雷锋网AI金融评论按：本文作者为中国信息通信研究院（工信部电信研究院）专家敖萌博士，雷锋网（公众号：雷锋网）独家特约文章，雷锋网与信通院联合首发。未来，敖萌博士原创的区块链系列文章还将继续刊出，雷锋网与信通院相关平台同步更新，敬请关注！

比特币最迷人的地方就是挖矿了。为什么挖矿这么迷人？因为挖矿能获得比特币呗。我写这篇文章的时候比特币的价格是3900美元，如果能挖到一个区块，就能获得48750美元的挖矿收入和约6000美元的交易手续费收入，这不是非常迷人吗？

那么到底什么是挖矿呢？矿工又如何通过挖矿获得比特币的呢？这就需要从比特币区块链系统采用的PoW（工作量证明）共识机制说起了。

PoW（工作量证明）共识机制

先讲一个故事：

有一个村子，这个村子里很多事情都需要大家一起决策。比如某天，村长需要全体村民一起决策今天中午村里的大食堂是包饺子还是擀面条。通常，我们能想到的方法就是投票----每个村民一票，少数服从多数。但是有些村民并不想在食堂吃饭，所以他可能就会把票送给别人，这样就有可能会导致不公平，在食堂吃饭的大多数人可能没有实现他们的愿望。

于是村长换了一种办法，他在10点50的时候，用大喇叭给全体村民广播：“大家来选择食堂中午是做饺子还是做面条，想来食堂吃饭的人，就去食堂门口推那个巨大的石头，到了11点整，石头被推到了大门东边，中午就吃饺子；推到了大门西边，中午就吃面条。”

于是想去食堂吃饭的人，就跑去推石头了。出力多的人群最终实现了自己的愿望，出力少的人群也心甘情愿，因为村里一直都是这样的规矩。

这个故事讲了一种实现人群共识的方式，我们可以叫它“工作量证明机制”。利用出力的多少，来证明自己的选择意愿。

在这个系列的第一篇文章里，我们讲到了区块链系统能够让所有人的账本保持一致。这种让所有节点数据保持一致的机制，我们称之为共识机制。采用不同的共识算法，能够实现不同性能的共识效果，其最终目的都是保持数据的一致性。

记录工作量证明，不可篡改

我们已经知道，在比特币系统中，记录交易是系统工作的基础方式。在比特币区块链系统中，区块是记录交易的最基本容器。在比特币（BTC）中目前区块大小限制为1MB，（前几天刚刚诞生了一种新的虚拟货币，叫做比特币现金——BCC，这个区块大小限制目前是8MB）。由于区块的大小有限制，因此每个区块所能容纳的交易数量也是有一定限制的。目前比特币系统规定平均每10分钟产生一个区块，因此，矿工工作的方式实质上就是在10分钟内收集网上产生的所有交易，然后将交易填到一个区块里。这个区块大约如下表所示：

注意第一条，在任何区块里，第一条都是没有转出地址的，就是所谓的CoinBase（挖矿交易）。没有任何人付给矿工这笔钱，矿工只是理所应当的写上自己获得了12.5比特币。所有节点都认可矿工这样写，因此矿工就得到了挖矿收入。

不同的矿工在填写区块的时候，数据一定是不一样的，因为每个矿工的第一条肯定不一样，矿工只会把挖矿收入转入自己的地址。所以矿工Michael的CoinBase是“Michael获得了12.5比特币”，矿工Nancy的CoinBase是“Nancy获得了12.5比特币”。

每一个矿工都把自己收集到的交易和自己该获得的收入填好了，那么，到底谁的记录才会被大家认可呢？比特币就采用工作量证明机制，让矿工互相间竞争求解一个数学题，谁先解出来了，谁的区块就会被所有人认可。就好像开篇的故事讲的那个村子一样，每个矿工都在努力地推那个巨石，一旦石头把自己记录的那一页账目压住了，他就大喊一声，“我的工作量证明成功了，你们快来看！”全体矿工就都过来把那一页账目抄写一份，贴在自己账本的最后面，然后又开始新的记账过程。周而复始，生生不息，账本一页一页的增加，账本越来越厚。

“中本聪”决定采用工作量证明机制的时候，出发点是避免系统受到攻击。“中本聪”认为，如果一个攻击者想用搞乱账本的方式来进行攻击，那么他就需要足够的计算能力。也就是说，他要比大多数推石头的人的力量更大。这样，他就需要付出巨大的成本，但是换回的收益并不足以抵消成本，因此攻击者是没有攻击比特币系统的经济学动力的。

与推石头的方式不同的地方在于，比特币中是大家一起通过穷举结果的方式，来求解一个数学题，并不是算力强的人每次都会赢，因为有人可能很幸运，一下子就搜索到了那个答案。而算力强的人，可能这次没那么幸运，穷举了很多次也没有碰到解。但是从概率上看，求出答案的次数和自己在整个比特币网络中算力的比例是一致的，也就是说，如果一个矿工拥有了全网30%的算力，那么基本上在1000分钟（产生了100个区块）里，有30个区块都是他找到的答案，他获得了30%的挖矿收益

。

但是，现在由于比特币的价格越来越高，推石头的人已经不满足于自己去推了，而是把家里的大骡子大马都派上去干活了。在“中本聪”最初的设计里，一个CPU一票，用算力来决定哪个矿工记的账成为最终的账目。随着比特币价格的增高，开始出现了GPU挖矿，后来人们又不满足于GPU的速度，开始制造专用芯片挖矿。专用芯片在计算比特币问题的能力上是普通CPU的数万倍，因此现在比特币已经不是“一个CPU一票”了，这也背离了当初“中本聪”的设计，比特币网络已经基本上被几大矿池所垄断，背离了去中心化货币这一初衷。