1. **挖矿难度**

挖矿就是不断尝试区块块头中的nonce和extra nonce的值，使得：



显然目标阈值target越小，则挖矿的难度就越大。所以调整挖矿难度就是在调整target，**以调整目标空间在整个输出空间中所占的比例**。

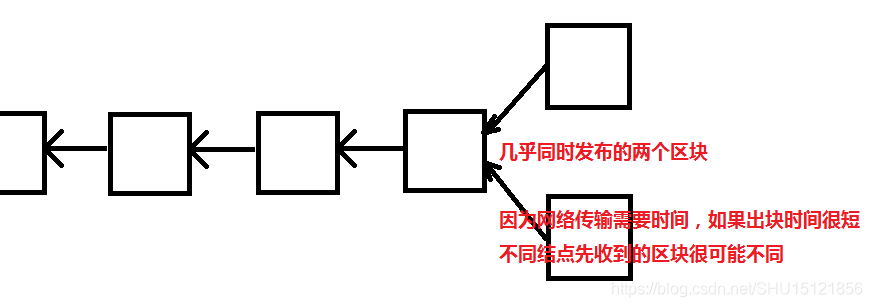
比特币中使用的哈希函数是SHA-256，产生的哈希值是256位的，所以整个输出空间是 ，调整目标空间所占的比例，在这个问题里直观的来看就是最后得到的哈希值前面有多少位0（这只是通俗直观来看的），这个0越多显然值就越小，也就是挖矿难度越大了。挖矿难度和目标阈值的大小成反比，具体可见以下公式：



上式中常量difficulty\_1\_target是指挖矿难度difficulty=1时所对应的目标阈值target的值。挖矿难度最小就是1，所以这个常量也就是target允许的最大值。

1. **为什么要调整挖矿难度**

系统中的总算力越来越强，如果挖矿难度保持不变，那么平均出块时间会越来越短，这会造成一些问题。假设平均出块时间减小到了1秒钟，也就是每隔1秒左右就有一个新的区块携带一些列交易被发布到比特币网络上，而在比特币网络上这个区块传播给大多数结点可能就要几十秒。如果有两个结点几乎同时发布了区块，那么就会出现分叉：



这是一个二分叉的情况，如果出块时间很短，就会导致这种分叉成为常态。而且不仅仅是二分叉，可能会出现很多分叉。

分叉过多对比特币系统达成共识没有好处，并且会危害比特币系统的安全性。例如前面说的分叉攻击，正常情况下，因为大部分结点是诚实的，有恶意的结点想要在6个确认后拿这段时间集中算力算出的新链去覆盖掉最长合法链是很难的，因为诚实结点也都在集中算力扩展最长合法链。如果出块时间很短，就会导致分叉过多（因为相比于出块时间，可以认为网络上传输的时间变长了），这样**诚实结点的算力就被分散了**，这时恶意结点要进行51% attack很可能就不需要50%以上的算力了，可能百分之十几就足够了，这样**大大降低了比特币系统的安全性**。

|  |
| --- |
| 比特币10分钟的平均出块时间也未必是最优的，后面要学的以太坊的出块时间就降低到了15秒。大幅降低了出块时间，所以以太坊就要设计一个新的共识协议——GHOST。在这个协议中，分叉产生的orphan block不能简单丢弃掉，而是也要给予一些奖励——uncle reward。 |

总之，在不同的区块链账本系统中，**不论出块时间设计成多长，都要设法让其保持稳定**，而不能允许它随着系统中总算力的提高而无限减小下去。

1. **怎么调整挖矿难度**

比特币协议中规定，每隔2016个区块（大约每2个星期）要重新调整一下目标阈值target，具体的迭代更新公式是：



这里expected time就是**预期的**两次调整的间隔时间，即2016乘以10分钟(大约两周)；而actual time是系统中产生最近的2016个区块**实际的**花费时间。为了避免系统中出现某些意外情况，导致系统出现非常大的波动，每次对目标阈值target的调整最大不能超过4倍，最小不能小于1/4​。也即上式中的actual time / expected time即便超过4了也按4使用，即便小于 1/4​也只按1/4​使用。

1. **如果恶意的结点不调整target怎么办**

target是写在比特币系统的代码里的，代码也都是开源的，如果有结点到了该调整的时候不调整target怎么办。这也是一个大部分结点诚实的问题，如果不调整target，那么发布的区块块头里的4字节nBits域（32字节的target压缩编码后的版本）就不是正确的，诚实的结点不会接收这样的区块。