07 比特币挖矿难度

H(block header) <= target

SHA - 256

Difficulty = (difficulty_1_target) / target　　其中difficulty为1的时候，target是最容易实现的。所以difficulty就是最容易的target除以当前的target算出来的。

target越大的时候，越容易。difficulty越大说明越难。

如果挖矿的难度一直不变，那么平均的出块时间就会越来越短。直觉上来说出块时间变短应该是好事儿，因为交易被写入到区块链中的等待时间就会变短。

如果不到一秒钟就出一个区块，会有什么问题?

区块的网上传播的速度可能需要几十秒进行广播。如果两个节点同时发布一个节点，那么这个时候就会出现分叉。如果出块的时间越来越短，那么 出现的分叉的情况就会变得越来越多。分叉如果过多，对于维护系统的一致性就越难，对系统的安全性是没有好处的。但是坏的矿工如果掌握了51%以上的算力，就是51%attack，那么就可以回滚交易。

如果分叉过多的话，出现的分叉就很多，就不一定需要51%的算力就可以发动攻击，可能需要的算力就会更少。

以太坊的平均出块时间只有15s，所以需要新的共识协议就是ghost，所以分叉的orphan block，就不能简单的进行丢弃，而是需要进行一定奖励，称之为uncle reward。以太坊中同样需要调整挖矿难度，让平均出块时间保持稳定，不能无限的减少下去。

每隔2016个区块调整一次难度，(2016 * 10) / (60 * 24) 大概是十四天。

target = target * (actual time / expected time) 这其中的expected time 就是2016 * 10，actual time是系统中产生最近的2016个区块实际上花费的时间。当actual time > expected time，那么后面的分数就是大于1的，所以target会变大，相当于挖矿难度变低。反之就是挖矿难度变高。实际的代码当中，有四倍的限制，如果实际的2016个区块花费的时间超过8个星期，那么也按照8个星期来算。如果比半个星期还短，也按照半个星期来算。

那么怎么能让所有的矿工都那么听话，同时调整挖矿的难度？因为比特币的系统里就是这么写的。但是这个代码是开源的，如果有恶意的节点就是不调整难度怎么办？如果不调的话，你发布的区块诚实的矿工是不会认的。区块的header里有一个nBits域，是target的压缩编码，如果有恶意的矿工发布新的区块（没有调整难度），那么诚实的矿工就不会接受这个区块。