这是博主的第二个内容&#039；的采矿科普专辑。上一篇文章《比特币交易流程》之后，继续分析比特币挖矿从发起到确认的全过程。

比特币的交易过程，本质上就是一堆UTXO的消费和生成过程。。这些流程由交易发起方按照比特币协议中规定的方法构建，由比特币网络生成。记录并确认新块。交易信息一旦被比特币区块记录确认，交易就完成了，比特币网络也实现了价值的转移。

在文章《比特币交易流程》中，我们已经知道比特币的交易信息是如何构造的，但是这些信息是如何进入比特币的新区块的呢？

接下来，博主将通过创建一个新的比特币区块的过程，详细说明比特币区块是如何记录和确认交易信息的。

以下是一些关于安利的知识：

事务池也称内存池，用于存储待确认的事务。。每个比特币挖矿节点都有自己独立的交易池。由于交易池的交易量，最低交易手续费率(本文所说的交易手续费率是单位交易量中包含的费用，单位为Sat/B，即每笔B字节的交易手续费为X比特币。，下同)限制。交易池也不同。当采矿者(矿石池)建立储备区块时，他们需要从交易池中选择要打包的交易。因为事务池被频繁调用，所以它的数据存储在节点服务器

的RAM中

比特币网络中的挖矿节点参与记录和验证比特币交易，区块是存储比特币数据的节点。一些节点不仅参与记录和验证工作，还参与创建新的比特币区块。他们通过PoWworkloadproof构建新块，并争夺记账权。，然后获得创建新块的权限。这些节点是挖掘节点。早期有矿工，有矿池，但目前由于比特币挖矿难度大，单个矿工很难获得记账权，也很难创造新的区块。目前主要的比特币挖矿节点是各种矿池，比如，等等。

UTXO库，比特币节点通过扫描节点的所有交易信息，构建一个UTXO集群。它包含所有未使用的UTXO。每当生成一个新块时，UTXO库都会从自己的列表中删除新块中消耗的UTXO。，并将新生成的UTXO添加到您自己的列表中。

奖励，也称为硬币创造交易。比特币协议规定，每生成一个新的比特币块，比特币网络就会生成N个比特币，作为维护奖励支付给上线的比特币网络。。建造这个街区的矿工。同时，该区块中除奖励外的其他交易所包含的所有交易费用也将合并到奖励中，支付给创建该区块的矿工。其中，比特币诞生时，n值为50，之后每四年

减半。目前是6.25。。@比特币的总量。奖励是每个区块中记录的第一笔交易。

待确认的交易会先进入交易池

当我们要发起一个比特币交易时，交易发起方会构造交易信息。此时的交易信息有待确认。，包括交易输入信息(未使用的UTXO和正确的私钥签名)和交易输出信息(未确认的UTXO锁定的新钱包地址)。

交易验证后，由交易发起方广播至比特币网络。比特币网络中的节点可以验证并记录广播信息。其中，挖掘节点在接收到广播后会对待确认的交易信息进行验证。验证通过后，挖掘节点将要处理的交易添加到自己的交易池中。

图1待处理的交易进入交易池

需要验证的交易信息包括：

交易是否包含有效的输入/输出钱包地址；交易量是否小于块的最大大小(比特币块的最大大小目前是1m)；输入的UTXO合法吗(与节点的UTXO库相比)，输入的UTXO没有用过)；交易的总投入和总产出是否合理(总投入总产出)；判断交易的输入是否可用。，对应的货币至少需要100块确认后才能使用；确认交易池中没有重复交易；交易设置交易成本高于交易成本比率(Sat/B)的限制，以及其他验证(如隔离交易的验证和跟踪)。

挖掘节点从事务池中选择事务，构建一个预备块

当挖掘节点要构建一个预备块，准备生成新块时，会按优先级排序，从事务池中取出要处理的事务。保留块通常为高优先级事务保留一些空间。，剩余空间将根据交易手续费率(Sat/B)从高到低填满区块，或者用完交易池中的交易。

但比特币区块包含的不仅仅是从交易池中提取的待处理交易。根据比特币协议比特币的块主要包括幻数、块大小、块头、交易计数器、交易信息五个部分。如下图：

图2比特币块的结构

其中"幻数&quot是一个常数值；"块卷&quot是块中所有数据的总容量；"块头&quot可以看作是整个区块的简称信息，用于挖掘。。块信息是块头；&quot交易计数器&quot用于记录块中的事务数量；"交易数据&quot是块中包含的所有交易信

