挖矿的 7 个步骤

想知道在区块链上是如何挖矿的，交易是如何上链的?

没有找到一个清晰的可以一步一步解释这个过程的文章，于是我决定自己写一篇。以下就是我的分享，在区块链上矿工挖矿的7个步骤。

步骤一

用户进入钱包[1]，执行一个交易操作，他将一个加密货币或者一个token发送给另一个用户。

步骤二

现在这个交易被钱包[2]广播，等待区块链上的矿工们来拾取它。在被拾取前，它会一直在“**未确认交易池**”中等待。

所有等待被处理的交易都会在未确认交易池中，未确认交易池不是网络上的一个巨大的池，而是很多小的分散的本地池。

步骤三

区块链网络上的矿工(有时叫节点，但不完全一样)从未确认交易池中选择交易打包成数据块。除了一些额外的元数据外，数据块基本上就是交易数据(此时仍然是未确认交易)。每个矿工打包它们拾取的交易数据块，多个矿工可以选择同样的交易数据打包。例如，两个矿工，矿工A和矿工B都决定打包交易X。

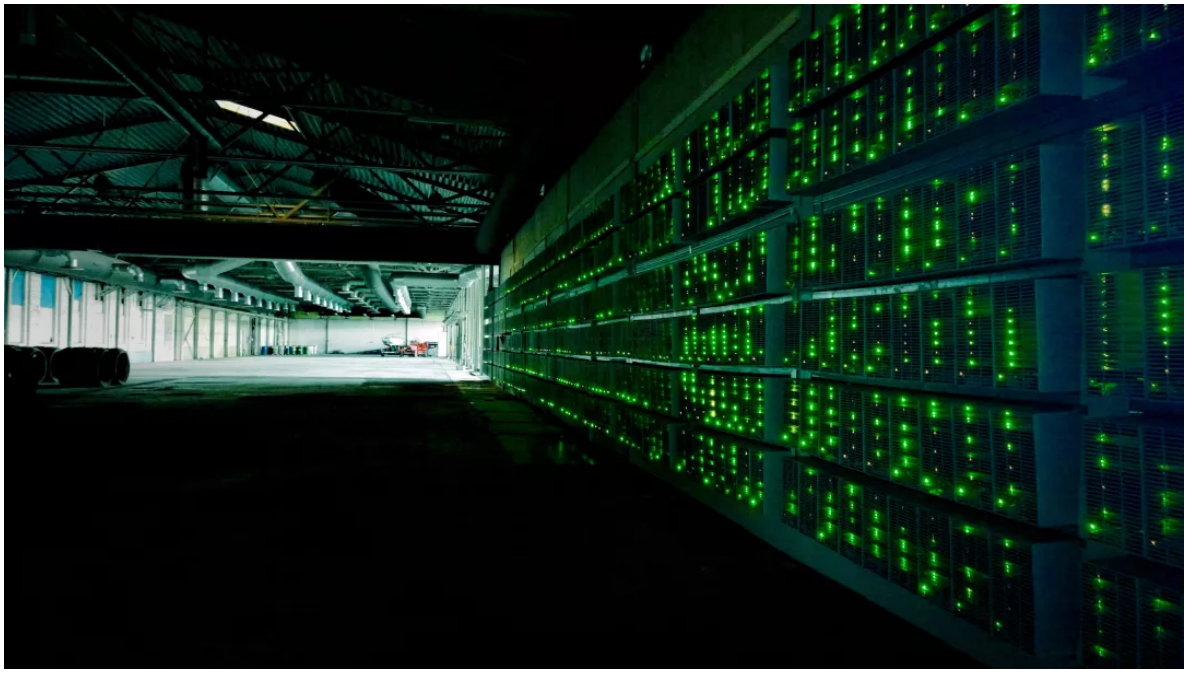
每个区块链对数据块都有最大限制。在比特币区块链上，这个最大值是1MB。

在打包交易前，矿工需要先根据区块链的历史数据检查这个交易是否有资格被打包。根据区块链历史数据记录，如果支付者的钱包里有足够的余额，这笔交易被认为是有效的，并且可以被打包上链。

假如一个比特币持有者想要加速他的交易进度，他可以选择支付更高的挖矿奖励。矿工通常会优先打包这些支付更高挖矿奖励的交易。

步骤四

矿工的工作就是选择交易数据并打包成块。要把这些块添加到区块链上(这意味着让区块链上所有节点都接受这个块的数据)，这个数据块首先需要签名(也叫“工作证明”)。这个签名是在解决了一个非常复杂的数学问题后得到的，这个签名是独一无二的。每个区块需要解决的数学问题难度是一样的。为了解决这个数学问题，需要耗费相当多的**算力**(所以，要消耗相当多的电力)。这个过程就被叫做挖矿。如果你想知道更多关于这个问题的内容，请继续阅读，如果你只想简单了解一下，请跳到第五步。



挖矿即哈希(工作量证明[3])

