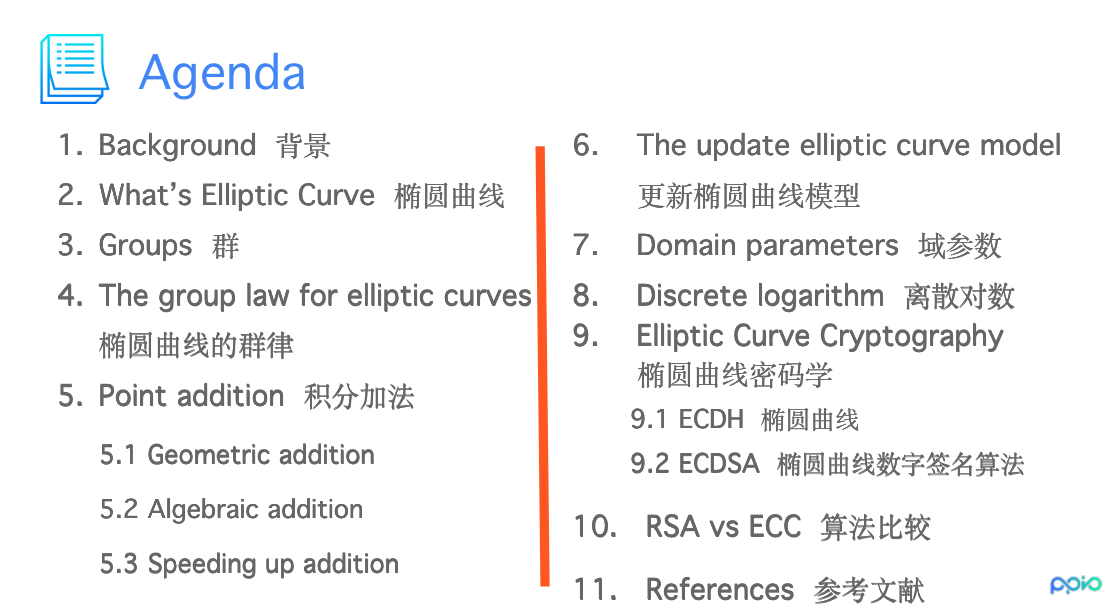
当天活动由原力区COO—Adeline Sun主持。她对远道而来的嘉宾及参会者表示欢迎，并简要介绍了IPFS原力区及本次活动议程，随后开始了参会者自我介绍环节。

