比特币网络

比特币工作在应用层(application layer:Bitcoin block chain)，它的底层是一个网络层(network layer:P2P overlay network)。

比特币的P2P网络是非常简单的，所有节点都是对等的。不像有的P2P网络有所谓的超级节点、纸节点。

要加入P2P网络首先得知道至少有一个种子节点，然后你要跟种子节点联系，它会告诉你它所知道的网络中的其他节点，节点之间是通过TCP通信的，这样有利于穿透防火墙。当你要离开时不需要做任何操作，不用通知其他节点，退出应用程序就行了。别的节点没有听到你的信息，过一段时间之后就会把你删掉。

比特币网络的设计原则是:简单、鲁棒，而不是高效。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flooding的方式。节点第一次听到某个消息的时候，把它传播给去他所有的邻居节点，同时记录一下这个消息我已经收到过了。下次再收到这个消息的时候，就不用转发给邻居节点了。

邻居节点的选取是随机的，没有考虑底层的拓扑结构。比如一个在加利福尼亚的节点，它选的邻居节点可能是在阿根廷的。这样设计的好处是增强鲁棒性，它没有考虑底层的拓扑结构，但是牺牲的是效率，你向身边的人转账和向美国的人转账速度是差不多的。

比特币系统中，每个节点要维护一个等待上链的交易的集合。假如一个集合的交易都是等待写入区块链里的，那么第一次听到某个交易的时候，把这个交易加入这个集合，并且转发这个交易给节点，以后再收到这个交易就不用转发了，这样避免交易会在网络上无线的传播下去。转发的前提是该交易是合法的。

这里有冲突的情况，有可能你会有两个有冲突的交易，差不多同时被广播到网络上。比如说A→B和A→C，这两个如果同时广播在网络上，那么每个节点根据在网络中的位置的不同，收到两个交易的先后顺序不同。

比如一个人先收到第一个交易，就写入到集合里，再收到第二个交易的时候就不会写入集合，因为跟上一个交易有冲突，就认定是非法的。假设这两个交易花的是同一个币，那么写入集合的交易就会被删掉。

比如说节点听到一个新发布的区块，里面包含了A→B的交易，那么这个交易就可以删掉了，因为已经写入到了区块链里。如果节点又听到了A→C的交易，该怎么办?这时候也要把A→B删掉。因为A→C如果已经被写入到了区块里，那么A→B就变成了非法交易，就变成了double spending，这就是冲突的情况。可能某个先收到A→C的节点，抢先挖到了矿，发布了区块。

新发布的区块在网络上的传播有很多方式，跟新发布的交易是类似的。每个节点除了要检查区块的内容合法性之外，还要查它是不是在最长合法链里。越是大的区块，在网络上传播速度越慢。

比特币协议对区块的大小有1M字节的限制。比特币系统采用的传播方式是非常耗费带宽的，带宽是瓶颈。按1M的区块大小限制来算的话，一个新发布的区块有可能需要几十秒，才能传输到网络大部分境地，这已经是挺长时间了，所以这个限制值不算小。

还需要注意的一点:我们讲的比特币网络的传播属于best effort 。一个交易发布到比特币网络上，不一定所以的节点都能收到，而且不同的节点收到这个交易的顺序也不一定是一样的。网络传播存在延迟，而且这个延迟有的时候可能会很长，有的节点也不一定按照比特币协议的要求进行转发。

