比特币挖矿科普专辑到这里就要收尾了，经过前两篇文章铺垫，相信读者朋友已经对比特币交易和区块产生的过程有一定的认识。那么它们跟“挖矿”有什么关系呢？

我们知道，在比特币网络中，有很多挖矿节点和矿工参与创建比特币新区块。如果多个挖矿节点都创建了同一个高度的区块，该判定谁的区块更合法呢？比特币引入了PoW（Proof of Work）共识机制，通过挖矿的方式，来竞争新区块的记账权。谁拿到新区块的记账权，它创建的新区块就合法。挖矿的目的就是赢取记账权，确认新区块和交易。那么挖矿节点和矿工是如何配合工作，完成挖矿的呢？

矿工破解挖矿任务

挖矿节点创建好预备区块后，将预备区块的区块头数据发送给矿工。矿工收到挖矿任务后，会递增区块头中的随机数。每调整一次，就会按照比特币协议规定，用SHA256算法计算区块头的哈希值。如果区块头的哈希值大于目标哈希，就继续变更随机数，直到区块头的哈希值小于或者等于目标哈希为止（或者挖矿节点发现新区块已经由其他节点挖到，此时就会放弃原来挖矿任务，构造新的预备区块，重新开始挖矿）。

挖矿节点验证区块，延长本地区块链

当矿工找到可以使预备区块头哈希值小于目标哈希的随机数时，会立即向挖矿节点上报挖矿结果。挖矿节点接收到信息后，立刻按照矿工上报信息重组区块，并验证区块。验证无误后，挖矿节点将新区块保存到节点本地数据库，并添加到节点本地区块链上。

区块的验证信息包括：

区块头是否合法（区块头哈希≤TargetHash）；

区块头的MerkleRoot哈希跟区块中交易数据的MerkleRoot哈希是否一致（验证交易是否被篡改）；

交易数据中第一笔是否为Coinbase交易；

区块中每一笔交易是否合法等等。

向全网广播新区块

挖矿节点将新区块在本地保存后，同步向比特币网络广播挖矿结果。由于整个区块的区块体积较大，一般会先广播新区块的区块头。其他节点在接到广播后，先验证区块头信息，验证通过后，节点会先在其本地的区块索引库中创建新区块的索引。在接收到新区块的全部信息后，节点验证交易信息和区块头的MerkleRoot哈希，验证通过后，节点将这些交易信息录入新区块，并延长本地区块链。至此，新区块的广播和验证完毕，挖矿节点开始下一个区块的挖矿工作。

当前挖矿的一些特点集群挖矿-矿池：

比特币挖矿这件事情，理论上任何人都可以自建比特币挖矿节点，参与挖矿，甚至可以通过手工验证区块头哈希，破解挖矿任务，竞争记账权。

但博主在上一文中提到，按照当前的挖矿难度，即便使用现在的主流矿机，要找到一个符合比特币网络要求的新区块，理论上需要42年时间，而如果使用普通PC或者是手工计算，则需要上万年甚至上百万年。

因此，普通矿工单独挖矿的经济效益太低，可能挖到机器报废，还挣不到一分钱。矿池就是在这种情况下应运而生的，大量矿工将自己的矿机接入矿池，从矿池的挖矿节点获取挖矿任务，集体挖矿。这样就可以在较短时间内挖到新区块，获得区块奖励，矿池按照挖矿过程中每个矿工的贡献情况，分配挖矿收益，所有矿工都可以实时获取挖矿收益，进行回本或者二次投资。

矿机实际收到的挖矿任务中，TargetHash远大于比特币网络要求的TargetHash：

矿池和矿工一起挖矿的流程，一样遵循上述过程。矿机通过网络跟矿池通讯，请求挖矿任务，矿池将挖矿任务（包含区块头等数据）发送给矿机，矿机变更区块头的随机数，并验证区块哈希。符合挖矿任务TargetHash要求的随机数，将按照挖矿协议的格式提交给矿池，矿池给矿机提交的挖矿结果计算收益。

需要注意的是，如果给矿机下发的挖矿任务中，TargetHash是此时比特币网络的TargetHash，那么这个TargetHash太小，矿机基本不可能找到符合要求的随机数，提交挖矿结果，也就不可能获得挖矿收益。

因此，矿池给矿机下发的挖矿任务中，有一个单独的信息：初始挖矿难度。这是一个远低于全网挖矿难度的数值，对应更大的TargetHash，在这个难度下，矿机可以在较短时间内找到符合要求的随机数，向矿池提交更多挖矿结果。

矿池算力不同于矿机本地算力：

谈及挖矿，总有一个绕不开的名词：算力。到底什么是算力呢？

算力，其实就是矿工验证区块头哈希值的速度。矿机在获得挖矿任务后，会按照挖矿任务的信息，递增区块头的随机数，随机数每调整一次，就验证一次区块头的哈希值。可以看到，限制矿机挖矿快慢的唯一一个因素就是它验证区块头哈希值的快慢，因此有了“算力”这个指标。

目前，常规比特币矿机的算力单位是TH/s，它的意思，每秒钟可以验证1T次哈希，1T=1×103G=1×106M=1×109K=1×1012次。

有过挖矿经历的朋友，都会发现，矿机本地显示的算力跟矿池显示的算力总是有差异。这是因为，矿机本地显示的算力，是矿机验证哈希的速度，它只跟矿机的性能有关，不管有没有找到符合挖矿任务要求的随机数，矿机本地算力都一直存在。而矿机在矿池显示的算力则不同，它是矿池按照矿机实际提交的挖矿结果计算出来的，如果矿机的运气较差，在较长时间内都没有找到符合挖矿任务要求的随机数，无法向矿池提交挖矿结果，矿机在矿池的算力就会降低。

但时间拉长后，运气对矿机破解挖矿任务的影响会降低，矿机较长时间的矿池平均算力，跟矿机本地算力相差不大。

以上是比特币挖矿的基础知识，如果能读懂这三篇文章，相信读者朋友对比特币挖矿会有一个初步的认识。如果想要跟博主交流探讨更多挖矿方面的问题，欢迎关注“闲话挖矿”微信公众号，同时也能更及时的了解博主更新的挖矿知识。

文中涉及的几个知识点：

区块高度：又叫Block Height，相当于区块的编号，它的值等于区块链中这个区块之前所有区块的数量。区块链的第一个区块是创世区块，区块高度为0，第二个区块的区块高度为1，第三个区块的区块高度为2，以此类推。区块链中区块的总数，即为最新区块的区块高度+1。

PoW：全称为Proof of Work，中文名称为工作量证明。是比特币网络使用的一种用于解决比特币新区块确权问题的方法。在比特币网络中，人人都可以参与新区块的创建工作，PoW机制规定，谁能够在最短时间内找到一个区块头哈希值小于比特币网络指定的TargetHash的预备新区块，谁就拥有正式新区块的记账权。

记账权：比特币的区块链，实质上是一个链式的大账本，链上的每一个区块，都是一本账，上边记录了发生在区块链上的比特币交易信息。因此，我们把创建新区块的过程看作记账的过程。记账权，顾名思义为记录交易账本的权利，也即在比特币

区块链上创建正式新区块的权利。