本次活动分享嘉宾分别为来自IPFS原力区的李昕、来自PPIO的蒋鑫和来自西安元知慕语的骞永军，以下为活动内容回顾。

**Part I**

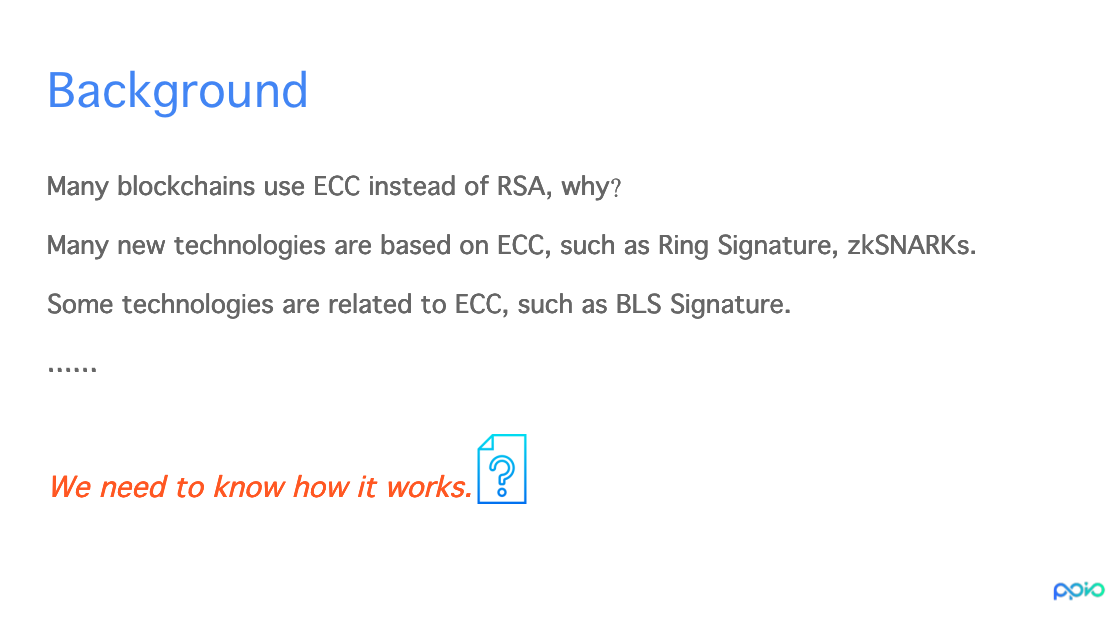


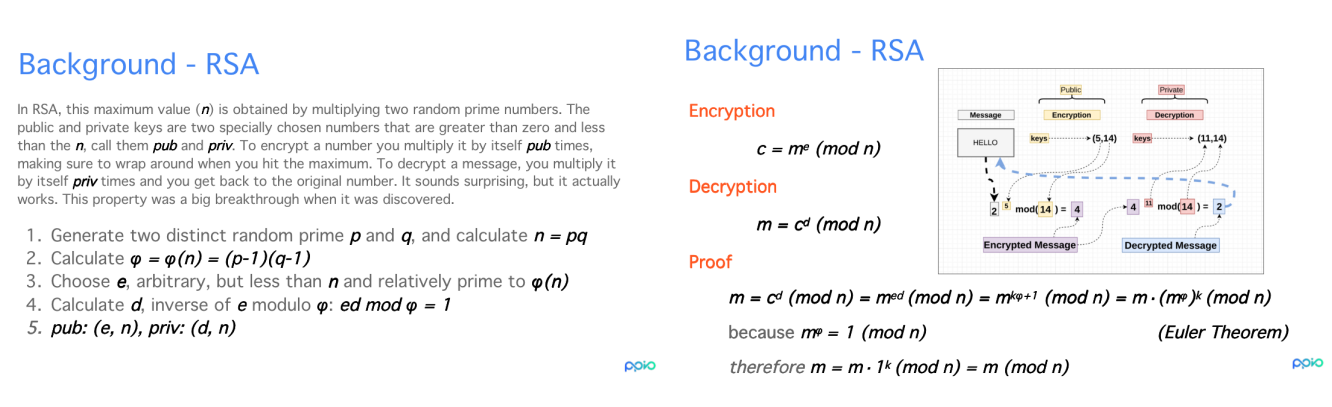
首先，来自PPIO的高级工程师蒋鑫作为第一个演讲嘉宾，带来关于《椭圆曲线密码学》在区块链加密与验证的相关解读。

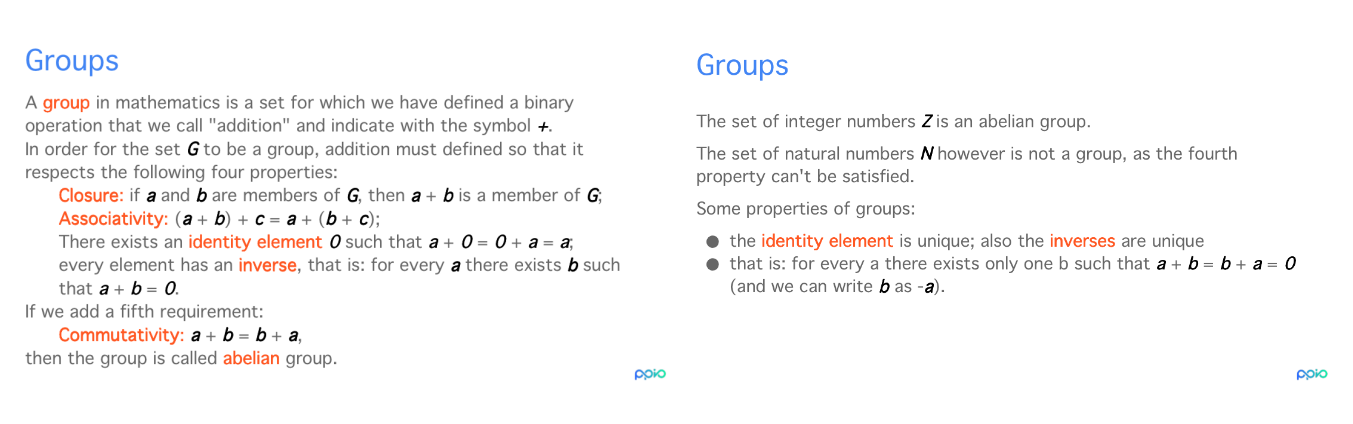
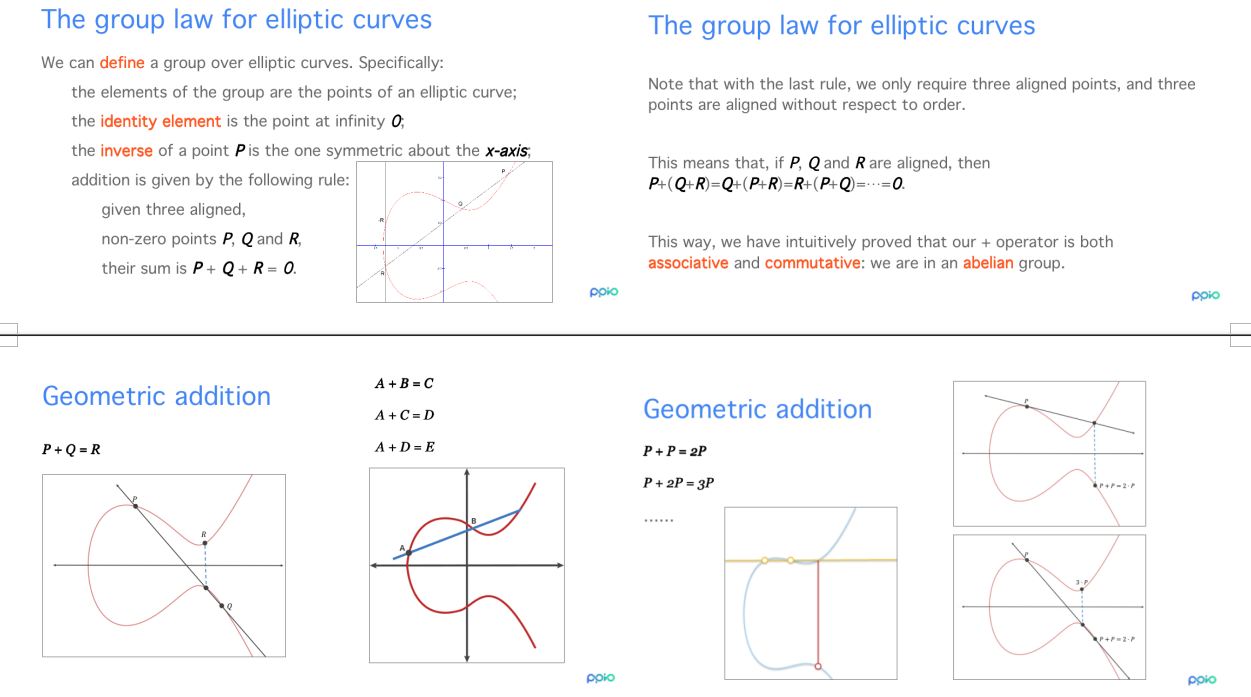


