

区块链入门教程第二期：挖矿？

上一期我们讲了关于区块链的基本知识，链接在这《区块链入门教程第一期：区块链》，今天我们就来讲一下区块链关于挖矿的知识。

作者：BCTOPIA区块链学院 来源：今日头条 | 2018-06-14 11:15

收藏 分享

开发者盛宴来袭！7月28日51CTO首届开发者大赛决赛带来技术创新分享

上一期我们讲了关于区块链的基本知识，链接在这《区块链入门教程第一期：区块链》，今天我们就来讲一下区块链关于挖矿的知识。



一、挖矿和矿工

在上一期我们已经说了，区块链是由很多个节点组成的，为了保证节点之间的同步，所以每一个新区块的添加速度不能太快。试想一下，你刚刚同步了一个区块，准备基于它生成下一个区块，但这时别的节点又有新区块生成，你不得不放弃做了一半的计算，再次去同步。因为每个区块的后面，只能跟着一个区块，你永远只能在最新区块的后面，生成下一个区块。所以，你别无选择，一听到信号，就必须立刻同步。

所以，区块链的发明者中本聪（这是假名，真实身份至今未知）故意让添加新区块，变得很困难。他的设计是，平均每10分钟，全网才能生成一个新区块，一小时也就六个。

这种产出速度不是通过命令达成的，而是故意设置了海量的计算。也就是说，只有通过极其大量的计算，才能得到当前区块的有效哈希，从而把新区块添加到区块链。由于计算量太大，所以快不起来。

编辑推荐

- 热点** 80万年薪挖不来一个区块链工程师，转型潮却远未到来
- 头条** 盘点国内十个最大以区块链为名义进行诈骗的项目
- 关注** 区块链硅谷之争，中国已掉队？
- 头条** 深度解析：区块链的数据存放在哪？如何保存个人的信息数据？
- 关注** 华为云应用服务“完美搭配”助力企业开发上云更高效

24H热文 一周话题 本月最赞

- 区块链的去中心化能否真正实现？
- 看看区块链未来应用的36种场景，有你从事...
- 区块链是目前最热门的技能之一，你对它了...
- 物联网有望成为区块链的杀手级应用
- 全球最牛的四个区块链项目都在这里！
- 从Java到区块链：如何成为一名区块链开发...
- 盘点国内十个最大以区块链为名义进行诈骗...
- 3000多人被骗3亿元！又一区块链骗局曝光

视频课程

[+更多](#)

-  **【王佩丰】Excel VBA视频教程 完整版**
讲师：王佩丰 983019人学习过
-  **2018年软考信息系统项目管理师-论文写作精讲**
讲师：小任老师 74406人学习过
-  **MySQL入门实战精讲视频课程**
讲师：谢星星 5012人学习过

CTO专属活动

[+ 更多](#)

这个过程就叫做采矿（ mining ），因为计算有效哈希的难度，好比在全世界的沙子里面，找到一粒符合条件的沙子。计算哈希的机器就叫做矿机，操作矿机的人就叫做矿工。

二、难度系数

读到这里，你可能会有一个疑问，人们都说采矿很难，可是采矿不就是用计算机算出一个哈希吗，而计算也正是计算机的强项啊，怎么会变得很难，迟迟算不出来呢？

原因为不是任意一个哈希都可以，只有满足条件的哈希才会被区块链接受。这个条件特别苛刻，使得绝大部分哈希都不满足要求，必须重算。

因为每一个区块都包含了一个难度系数（ difficulty ），这个值决定了计算哈希的难度。举例来说，第100000个区块的难度系数是 14484.16236122。我们也可以将difficulty简单的可以理解为：挖到数据区块的所用时间多少。

同时难度值 difficulty的计算公式为：**难度值 = 最大目标值 / 当前目标值**

那什么是目标值：目标值是当前区块生成所达成目标值的hash值，用于矿工的工作量证明。矿工挖掘的区块的头部hash值必须小于目标值，数据区块才能被挖掘成功。

当前目标值是指现在产生数据区块的头部信息hash值参考指标。最大目标值是一个定值：0x00000000FF。

由于只有小于目标值的哈希才是有效的，否则哈希无效，必须重算。由于目标值非常小，哈希小于该值的机会极其渺茫，可能计算10亿次，才算中一次。这就是采矿如此之慢的根本原因。

上一篇文章也说过，当前区块的哈希由区块头唯一决定。如果要对同一个区块反复计算哈希，就意味着，区块头必须不停地变化，否则不可能算出不一样的哈希。区块头里面所有的特征值都是固定的，为了让区块头产生变化，中本聪故意增加了一个随机项，叫做 Nonce。

Nonce 是一个随机值，矿工的作用其实就是猜出 Nonce 的值，使得区块头的哈希可以小于目标值，从而能够写入区块链。Nonce 是非常难猜的，目前只能通过穷举法一个个试错。根据协议，Nonce 是一个32位的二进制值，即最大可以到21.47亿。第 100000 个区块的Nonce 值是274148111，可以理解成，矿工从0开始，一直计算了 2.74 亿次，才得到了一个有效的 Nonce 值，使得算出的哈希能够满足条件。

运气好的话，也许一会就找到了 Nonce。运气不好的话，可能算完了21.47亿次，都没有发现 Nonce，即当前区块体不可能算出满足条件的哈希。这时，协议允许矿工改变区块体，开始新的计算。

三、难度系数的动态调节

正如上一篇所说，采矿具有随机性，没法保证正好十分钟产出一个区块，有时一分钟就算出来了，有时几个小时可能也没结果。总体来看，随着硬件设备的提升，以及矿机的数量增长，计算速度一定会越来越快。