可能有的该转发的不转发，导致某些合法的交易收不到，也有的节点可能转发一些不该转发发的消息，比如说有些不合法的交易也被转发了。这就是我们面临的一个实际问题。

比特币的挖矿难度调整

目标预值越小，挖矿的难度越大。调整挖矿的难度就是调整目标空间在整个输出空间中所占的比例。

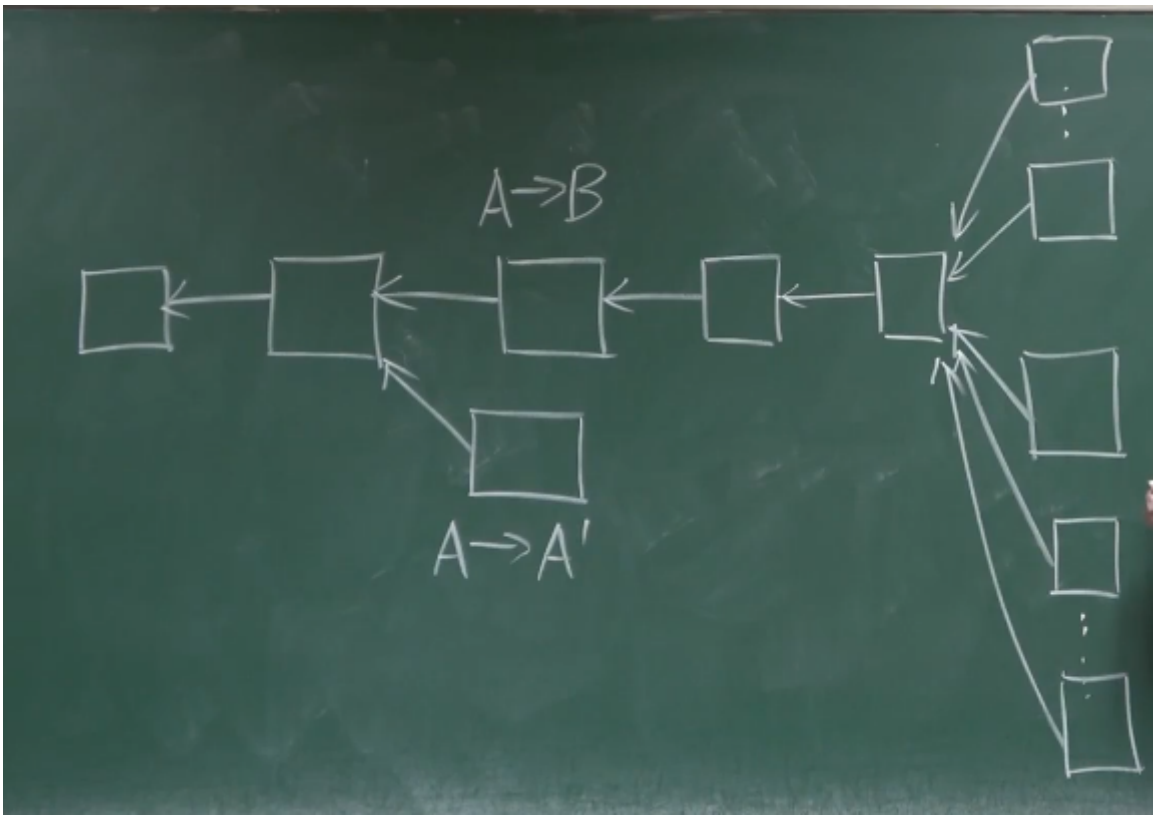
比特币用的哈希算法是SHA-256，这个产生的哈希值是256位。所以整个输出空间是2的256次方。调整这个比例，即目标空间占输出空间的比例，通俗的说，就是哈希值前面要有多少个0。比如说256位的哈希值，要是合法的区块，要求算出来的哈希，前面至少有70个0。当然这只是通俗的说法，因为这个目标预值，并不是说前面都是0，从某一个位置开始，后面都变成了1。

挖矿的难度跟目标预值是成反比的，公式是:difficulty=difficulty_1_target / target。上面是指挖矿难度等于1的时候所对应的目标预值，挖矿难度最小就是1，这个时候对应的目标预值是个非常大的数。

即target越大，挖矿是越容易的。所以公式里很大的一个数，除以当前的目标预值，得到的就是当前的挖矿难度。所以difficulty和target大小是成反比的。

为什么要调整挖矿难度呢?如果不调会有什么问题呢?系统里的总算力越来越强，挖矿难度保持不变的话，出块时间是越来越短的。

出块时间越来越短，会有什么问题吗?