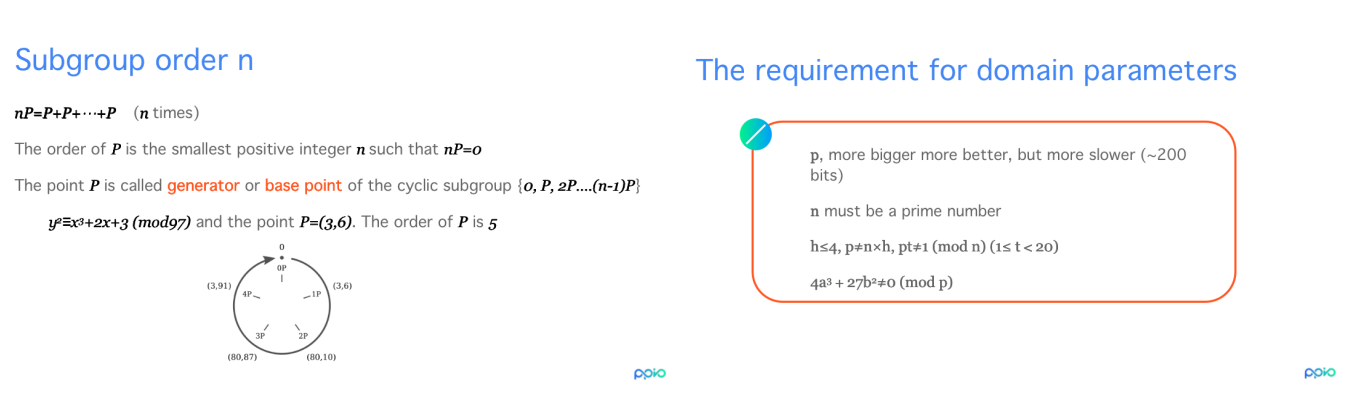
（目录）

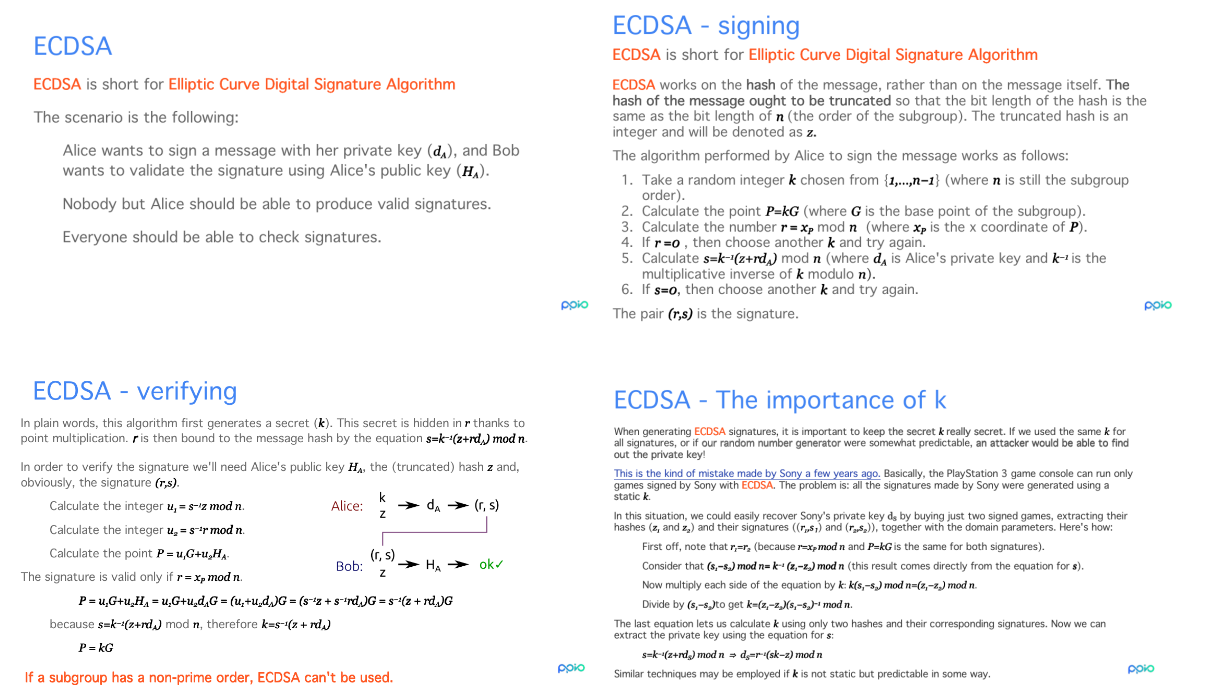
蒋鑫提到：区块链的原签名、零知识证明都需回归到椭圆曲线，要搞清楚这些问题，就要先搞清椭圆曲线问题。

