1. 网络模型

比特币以P2P网络进行构建，采用的是P2P网络中的纯P2P非结构化网络，所有结点之间都是对等的，没有超级结点。要加入这个网络，至少要有一个种子结点（seed node），和种子结点联系，它会告知它所知道的网络中的其它结点（有点像构造路由表的过程）。结点之间通过TCP来通信。要离开网络也不必通知其它结点，只需要直接退出应用程序，其它结点一直没有听到你的消息，过一段时间就会将你删除掉。

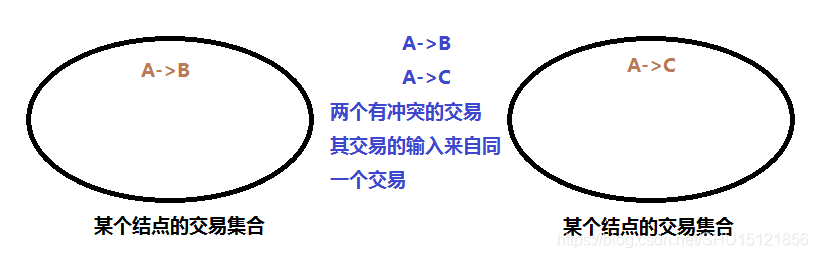
比特币网络的设计原则是简单、鲁棒，而不是高效。每个结点维护一个邻居结点的集合，消息在网络中采用flooding(泛洪)方式传播，结点第一次听到某个消息，会将它传播给所有邻居结点，同时记录一下自己已经收到过这个消息了。

|  |
| --- |
| 邻居结点的选取是随机的，没有考虑底层的拓扑结构。比如美国的一个结点可能和中国的一个结点是邻居结点。这样设计的好处是增强鲁棒性，牺牲了效率。 |

1. 新发布的交易的传播

比特币网络中，每个结点要维护一个等待上链的交易的集合，这个集合中的交易都是要写入区块链的合法的交易，结点第一次收到这个交易的时候就会把它写入这个集合，并转发给所有邻居。

如果有两个有冲突的交易，几乎同时发布到网络上，每个结点根据其位置的不同，可能先收到的交易是不同的，那么另一个交易对于这个结点而言就是非法的了，不会被收纳到集合中。



以左边的集合为例，它先听到A->B的交易，将其写入到了自己的交易集合中。接下来它收到了一个新发布的区块，其中包含A->B这个交易，说明这个交易已经被写入区块链了，所以就要在自己的交易集合中将其删除掉。

* Risk condition

如果这个结点收到的新发布的区块中的交易是被自己丢弃掉的A->C的这个交易呢？这时也要将集合中的A->B删除掉，因为检查可以发现此时集合中的A->B这个交易是非法交易，因为它和新发布的区块中的A->C这个交易冲突了。

也就是说要看接收A->B交易的结点先获得记账权，还是接收A->C交易的结点先获得记账权。

* Best effort

一个交易发布到比特币网络上，未必所有结点都能收到（有的结点不一定按照比特币协议的要求来转发，可能合法的不转发，不合法的又转发了），而且不同结点收到交易的顺序也很可能是不一样的（网络传输中的延迟可能很大）。这是一个去中心化的系统中要面临的实际问题，只能尽力而为。

1. 新发布的区块的传播

和新发布的交易的传播方式是类似的，不过每个结点除了要检查区块的内容是不是合法的，还要检查区块是不是在最长合法链上。

越大的区块在网络上传播越慢，比特币协议要求区块大小不能超过1M，因为比特币网络的效率比较低，一个1M大小的区块可能要几十秒才能传播给比特币网络上的大多数结点。