比特币的挖矿计算其实就是大家一起做数学题，题干是需要被记录的交易，大家通过做题抢夺记账权，抢到的矿工就能获得系统奖励和交易手续费。

比特币用的SHA256算法的特点是已知答案验证正确很容易，但是要得到答案非常麻烦，需要一个一个数字去试。最先得到答案的矿工大家就都认可他是抢到了记账权，奖励就归他了。大家继续抢下一题的记账权。简单来说这些计算的意义只在于保证整个系统的稳定安全，并没有更多的意义。把比特币看作是计算的副产品是不全面的，比特币的产生发行、比特币链上所有的交易流通、比特币系统的稳定性，都是计算的目的，是一体的。当然除了维护这个系统之外，的确并没有产生其他的价值和产物。这也是比特币被指责不环保浪费资源的一个黑点。总的来说，比特币作为一个里程碑式的区块链数字货币，其源于大量的算力投入和用户信任的巨大价值。这一点还是毋庸置疑的。区块链实质上是由一个个记录着交易信息的数据块链接而成的，生成一个新区块所需要完成的工作量证明，就是找到一个随机数，使得将这个随机数、上一个区块的哈希值、这个新区块的交易数据组成的字符串代入做哈希运算，所得到的哈希值符合目标难度要求。哈希运算，简单来说，就是输入任意长度的字符串作哈希运算会得到一个较短的固定位数的字符串，称为这些输入信息的哈希值，并且不同的输入信息，哪怕是一个标点的不同，都会生成截然不同的哈希值。上一个区块的哈希值即是把上一个区块信息代入做哈希运算得到的唯一一个哈希值。哈希值的表达是由0至9这10个数字以及abcdef这6个数字构成的，也就是说每一位有16种可能。而任何输入所生成的哈希值的表达是非常随机不可控的。具体的难度要求则是指限定一个哈希值表达的目标范围——哈希值开头连续多位数字是0。我们知道，随机代入数值，要实现开头1个字位是0的概率是1/16，而要实现开头8位都是0的概率则是1/2^

32，也就是大约需要代入2^

32个随机数才能够得到一个开头8位都是0的哈希值。所以记账节点们在耗费大量算力计算的过程，就是代入大量随机数进行哈希运算直到找到一个能够让其参与生成的哈希值实现要求数量的0作为开头。而这个难度要求是根据全网算力的变化进行调整的，比特币网络共识每生成2016个区块后，全网节点重新评估算力水平确定新的难度要求，以保证找到一个目标随机数的时间大约是10分钟。简单的说就是不停地拼凑字符串，计算的SHA256哈希值，直到找到产生合适的哈希的字符串，这个字符串就是解。为什么要做这些计算?本质上这个计算是为了解决分布式网络的同步问题，也常被称为”拜占庭将军问题 “。中本聪曾经回复过这个问题

比特币采用了工作证明来解决拜占庭问题，而且中本聪选择了计算哈希来作为过程中计算的问题。比特币网络的区块链实际上就是一个大账本，在分布式的网络中会存在多个版本的账本，怎么找最新的账本呢?你只需要找计算难度最大而且长度最长的账本，这样每个人都能安全地同步到同一个账本上来。