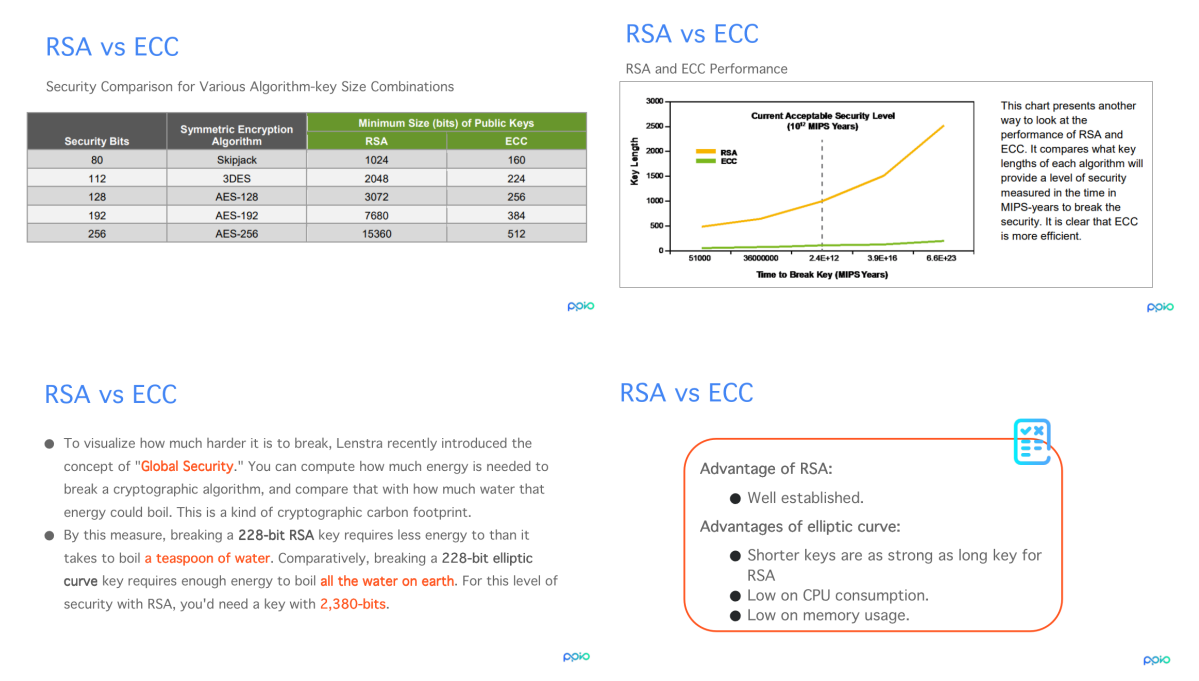


从加密函数RSA着手，讲解了RSA函数里p、q、n的数据解密和数据重组逻辑过程。

从Groups群‘零圆’与‘逆圆’到通过“p+q=r”获得椭圆曲线的运算逻辑。

椭圆函数的阶及其点的确定过程，以及找到好的椭圆曲线的特性，通过更好的椭圆曲线函数提升加密性能。

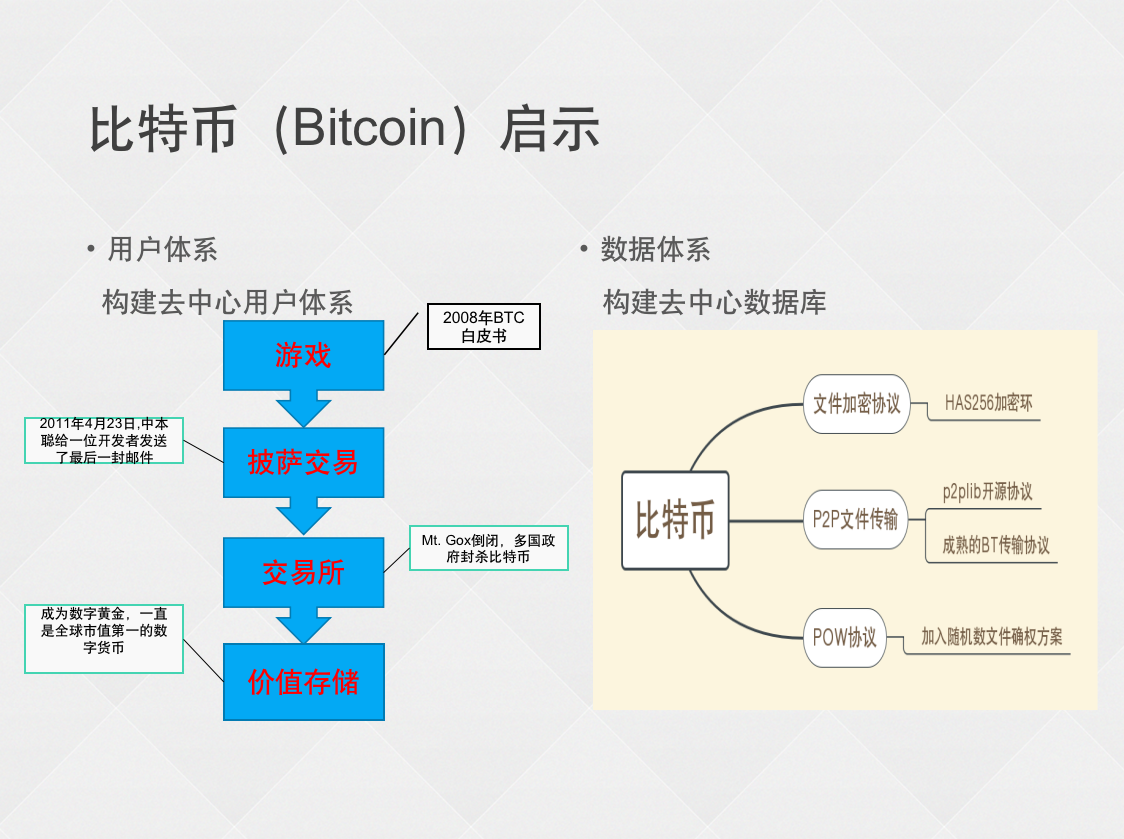
其中，离散曲线算法+对称密钥技术，是用在数据传输这一环节的验证功用：Q=“K”P。已知Q、P的情况下求K。例如：Bob代号「A」、Alice代号「B」，处于同一“椭圆函数”加密算法，G相同，当各自私钥生成公钥，交换公钥，A私\*B公=B公\*A私=S；当其成立，即验证成功可相互传输数据；