比如说不到一秒就出一个区块，区块在网络上传播的时间可能需要几十秒，底层的比特币网络可能需要几十秒才能让其他节点都收到。别的节点没有收到这个区块之前还是继续沿着已有的区块链往下扩展。如果有两个节点同时都发布一个区块，这个时候就会出现分岔。

出块时间如果越来越短的话，这种分岔会成为常态，而且不仅会出现二分岔，可能会出现很多的分岔。比如10个区块同时被挖出来，系统可能会出现10分岔。

分岔如果过多，对于系统达成共识是没有好处的，而且危害了系统的安全性。比特币协议是假设大部分算力掌握在诚实的矿工手里。系统当中的总算力越强，安全性就越好，因为有恶意的节点想掌控51%的算力就越难。如果掌握了51%的算力，它就可以干很多坏事，比如分岔攻击。

如果后面分岔多的话，前面某个区块里的某个交易，很可能就遭受分岔攻击，恶意节点会试图回滚。因为后面分岔多，**算力就会分散**，恶意节点得逞的概率更大。这个时候恶意节点就不需要51%的算力了，可能10%的算

力就够了，因此出块时间不是越短越好。

那10分钟的出块时间是不是最优的呢?不一定。改成其他值也可以，有间隔只是说应该有个常数范围。以太坊系统出块时间就降低到了15s，所以以太坊的出块速度是比特币的40倍。

出块时间大幅度下降之后，以太坊就要设计新的协议，叫ghost。在该协议中，这些分叉，产生的orphan block(即产生最长合法链后另一个要被丢弃的区块)就不能丢弃掉了，而是也要给它们一些奖励，这叫uncle reward。以太坊也要调整挖矿难度，使出块时间保持在15s。

讲完了为什么要调整挖矿难度，现在讲一下怎么调整挖矿难度。比特币协议中规定，每2016个区块后就要调整目标预值，这大概是每两个星期调整一次。

具体的调整公式:target =target×(actual time/expected time)。actual time指产生2016个区块实际花费的时间，expected time指产生2016个区块应用的时间，即2016×10min。

如果实际花费时间超过了两周，即平均出块时间超过了10min。那么这时候挖矿难度要调的低一点，应该让出块更容易。因此该公式算出来的target会变大，则难度会下降。

实际上，上调和下调都有四倍的限制。假如实际时间超过了8个星期，那么我们计算公式时也只能按4倍算，目标预值增大最多只能增大4倍。

那怎么才能让所有的矿工同时调整目标预值呢?计算target的方法写在比特币系统的代码里，每挖到2016个区块会自动进行调整。如果有有恶意的节点故意不调，会怎么样?

如果一个节点不调，将区块发布出去，诚实的节点是不会认的。nBits是target一个编码的版本，在block header里没有直接存储target的域，因为target的域是256位，直接存target的话要32个字节。nBits在header里只有四个字节，所以可以认为是它的一个压缩编码。

如果遇到有恶意的矿工，该调的时候不调，这时检查区块的合法性就通不过。因为每个节点要独立的验证发布的区块的合法性。检查的内容就包括:nBits，目标预值设的对不对。如果投机取巧设计一个过大的目标预值，使得你自己挖矿容易了，但这个区块是不会被接受的。

如图(第七节视频 第26分钟)显示的是比特币系统中总算力的变化情况。在比特币没有流行前，有很长一段时间，算力没有太明显的增长，前面这些年的hash rate几乎是0。其实这些年算力也是增长的，只是后面这些年算力增长的太快了，所以前面部分看上去像是一条直线。去年是涨得非常猛的一年，这也体现在了hash rate的增长上，算力呈现出指数级的增长。即使在这段黄金时期，算力也不是单调递增的，中间也是有很多波动。

如图(第七节视频 第27分钟)是挖矿难度的变化情况，跟算力的增长基本上是同步的，这也符合难度调整的设计目标。通过调整挖矿难度，使得出块时间保持稳定。注意这个图显示的是挖矿难度，不是目标预值。

如图(第七节视频 第27分第27秒)是最近半年的难度调整曲线，可以看出很明显是一段一段的。每隔两个星期，难度上一个台阶，说明挖矿的人越来越多，用的设备越来越先进，反应出大家对比特币的热情越来越高。如果出现相反的情况，比如某个加密货币的挖矿难度越调越小，说明挖矿变得越来越容易了。但这不是好事，说明大家对币的热情是逐渐减小的。持续出现这种情况说明这个币将被淘汰。

如图(第七节视频 第28分第13秒)显示的是每天的出块时间。可以看出，总的来说出块时间稳定在10分钟上下振动。

如图(第七节视频 第28分第36秒)显示最近半年的出块时间，也是维持在10分钟左右。

挖矿难度的公式:下一个难度=前一个难度 * 两周/挖前2016个区块用的时间(注意:前面的公式是目标预值的公式，不要混淆了)