首先，记账是有奖励的
。一部分奖励是被打包区块里用户自己出的手续费，手续费用比特币支付，这个手续费可高可低，给得高，记账者就倾向于先记这笔手续费高的账。另一部分奖励则是区块奖励，打包一个区块，就获得一定的区块奖励。比特币诞生之初，区块奖励为 50个比特币，按比特币程序设定，每出
210000个区块后，奖励减半，现在已经经历了两次减半，预计 2020年5月时会发生第三次减半。区块奖励一方面调动了大家去记账，另一方面也解决了比特币的发行问题。按照上述规则，我们可以按这个公式计算比特币的总量，就是
210000×50×（1+1/2+1/4+……），总共 2100万个。

有了奖励，而且奖励颇丰，大家当
然抢着去记账
。为了确定以谁的账本为准，比特币
又设定：
记账者要先把收集到的账单打包成一个
区块
，区块由区块头和区块体组成，区块头里有个记账者自定的随机数，记账者换上不同的随机数，对区块头进行哈希运算，谁先试出符合要求的哈希值，他就将这个区块广播全网，大家都以他的账本为准。

区块头和区块体是什么关系呢？
区块体里
记录了具体的账单

，包括记账者自己所得奖励和手续费
的账单。
区块头则相当于该区块的身份信息，里面有上一个区块头的哈希值、时间戳、哈希运算的难度目标、随机数等信息，还有一个 Merkle树哈希值，Merkle树哈希值由区块体里的账单经过一系列哈希运算得到，相当于区块体里那些账单的摘要信息，只要账单稍有变化，Merkle树哈希值就会大不相同。

哈希算法又被称为摘要算法，输入任何数据，经过哈希运算后，都会得到一个固定长度的输出值，称为该输入数据的哈希值
。哈希运算有两大特点。
第一，只要输入数据稍有变动，哈希值就会大不相同，比如输入一本书的内容，只要多加一个字，哈希值都会面目全非。第二，哈希运算只能正向算，不能反向算，输入数据后可以很快算出哈希值，但给出哈希值，就没法反推它的输入数据，要想知道输入数据就只能一次次输入不同数据去尝试，直到试出为止。这可能比较难理解，这就好比可以轻易地算出29179×87013=2538952327，但要是问你2538952327是哪两个数的乘积，你就只能一个数一个数地试。

争夺比特币记账权时算的哈希值是个 256位的二进制数，符合要求的哈希值，就是小于某个特定数值的哈希值，这个特定数值也就是区块头里的难度目标，可以简单地将其视作前面数位都是
0的哈希值（当然后面数位的大小也有要求，这里为简便起见只谈论前面数位为0的情况）。例如，难度目标要求哈希值前面 70位都是 0，在计算过程中，记账者手头的账单、时间戳等信息都是固定的，记账者能改变的只有随机数，他就加上不同的随机数去试。算出的哈希值是毫无规律的，哈希值每个数位上出现 1和
0的概率各是 1/2，一次就试出前面 70位都是 0的哈希值，概率是 1/2^70，想增大试出的概率只能做更多哈希运算。全世界想获得比特币奖励的人都会收集网络上的比特币账单，打包成区块，进行哈希运算。谁先试出了前面 70位都是 0的哈希值，他就立马将自己的区块广播全网。大家一接收到该区块，验证无误后，就以该区

种试出符合要求的哈希值并获得比特币奖励的行为，也被称为挖矿，专门进行这种计算的机器，就被称为矿机，参与挖矿活动的人，称作矿工，记账的手续费，就叫矿工费。