最后蒋鑫从加密算法优劣性角度收尾，用RSA与ECC做事例，阐述出椭圆曲线加密性好在于其紧凑性更好，同样长度密钥，破解难度指数级增长。

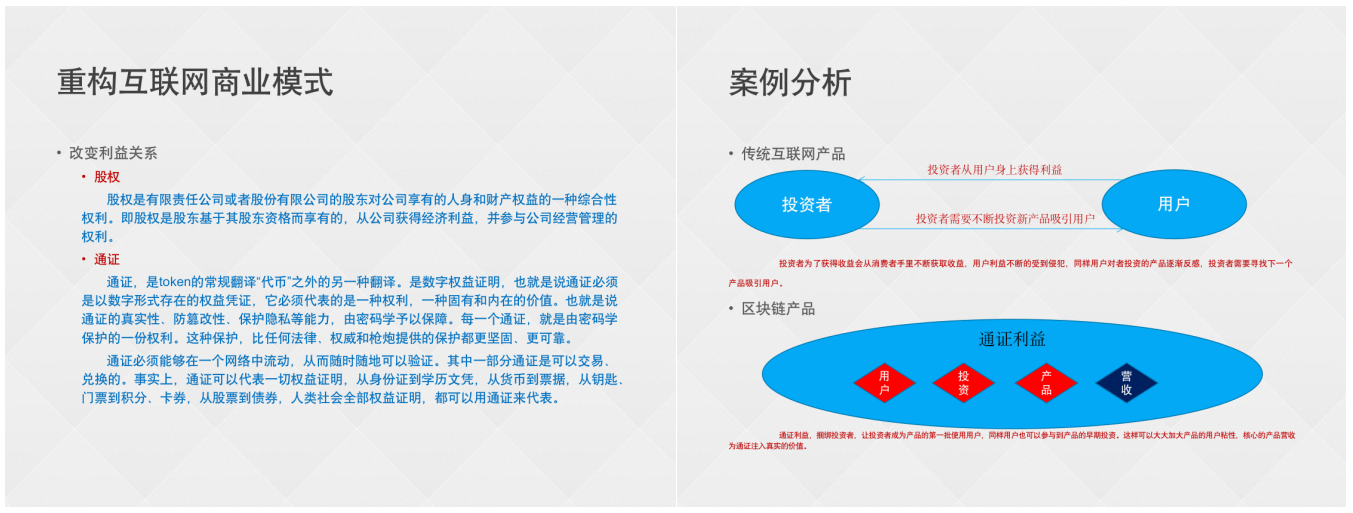
**Part II**

****

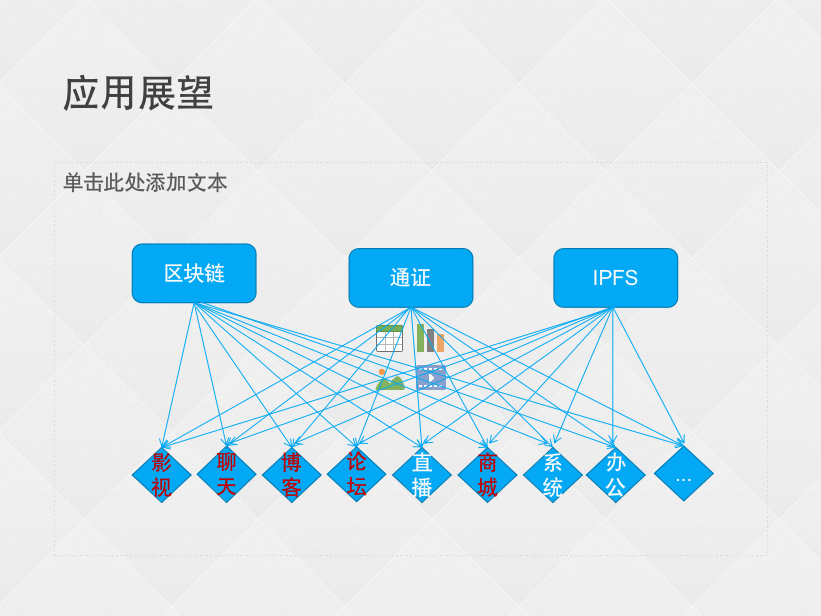
来自元知慕语的骞永军此次带来的是《IPFS的Web开发》，从区块链价值可用性角度，分享区块链发展方向、IPFS项目技术实现，到价值落地。

