

比特币如何挖矿（挖矿原理）-工作量证明

2017-11-04 | 2018-07-31 | [比特币](#)

在[区块链记账原理](#)一篇，我们了解到记账是把交易记录、交易时间、账本序号、上一个Hash值等信息计算Hash打包的过程。

我们知道所有的计算和存贮是需要消耗计算机资源的，既然要付出成本，那节点为什么还要参与记账呢？在中本聪（比特币之父）的设计里，完成记账的节点可以获得系统给与的一定数量的比特币奖励，这个奖励的过程也就是比特币的发行过程，因此大家形象的把记账称为“挖矿”，本文将详细讨论这个过程。

记账工作

由于记账是有奖励的，每次记账都可以给自己凭空增加一定数量的个比特币（当前是12.5比特币，博文写作时每个比特币是4万人民币以上，大家可以算算多少钱），因此就出现大家争相记账，大家一起记账就会引起问题：出现记账不一致的问题，比特币系统引入工作量证明来解决这个问题，规则如下：

- 一段时间内（10分钟左右，具体时间会与密码学难题难度相互影响）只有一人可以记账成功
- 通过解决密码学难题（即工作量证明）竞争获得唯一记账权
- 其他节点复制记账结果

不过在进行工作量证明之前，记账节点会做进行如下准备工作：

- 收集广播中还没有被记录账本的原始交易信息
- 检查每个交易信息中付款地址有没有足够的余额
- 验证交易是否有正确的签名
- 把验证通过的交易信息进行打包记录
- 添加一个奖励交易：给自己的地址增加12.5比特币

如果节点争夺记账权成功的话，就可以得到12.5比特币的奖励。

工作量证明

[区块链记账原理](#)我们了解到，每次记账的时候会把上一个块的Hash值和当前的账页信息一起作为原始信息进行Hash。

如果仅仅是这样，显然每个人都可以很轻松的完成记账。

为了保证10分钟左右只有一个人可以记账，就必须要提高记账的难度，使得Hash的结果必须以若干个0开头。同是为了满足这个条件，在进行Hash时引入一个随机数变量。

用伪代码表示一下：

1 Hash(上一个Hash值, 交易记录集) = 456635BCD

1 Hash(上一个Hash值, 交易记录集, 随机数) = 0000aFD635BCD


我们知道改变Hash的原始信息的任何一部分，Hash值也会随之不断的变化，因此在运算Hash时，不断的改变随机数的值，总可以找的一个随机数使的Hash的结果以若干个0开头（下文把这个过程称为猜谜），率先找到随机数

的节点就获得此次记账的唯一记账权。

计算量分析

（这部分可选阅读）我们简单分析下记账难度有多大，Hash值是由数字和大小写字母构成的字符串，每一位有62种可能性（可能为26个大写字母、26个小写字母，10个数字中任一个），假设任何一个字符出现的概率是均等的，那么第一位为0的概率是1/62（其他位出现什么字符先不管），理论上需要尝试62次Hash运算才会出现一次第一位为0的情况，如果前两2位为0，就得尝试62的平方次Hash运算，以n个0开头就需要尝试62的n次方次运算。我们结合当前实际区块#493050信息来看看：

区块 #493050

概览		哈希值	
交易次数	2428	哈希值	00000000000000000003c76fb6e49de8c9f038971f1224e4d23ed72ce96eaea8c
总输出量	105,563.92341131 BTC	上一区块	0000000000000000009606f32345f878841aa4e836fbaca54139fefec3dc14fb
预计交易量	1,084.63321235 BTC	下一区块	
交易费	1.54816407 BTC	二进制哈希树根	c017e2dc67bfb80efab3e4cc913f54674521eb148149a46989ce5fdc8dce335e
高度	493050 (主链)		
时间戳	2017-11-04 14:47:52		
时间	2017-11-04 14:47:52		
播报方	BTC.com		
难度系数	1,452,839,779,145.92		
计算目标	402702781		
大小	1043.455 kB		
重量	3992.704 kWU		
版本	0x20000000		
随机数	2776680252		
新区块奖励	12.5 BTC		

注：数据来源于<https://blockchain.info>

我们可以看到Hash值以18个0开头，理论上需要尝试62的18次方，这个数是非常非常巨大的，我已经算不清楚了，应该是亿亿级别以上了。如此大的计算量需要投入大量的计算设备、电力等，目前应该没有单矿工独立参与挖矿了，基本都是由矿工联合起来组成矿池进行挖矿（矿池里的矿工按算力百分比来分收益）。

从经济学的角度讲，只有挖矿还有收益（比特币价格不断上涨也让收益变大），就会有新的矿工加入，从而加剧竞争，提高算力难度，挖矿就需要耗费更多的运算和电力，相互作用引起最终成本会接近收益。

题外话：国内由于电力成本较低，相对收益更高，中国的算力占整个网络的一半以上

验证

在节点成功找到满足的Hash值之后，会马上对全网进行广播打包区块，网络的节点收到广播打包区块，会立刻对其进行验证。

如果验证通过，则表明已经有节点成功解谜，自己就不再竞争当前区块打包，而是选择接受这个区块，记录到自己的账本中，然后进行下一个区块的竞争猜谜。

网络中只有最快解谜的区块，才会添加的账本中，其他的节点进行复制，这样就保证了整个账本的唯一性。

假如节点有任何的作弊行为，都会导致网络的节点验证不通过，直接丢弃其打包的区块，这个区块就无法记录到总账本中，作弊的节点耗费的成本就白费了，因此在巨大的挖矿成本下，也使得矿工自觉自愿的遵守比特币系统的共识协议，也就确保了整个系统的安全。

进阶阅读[比特币区块结构Merkle树及简单支付验证分析](#)，可以详细了解区块结构如何验证交易。

说明

矿工的收益其实不仅仅包含新发行的12.5比特币奖励，同时还有交易费收益（本文忽略一些细节是为了让主干更清晰）。

有兴趣的同学可以看看图中区块都包含了那些信息，红箭头标示出的是本文涉及的信息。

本文中有提到共识协议，比特币共识协议主要是由工作量证明和最长链机制 两部分组成，请阅读[比特币如何达成共识 - 最长链的选择](#)。