06比特币网络原理

The BiitCoin Network

application layer: BitCoin Block Chain

Network layer: P2P Overlay Network

比特币的P2P网络是非常简单的，所有的节点都是对等的。不像有的P2P网络中有super node或者master node。

想要加入这个网络的话，至少需要知道一个seed node种子节点，种子节点会告诉你他所知道的所有节点。节点之间通过PCP进行通信，退出的时候不需要任何操作，只需要退出程序就可以，当别的节点没有收到你的消息的时候就会给你删掉。

比特币网络的设计原则是simple and robust but not efficient。每个节点维护一个邻居节点的集合，消息传播在网络中采取叫做flooding的方式。节点第一次听到某个消息的时候，会传播给所有的邻居节点，并且记录这个消息已经传播过了，当再次收到这个消息的时候不会进行二次传播。邻居节点是随机选取的，不会考虑底层的拓扑结构。所以非常的robust但是不efficient。

每个节点需要维护一个等待上链的交易集合。第一次听到某个交易的时候，就会加入到这个集合中，并且转发给邻居节点。再次收到这个交易的时候就不会转发了，但是转发的前提是交易必须是合法的。

但问题是两个冲突的交易可能同时在网络中进行传播，A -> B和A -> C

有的节点会先收到A -> B, 那么就不会再接受A -> C

有的节点先收到 A -> C, 那么就不会再接受 A -> B

当新发布了一个区块之后，每个节点会将新区块中包含的交易，在维护的等待上链的交易集合中删掉，如果新发布的区块中包含等待上链的交易集合中冲突的交易，那么也需要删掉。因为这个冲突的交易已经变成非法的了。

比特币中区块的大小上限是1MB。

比特币的网络是best effort。一个交易发不到比特币网络上，不一定所有的节点都能收得到，而且不一定每个节点收到的顺序都是一样的。不一定所有节点都会按照比特币的协议进行转发，有的节点可能不转发一些合法的交易，有的节点可能故意转发一些非法交易。

当你购买了一个东西，但是对方不给你发货，可以找电商或者平台进行投诉（没有办法找比特币本身，因为是去中心化的），如果电商没有信誉那就白给了。然后退款的时候并不需要回滚交易记录，而是发起一个新的交易，将同等的金额转回给支付方。