骞永军提到他转向区块链领域是从比特币得到到启示。通过早期比特币游戏性质到2011年第一次实物消费，到交易所到价值存储，得到区块链价值启示；

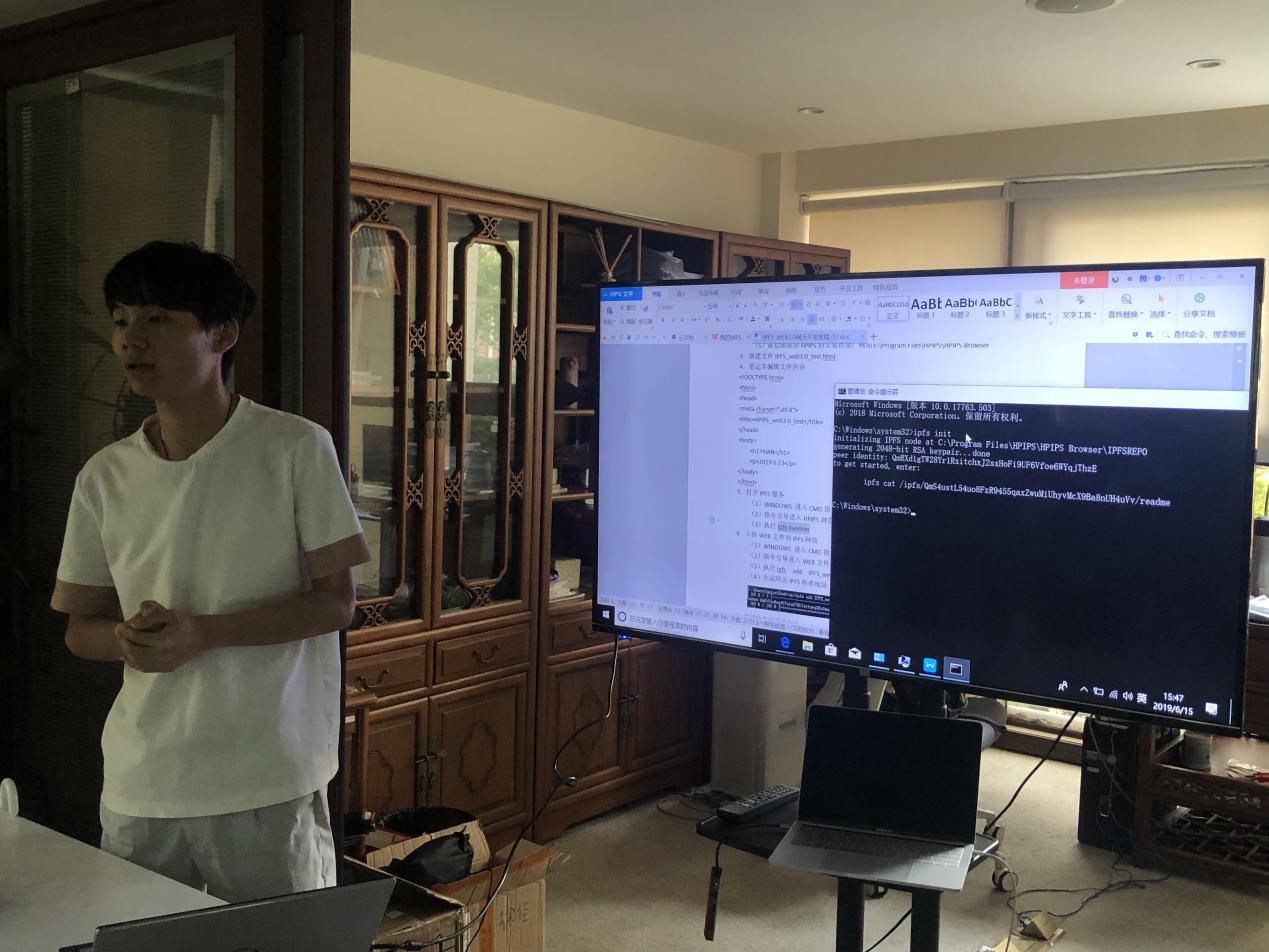
公链的发展，“区块链1.0-区块链2.0、p2p-bt-区块链-ipfs”，这些飞速发展的技术和项目，让骞永军确信提前建立股权模式、通证模式、项目发展规划及成本控制是极其重要的事情。

