北京大学肖臻老师《区块链技术与应用》公开课笔记

> 比特币网络篇，对应肖老师视频：click here 全系列笔记请见：click here **About Me:**点击进入我的Personal Page

比特币系统的工作过程： 用户将交易发布到比特币网络上，节点收到交易后打包到区块中，然后将区块发布到比特币网络上，那么新发布的交易和区块在比特币网络上是如何传播的呢?

比特币网络的工作原理

比特币工作于网络应用层，其底层（网络层）是一个P2P Overlay network（P2P覆盖网络）。比特币系统中所有节点完全平等，不像一些其他网络存在超级节点(super node)。要加入网络，至少需要知道一个种子节点，通过种子节点告知自己它所知道的节点。节点之间的通信采用了TCP协议，便于穿透防火墙。当节点离开时，只需要自行退出即可，其他节点在一定时间后仍然没有收到该节点消息，便会将其删掉。

比特币网络设计原则：**简单、鲁棒（最坏情况下能达到最优状况，即健壮性）而非高效。** 每个节点维护一个邻居节点集合，消息传播在网络中采用洪泛法，某个节点在收到一条消息会将其发送给所有邻居节点并标记，下次再收到便不会再发送该消息。邻居节点选取随机，未考虑网络底层拓扑结构，也与现实世界物理地址无关。该网络具有极强鲁棒性，但牺牲了网络效率。

比特币系统中，每个节点要维护一个等待上链的交易集合。第一次听到交易，若是合法交易，则将其加入该交易集合并转发给邻居节点，以后再收到该交易就不再转发（避免网络上交易无线传输）。假如网络中存在两个冲突交易，如交易1：A->B,交易2：A->C（假设花费的同一笔钱）。具体接收哪个取决于节点先接收到哪个交易，之后收到另一个交易会将其放弃。

> 假如某个节点先听到A->B，但又听到A->C已经上链，则此时A->B为非法交易，所以要在等待上链交易集合中删除A->B

新发布区块在网络中传播方式与新发布交易传播方式类似，每个节点除检查该区块内容是否合法，还要检查是否位于最长合法链上。区块越大，则网络上传输越慢。BTC协议对于区块大小限制为不大于1M大小。

> 区块大小越大，网络上传播时延越长；区块大小越小，则可以包含的交易数目越少。

此外，比特币网络传播属于 **Best effort（尽力而为）** ，不能保证一定传输成功。以一个交易发布到网络上，未必所有节点都能收到，也未必所有节点收到交易顺序都一致。