矿工在打包块时需要解决的数学问题实际上就是找到一个以一定量的零开头的哈希函数的输出结果(就是签名)。这听起来很复杂对吗？但是它并不难理解。

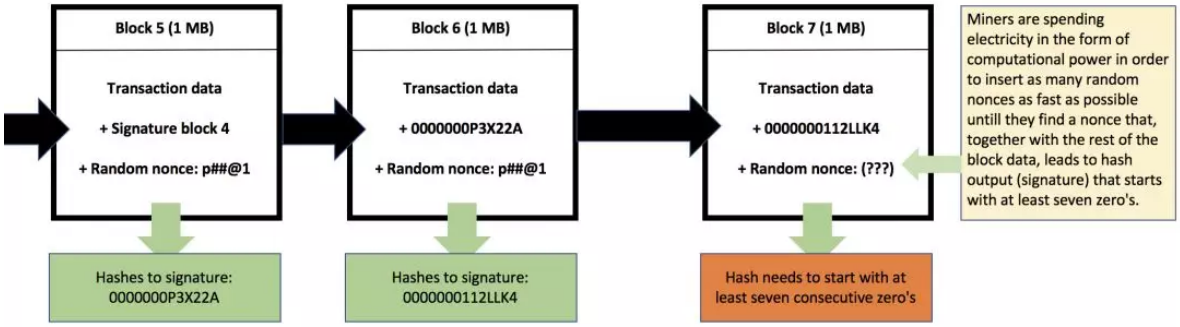
开始之前，我们需要先了解一下什么是哈希函数。哈希函数很难解，但其结果非常容易验证。

哈希函数的输入值可以是任意字符串，随机输出一个32位的字母和数字的字符串。如果输入中有任何一点小小的变动，输出也将会随机改变。然而，同样的输入字符串只会得到同样的输出。

矿工要打包的交易数据就是一个字符串，将它进行哈希计算，就会得到一个32位的输出值。比特币区块链有一个规则，要求打包的数据块签名必须以一定数量的零开头。然而哈希计算的输出值是对它的每个输入值都是随机的，那么，输入的字符串哈希后没有得到这么多零开头的值怎么办呢？这就是为什么矿工需要不断的去改变块里面一个叫"nonce"的值，每改变一次nonce的值，就会改变块的数据，哈希运算后得到的签名也会不一样，也就是，每改变一次nonce的值，就会得到一个全新的签名。

矿工无限次重复改变nonce的值，直到得到一个符合要求的签名。

下图例子中，签名是以7个零开头的。但是具体需要多少个零，取决于区块链上的区块难度。区块难度的问题相对要难一些，所以我建议你先收藏block difficulty[4] 。



这就是矿工们为什么需要为它们打包的数据块找到一个合格的签名，也是需要那么多算力来解决这个数学问题的原因。试想一下需要这么多次更改nonce值并计算需要多少时间和算力呀。此外，当更多的矿工加入到区块链，哈希运算的难度也将增加并且会导致更高的电费支出。现在我们继续第五步。

注意：此过程实际上不是定义为数学问题，而是定义确定性问题 - 计算机对数字执行预先确定的操作，以查看输出是否可取。

步骤五

矿工找到了一个合格的签名，他就可以向其他所有矿工广播他的数据块和签名。

步骤六

其他矿工现在要确认通过广播收到的数据块的签名合法性，他们要对这个数据块进行哈希运算，检查它是否输出一个以这么多零开头的签名。如果可以，其他矿工就会认为这个数据块有效，并且同意将它添加到区块链上(他们达成了共识，即他们所有矿工都同意彼此，所以术语叫共识算法)。这也是"工作量证明"的来源。签名就是矿工工作的证明(已花费的算力)，现在，数据块可以加到区块链上了，并且分发到网络上所有其他节点。只要这个数据块中的所有交易数据都跟区块链上的历史数据符合，其他节点将接收这个数据块并将其保存。

步骤七

当一个数据块被添加到区块链上后，这条区块链上的所有块都认为它是正确的。例如，我的交易包含在第502号块中，并且这条区块链现在最长是第507号块，它的意思就是说我的交易数据被确认过5次(507-502)。它被认为是正确的，因为每次有其他块上链的时候，区块链都会就所有交易记录达成共识，包括你的交易和你的块。你可以说，到这个时候，你交易已经被确认了5次。这也是Etherscan在显示交易详细信息时所指的。你的交易被确认的次数越多(即嵌入区块链越深)，攻击者就越难更改它。每当新的块加入到区块链，所有矿工都需要从第三步重新开始，打包一个新的交易数据块。

> 在完成一个块上链前，矿工们不能继续挖矿。
>
> 1、它可能包含已添加到区块链上已经确认过的交易(请记住，多个矿工可以选择同一个交易数据处理)，任何重新发起的交易都可能导致它们无效，因为支付者的余额可能已经不足。
>
> 2、每个块都需要将区块链上的最后一个块的哈希签名添加到到他们自己的元数据中。这也是让数据块链起来的原因。假如一个矿工打包的是已经上链的块，其他矿工会注意到它的签名和区块链上最后一个数据块对不上，并且会拒绝这个块。本文首发于系统学习区块链技术[5]博客——深入浅出区块链[6] - 打造高质量区块链技术博客，学区块链都来这里，关注知乎[7]、微博[8] 掌握区块链技术动态。

References

[1] 钱包: *https://learnblockchain.cn/2019/04/11/wallet-dev-guide/* [2] 钱包: *https://learnblockchain.cn/2019/04/11/wallet-dev-guide/* [3] 工作量证明: *https://learnblockchain.cn/2017/11/04/bitcoin-pow/* [4] block difficulty: *https://blog.goodaudience.com/blockchain-the-mystery-of-mining-difficulty-and-block-time-f07f0ee64fd0* [5] 系统学习区块链技术: *https://learnblockchain.cn/2018/01/11/guide/* [6] 深入浅出区块链: *https://learnblockchain.cn/* [7] 知乎: *https://www.zhihu.com/people/xiong-li-bing/activities* [8] 微博: *https://weibo.com/517623789*