通证利益是用户动力，有别于传统互联网产品，通证存在的天然优势必然促使区块链产品的市场有更便利的发展，更多赢的局面。

接下来，结合区块链、通证、IPFS，罗列业务可用性及产品落地状况，现场也交流了目前各垂直领域项目技术实现的阻碍。



最后，骞永军做了结合IPFS和视频娱乐分发的Web产品展示，并现场做了开发演示及教学。

****

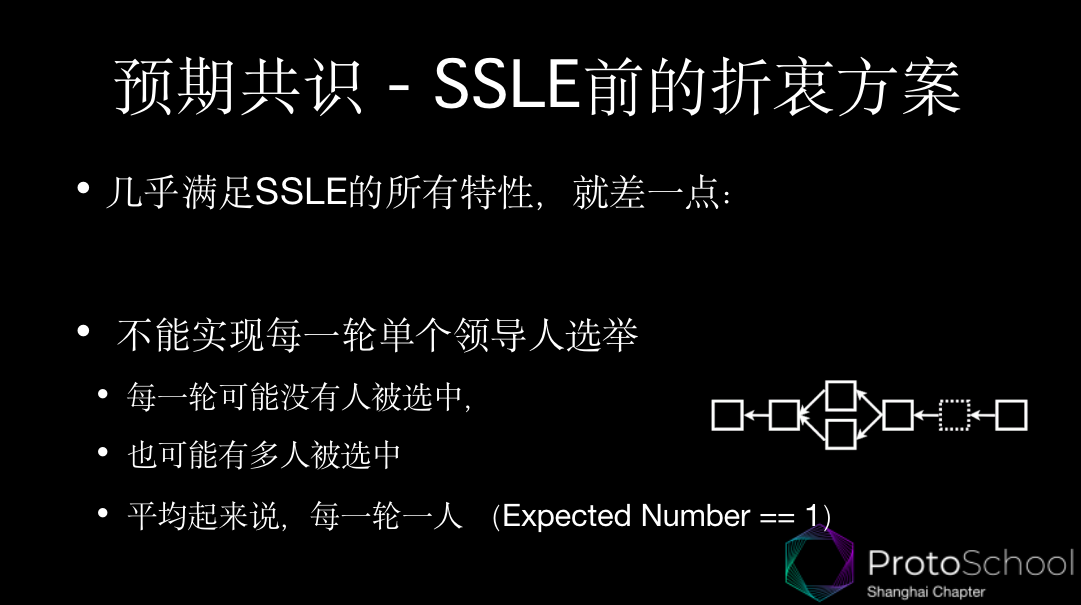
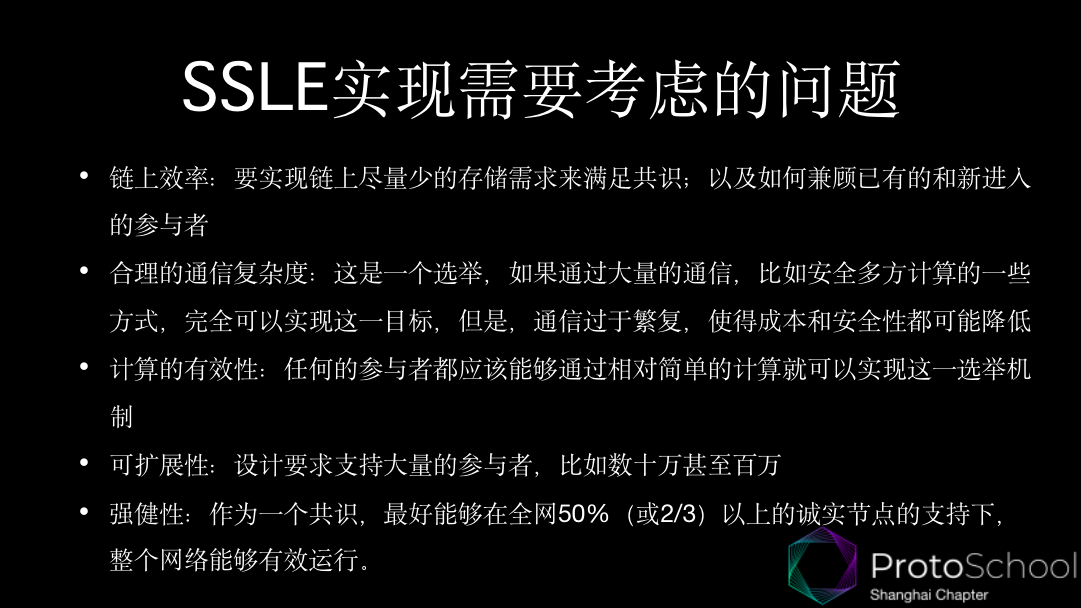
**Part III**

****

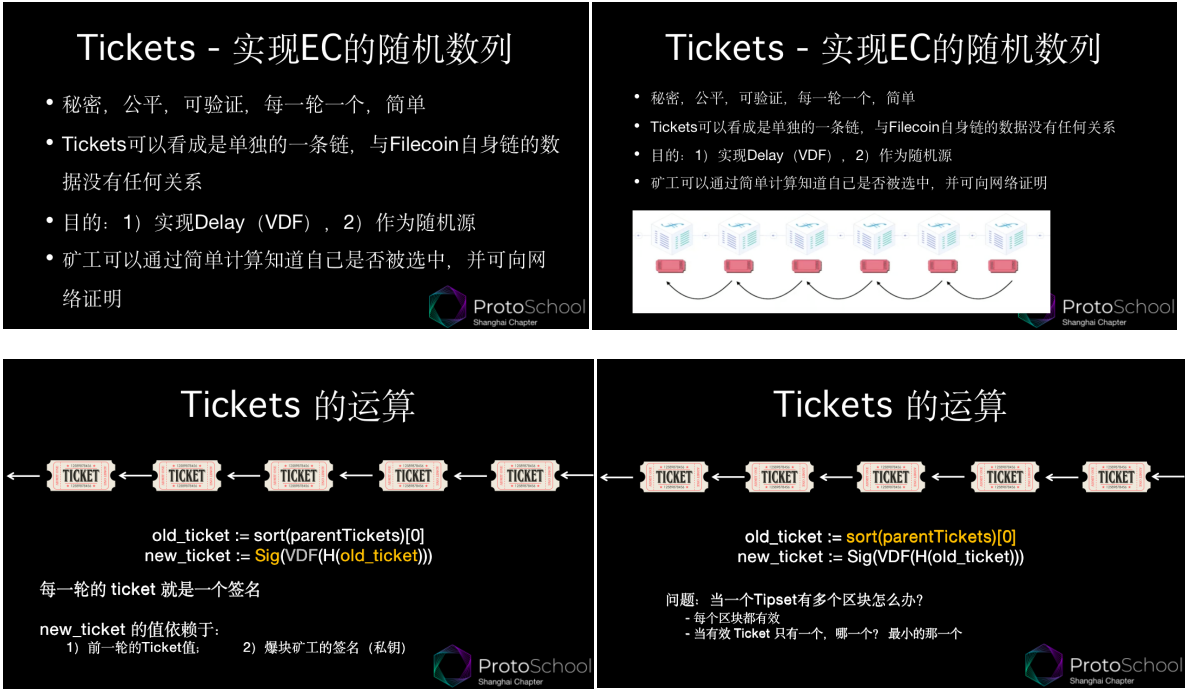
第三位分享的是来自IPFS原力区的技术负责人李昕，他的分享主题是《Filecoin的预期共识》，主要分享共识机制的评判纬度、共识机制现状及存在的问题、解决方案与实现逻辑。

