一、两类节点的责任

比特币系统中有两种节点，一种是全节点，一种是轻节点。

1. 全节点的特征
2. 一直在线
3. 在本地硬盘上维护完整的区块链信息
4. 在内存中维护UTXO集合，以便快速检验交易的合法性
5. 监听比特币网络上的交易信息，验证每个交易的合法性
6. 监听别的矿工挖出的区块，验证其合法性：
   1. 区块中的每个交易都要合法（包括铸币交易及其出块奖励）
   2. 发布的区块是不是符合难度要求、难度目标阈值的设置是否正确、每两周调整的挖矿难度
   3. 区块是在延伸最长合法链
7. 挖矿：
   1. 决定沿着哪条链挖下去
   2. 决定哪些交易被打包进区块
   3. 决定当出现等长分叉时选择哪个分叉（缺省情况是选择最先接收到的区块的分叉）
8. 轻结点的特征
9. 不是一直在线
10. 不用保存完整区块链，只要保存每个区块块头（这样和全节点的大小相差大约1000倍）
11. 不用保存全部交易，只需要保存和自己相关的交易
12. 没法验证大多数交易的合法性，只能检验与自己相关的交易的合法性
13. 无法检测比特币网络上发布的区块的正确性
14. 可以验证挖矿的难度（因为挖矿时候计算哈希值只用到了块头信息，而块头信息轻节点是保存了的）
15. 只能检测哪个是最长链，不知道哪个是最长合法链（因为无法检测这条链上所包含的交易都是合法的）

注：轻节点假设矿工（全节点）大多是有理智的，即假设矿工们不会沿着不合法的链一直挖下去。比特币网络中大部分节点都是轻节点

二、挖矿

当在挖矿过程中发现新发布了一个区块，那么应该停止挖矿，重新从UTXO中取出一系列合法交易组成候选区块，在刚发布的这个区块后面开始挖矿。因为一方面这个区块中的交易可能和刚刚在挖的那个区块有重复，另一个本质的原因就是候选区块的块头有指向前一个区块的哈希指针。因为最新的区块已经变了，这个哈希指针也要跟着改变。

|  |
| --- |
| 比特币系统安全性的保证：因为别人没法伪造你的私钥，也就没法把你账户上的BTC转走。但这个密码学上的保证是要以“系统中大部分节点是诚实的”为前提，即大家不会接受那些不合法的交易进入区块链。 |

三、挖矿设备

第一代挖矿设备：CPU

最早时候大家都是用普通计算机来挖矿，但如果专门搞一台计算机来挖矿是很不划算的。因为计算机大部分内存是闲置的（挖矿只要用到很少一部分内存），CPU大部分部件是闲置的（计算哈希值的操作只用到通用CPU中的很少一部分指令），硬盘和其它很多资源也都是闲置的。随着挖矿难度提高，用通用计算机上的CPU挖矿很快就无利可图了。

第二代挖矿设备：GPU

GPU主要用来做通用的大规模并行计算，用来挖矿还是会有不少浪费，而且GPU的噪音很大，其中很多部件还是浪费了（如用于浮点数计算的部件）。近些年GPU价格涨得很快，这不仅是DL火热的原因，实际上很多GPU是买来挖矿的。不过现在挖矿的难度已经提高到用GPU也有些划不来了，不会再有那么多人买GPU来挖比特币。

第三代挖矿设备：ASIC芯片

ASIC即Application Specific Integrated Circuit，这之中有专门为了挖矿而设计的芯片，没有多余的电路，干不了别的事，它的性价比是最高的，而且为某一种加密货币设计的ASIC芯片只能挖这一种加密货币的矿，除非两个货币用同一个mining puzzle。

|  |
| --- |
| 有些加密货币在刚启动的时候，为了吸引更多的人来挖矿，特意用一个和已有的其它加密货币一样的mining puzzle，这种情况叫merge mining。 |

研制挖特定加密货币的ASIC芯片需要一定周期，但和研制通用芯片的速度相比已经是非常快的了，如研制比特币挖矿的ASIC芯片大约用一年的时间。不过加密货币的价格变化是比较剧烈的，曾经就发生过比特币价格在几个月内下跌80%，因为加密货币多变的价格，这些挖矿设备的研制风险也是很大的。

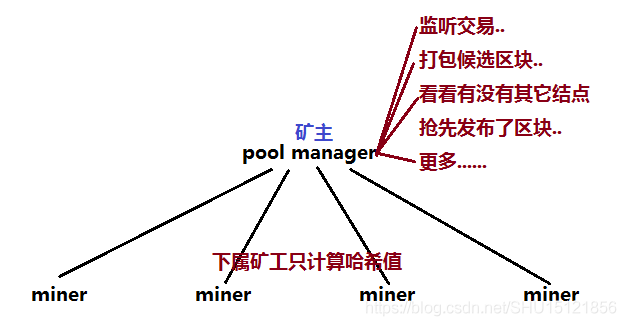
挖矿的竞争越来越激烈，定制的ASIC芯片可能用了几个月就过时了，到时候又要买新的ASIC芯片参与竞争。ASIC矿机上市后的大部分利润也就在前几个月，这个设备的迭代也是很块的。