息，包括奖励部分。一般来说，这部分数据占据了整个块。挡住大部分空间。比特币区块中的

块头是最重要的信息。包含了整个块的所有特征信息：

块版本号。创建该块的比特币节点的版本信息，用于跟踪比特币协议的升级和更新；前一个块的哈希值。也称为父块哈希，用于定位前一个块。。每个块都包含其前一个块的哈希值。任何一个块的微小变化都会导致后续块的哈希值发生巨大变化。所有比特币块形成单链结构，可以有效防止对比特币块数据的恶意篡改。哈希。在该块的交易数据列表中，取所有交易数据的hash值构建一棵树，这个树的根hash值就是hash(交易数据的树结构见图3)。由于哈希算法的敏感性，整个事务树中事务数据的任何微小变化都会产生联动效应，导致树的根哈希值发生很大变化。因此事务数据的根哈希值可以看作是整个事务的指纹，用来引用块中的事务数据。时间戳。创建准备块的时间。当前目标哈希。比特币协议规定，只有当矿工创建的预备块的哈希值小于目标哈希值时。，则该块有效。目标哈希值由挖掘难度决定。当挖掘难度增加时，目标哈希值变小，挖掘者更难找到符合比特币网络要求的哈希值。按照目前的挖掘难度，理论上S17矿机需要连续工作42年才能找到低于目标哈希值的哈希值。。所以基本不存在个人自建节点挖矿比特币的情况。随机数。也称为随机数。我们可以发现，在块头信息中，块版本号、前一个块的hash值、hash值、时间戳、当前目标hash都是已知信息，相对固定。不方便随意更改。所以，1个比特币需要多久？如果要调整块的哈希值，需要引入一个变量数据——和一个随机数。通过修改随机数，可以调整准备块的散列值。为了找到低于目标散列值的散列值理论上需要S17矿机连续工作42年。所以基本不存在个人自建节点挖矿比特币的情况。随机数。也称为随机数。我们可以在块头信息中找到块的版本号、前一个块的hash值、hash值、时间戳、当前目标hash都是已知信息，相对固定，不方便随意更改。因此，如果要调整块的散列值，则需要引入变量数据——和随机数。通过修改随机数，您可以调整准备块的哈希值。要找到低于目标哈希值的哈希值，理论上S17矿机需要连续工作42年。所以基本不存在个人自建节点挖矿比特币的情况。随机数。也称为随机数。我们可以找到在块头信息中，块版本号、前一个块的hash值、hash值、时间戳、当前目标hash都是已知信息，相对固定，不方便随意更改。因此，如果要调整块的散列值，则需要引入变量数据——和随机数。。通过修改随机数，可以调整准备块的散列值。基本上没有人设立自己的节点去挖矿比特币。随机数。也称为随机数。我们可以在块头信息中找到块的版本号、前一个块的hash值、hash值、时间戳、当前目标hash都是已知信息，相对固定，不方便随意更改。因此，如果要调整块的散列值，则需要引入变量数据——和随机数。通过修改随机数，您可以调整准备块的哈希值。基本上没有人设立自己的节点去挖矿比特币。随机数。也称为随机数。我们可以在块头信息中找出1个比特币需要多长时间。块的版本号、前一个块的hash值、hash值、时间戳、当前目标hash都是已知信息，相对固定，不方便随意更改。因此，如果要调整块的散列值，则需要引入变量数据—

—和随机数。通过修改随机数，您可以调整准备块的哈希值。哈希值、时间戳、当前目标哈希都是已知信息，相对固定，不方便随意更改。所以如果要调整块的hash值，需要引入一个变量data——和一个随机数。通过修改随机数，您可以调整准备块的哈希值。哈希值、时间戳、当前目标哈希都是已知信息，相对固定，不方便随意更改。所以如果要调整块的hash值，需要引入一个变量data——和一个随机数。通过修改随机数，您可以调整准备块的哈希值。

图3事务数据树结构

挖掘节点构造初步块后，会将块头信息发送给挖掘者。矿工通过不断调整块头中的随机数来改变预备块的散列值。。当预备块的哈希值低于当前比特币网络的目标哈希值时，这个块就是合法的新块。

挖矿节点会及时将新块广播到比特币网络，比特币网络中的其他比特币节点收到广播信息后会对新块进行验证。。块在本地添加和扩展节点的区块链。此时，新块被创建并确认，相应的事务完成。

参考：