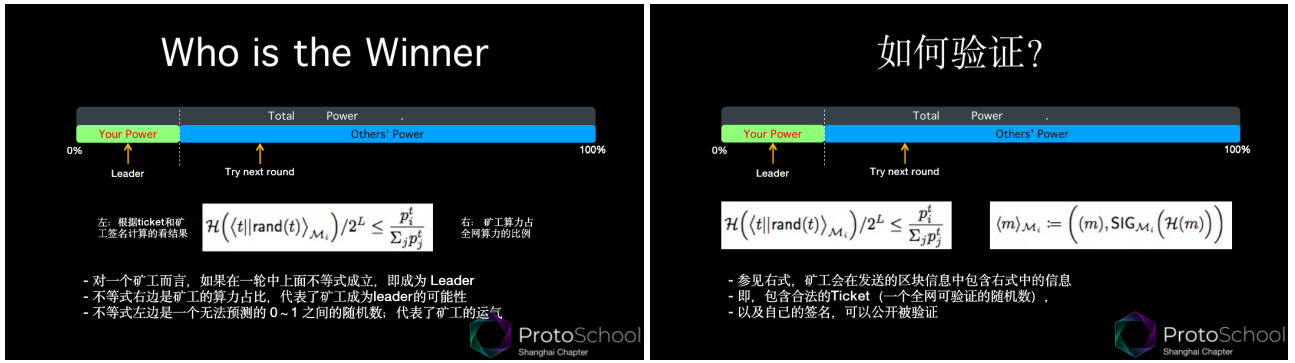


（共识机制评判纬度）



共识机制的完美实现是SSLE，但目前所有纬度问题的解决办法不完全兼容，预期共识（EC）作为目前最优解出现了，应用于Filecoin链。

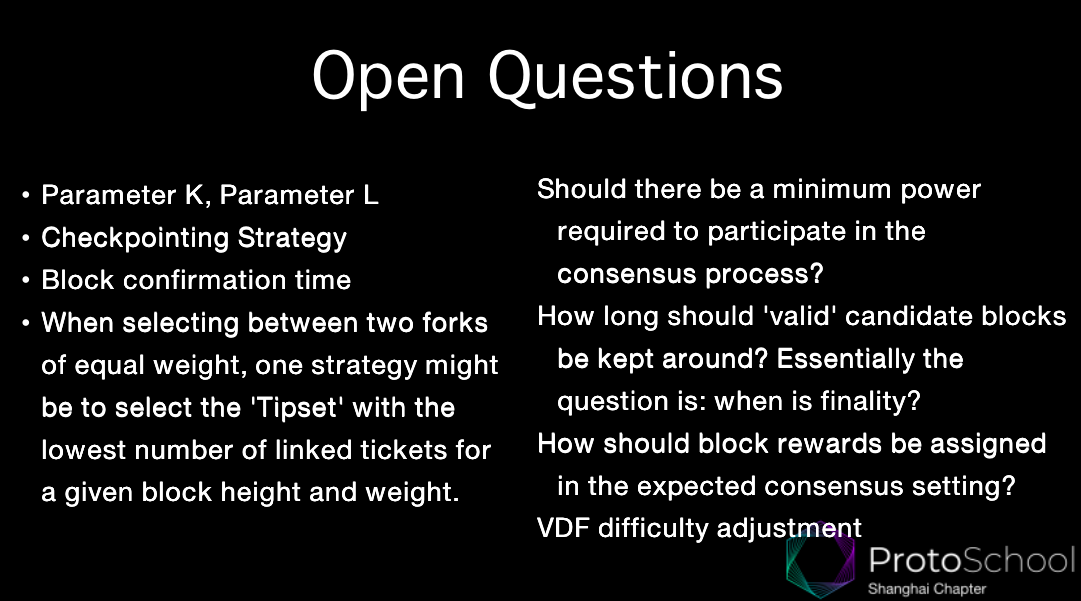
由简入深，李昕首先介绍了EC的基本术语，然后阐述了EC如何打破现实与目标的壁垒，紧接着从技术角度剖析实现贴近SSLE的设计逻辑。

随后李昕带大家营造的区块链预期共识的探索之路碰到了“出块延时机制”、“Leader选举机制”、“分叉”等问题，对应的分享了“sleep”暂行解决办法、“Leader选举公式”、“最重链法则”。

（Leader选举）

（最重链法则）

**最后李昕留下开放性问题，现场进入热烈的探讨及自由交流时间。**



大家带着各自的观点讨论热烈，以下为整理小部分圆桌探讨Q&A记录：

* Q：现在椭圆曲线签名除了比特币里常用的算法，其他的，公认是比较安全的吗？  
  蒋鑫：【https://safecurves.cr.yp.to/】这个网站，将现有椭圆曲线都罗列了出来，并有各个维度安全度评分；
* Q：关于tickets最小签名，多台机器并行，能否影响结果？

李昕：即便多台机器并行，总“算力”与爆块概率是不变的，所以并不影响结果。

以上即为IPFS原力区第三次线下技术沙龙回顾，旨在通过此次会议分享近期各位大咖的观点与见解。IPFS的市场应用前景、Filecoin的共识之路、密码学对区块链安全性的加持，通过同时、同地、同频的共鸣性探讨，抹除IPFS和Filecoin的未来在各自心中不尽相同的主观臆想。

另外

原力区**每周二线下分享活动**已经来到第77期，期待与你相遇。

信息对称 世界对称

**价值** 共建 **荣耀** 共享