为了将产出速率恒定在十分钟，中本聪还设计了难度系数的动态调节机制。他规定，难度系数每两周（ 2016个区块 ）调整一次。如果这两周里面，区块的平均生成速度是9分钟，就意味着比法定速度快了10%，因此接下来的难度系数就要调高10%；如果平均生成速度是11分钟，就意味着比法定速度慢了10%，因此接下来的难度系数就要调低10%。

难度系数越调越高（ 目标值越来越小 ），导致了采矿越来越难。

申请试听：CTO的4D领导力，打造你的管理

白熊视频：揭秘京东618背后的程序员GG

走访美团：美团背后的技术基因

CTO训练营		
申请入营	互联网班	金融班
CTO俱乐部		
申请加入	最新活动	全部课程

最新专题+更多



ThinkPad



运维/思考/AIOps



数据科学



Spring

精彩评论

- sqskg评论了：高通华裔工程师跳楼自杀！中年IT男，为何这么难？
- 这里说的确实比较现实，也比较残酷；
- 白色面具评论了：“无限流量”套餐偷偷扣钱，工信部都看不下去了！
- 都是套路 国企和部门联合套路吃瓜群众
- yeshou评论了：再见铁饭碗！又一个行业被颠覆！中国建设银行正式宣布
- 谁又在贩卖焦虑。

但是，有人会问，区块链是一个去中心化的，这个难度是由谁来调节的呢？难度的调整是在每个完整节点中独立自动发生的。每2,016个区块中的所有节点都会调整难度。难度的调整公式是由最新2,016个区块的花费时长与20,160分钟（两周，即这些区块以10分钟一个速率所期望花费的时长）比较得出的。难度是根据实际时长与期望时长的比值进行相应调整的（或变难或变易）。简单来说，如果网络发现区块产生速率比10分钟要快时会增加难度。如果发现比10分钟慢时则降低难度。

这个公式可以总结为：

$$\text{New Difficulty} = \text{Old Difficulty} * (\text{Actual Time of Last 2016 Blocks} / 20160 \text{ minutes})$$

四、矿工的收益

既然挖矿不容易，为什么有人愿意做矿工呢？以比特币举例。

一是交易的确认离不开矿工。

二是比特币协议规定，挖到新区块的矿工将获得奖励，一开始（2008年）是50个比特币，然后每4年减半，目前（2018年）是12.5个比特币。这也是比特币的供给增加机制，流通中新增的比特币都是这样诞生的。

你可能看出来了，每4年奖励减半，由于比特币可以分割到小数点后八位，那么到了2140年，矿工将得不到任何奖励，比特币的数量也将停止增加。这时，矿工的收益就完全依靠交易手续费了。

所谓交易手续费，就是矿工可以从每笔交易抽成，具体的金额由支付方自愿决定。你完全可以一毛不拔，一分钱也不给矿工，但是那样的话，你的交易就会没人处理，迟迟无法写入区块链，得到确认。矿工们总是优先处理手续费最高的交易。

目前由于交易数量猛增，手续费已经水涨船高，一个区块2000多笔交易的手续费总额可以达到3~10个比特币。如果你的手续费给低了，很可能过了一个星期，交易还没确认。

一个区块的奖励金12.5个比特币，再加上手续费，收益是相当可观的。按照目前的价格，可以达到75万人民币左右。想想看，运气好的话，几分钟就能挖到一个区块，拿到这样一大笔钱，所以人们才对挖矿趋之若鹜。

五、总结

一句话，矿工存在的原因的就是目前现在的收益大于自己的成本，有利可图这才是人性。

【编辑推荐】

1. 2018年区块链高考统一试题（A、B卷）
2. 说起来容易做起来难，区块链实施需要注意哪些？
3. 3000多人被骗3亿元！又一区块链骗局曝光
4. 区块链能够给物联网带来什么？
5. 区块链原理是什么？如何开发区块链程序？

【责任编辑：庞桂玉 TEL：(010) 68476606】

点赞 2

wx5b4431ad1fa56评论了：如何配置MySQL数据库超时设置

好文章

精选博文 论坛热帖 下载排行

Gitlab+Jenkins实现自动部署

快速生成百度地图大数据覆盖物的方法

与树莓派谈共享 Windows有现成的NFS

单机部署open-falcon 0.2

swarm 部署高可用harbor

读书

+更多



主流ARM嵌入式系统设计技术与实例精解

本书重点介绍了主流ARM应用系统的开发与实践。全书基于目前较为通用、流行的ARM处理器，介绍了其原理、硬件结构、硬件电路设计与开发和软件...



订阅51CTO邮刊

点击这里查看样刊

立即订阅

51CTO区块链社群正式开通

全球视野下的行业大势、国内外最新政策、区块链技术应用、案例解析、数字货币市场动态、相关投资经验.....区块链领域全方位价值信息，尽在51CTO区块链社群。大势已来，让我们共同缔造历史！



51币读官微

[区块链](#)[数字货币](#)[比特币](#)

分享:

内容点评

已有 0 条评论, 0 次赞

还可以输入500字

请输入你的评论

您还没有登录！请先 [登录](#) 或 [注册](#)

提交

还没有评论内容

大家都在看 猜你喜欢



AI Ops实践三板斧：从可视化、自动化到智能化



宜信研发总监张真：运维机器人之任务决策系统演进



看Kubernetes如何为“中国-东盟信息港”赋能



ZStack的云计算之路：黑科技层出不穷 产品化坚持不懈

51CTO旗下网站：领先的IT技术网站 51CTO | 领先的中文存储媒体 WatchStor | 中国首个CIO网站 CIOage | 中国首家数字医疗网站 HC3i

Copyright©2005-2018 51CTO.COM 版权所有 未经许可 请勿转载