要买ASIC矿机往往要先交钱预定，过一段时间厂商才会发过来。实际上有些黑心厂商在生产出来以后也不交付给用户，声称还没成产好，然后自己在这段黄金时间用矿机挖矿赚取比特币。不过这其实看得出来，比特币系统中算力突然有了大的提高，那一般是某个大的厂商生产出了新的矿机。所以真正赚钱的未必是挖矿的，而是卖矿机的。

四、比特币挖矿的趋势：大型矿池

单个矿工挖矿的收益是很不稳定的，平均出块时间10分钟是对于比特币系统中的所有矿工而言的。一个矿工用一个矿机挖出矿的时间可能要很久，并且除了挖矿之外还要承担全结点的其它责任。

矿池将很多矿工组织起来，一般的架构就是一个矿主（pool manager）全结点去驱动很多矿机，下属矿工只负责计算哈希值，全结点的其它职能只由矿主来承担。有了收益以后再大家一起分配。



矿池收益怎么分配？

如果矿池中的矿机都是属于同一个机构的，那怎么分配就只是公司内部怎么发工资的问题了。

如果矿机来自不同机构，这时候矿工很可能分布在世界各地，只是都加入了这个矿池。矿工和矿主联系，矿主将要计算的哈希值的任务分配给他，矿工计算好后将结果发给矿主，最终得到出块奖励后一起参与分红。

能否平均分配？即挖到区块后奖励平分给所有矿工。这样就完全是吃大锅饭的模式了，有的矿工完全可以不干活或者少干活，所以需要按矿工的贡献大小进行分配，所以这里也需要工作量证明，来证明每个矿工所做的工作。

每个矿工单打独斗之所以收入不稳定，是因为挖矿难度太大了（相比比特币系统的平均出块时间），所以可以考虑矿池将挖矿的难度降下来。比如本来要求前面有70个0，现在矿池只要求前面有60个0，这样挖到的是一个share（almost valid block），即这个区块差不多在一定程度上是符合难度要求的。矿工挖到这样的区块之后，将其提交给矿主，矿主拿到这些区块并没有什么用，仅仅是因为目标空间是这个问题的解空间的子集，并且求解两个问题的过程是一样的（都是计算哈希），因此这些区块可以作为证明矿工所做的工作量的证明。等到某个矿工真正挖到矿，获取出块奖励之后，再按照大家提交的share的多少来进行分配。

矿工能否在参与矿池时独吞出块奖励？

是否会有这样的矿工：挖到share提交给矿主，挖到真正的矿自己发布出去以获取出块奖励？这是没法独吞出块奖励的，因为每个矿工的任务是由矿主来分配的，矿主负责组装好区块，然后交给矿工去不断尝试nonce和CoinBase transaction中的extra nonce，有可能就是将它们划分一下，然后分配给不同的矿工去做，要注意铸币交易CoinBase transaction中的收款人地址是矿主的地址，不是任何一个矿工的地址。

如果自己把铸币交易的地址改成自己的，然后去挖矿，这样提交上去的share矿主是不认可的，所以还是没有用。

矿池之间的竞争

矿池之间是有竞争对手的，一种竞争方式就是到对方的矿池里去捣乱，即派遣一些矿工去加入到对方的矿池里去挖矿，只提交share，但挖到真正的矿就将其丢弃掉，故意不提交。然而如果这个对手矿池仍然获得了出块奖励，这些矿工也能参与分红。

大型矿池的危害

如果没有矿池，如果要发动51%攻击，攻击者要花费大量的硬件成本。有了矿池以后，矿池实际上将算力集中了起来，攻击者未必拥有很多算力，只要吸引大量的不明真相的群众将算力集中到自己的矿池就可以。

在2014年的时候GHash矿池的总算力就超过了比特币系统中总算力的一半，引起了恐慌，然后GHash主动减少了算力，以防止大家对比特币失去信心。

如今的矿池的算力还算比较分散，有好几家矿池在竞争，但一个集体的算力完全可以潜伏分散在不同矿池中，等到攻击时再集中起来，矿工要转换矿池是很容易的。

矿池要收取管理费，有的收取出块奖励中的一部分，有的收取赚取的交易费。有恶意的矿池可以在发动攻击之前故意将管理费降得很低，吸引大量矿工进入矿池。

假设出现超大型矿池，具体能发动哪些攻击？

假设有矿池占据了半数以上的算力，能够发动下面这些攻击：

**[1]分叉攻击**

因为算力占了半数以上，并且矿工挖矿任务被分配开并行进行，分叉出来的链的增长速度很快，最终势必成为最长合法链。

**[2]Boycott**

假设攻击者不喜欢某个账户A，不允许和A有关的所有交易上链。这时如果有人发布了含有和A有关的交易的区块，它可以很快发布一个不包含这些交易的区块，然后不必等候6个确认区块，立即发布到比特币网络上竞争最长合法链。

|  |
| --- |
| 这里不必等候的原因是，之前普通分叉攻击等候几个确认区块只是为了让收款人形成一种假象：认为已经没问题了，已经成功收款了。这里没有这种顾虑。 |

在之前学习共识协议时学过，大部分节点是诚实节点时，记账权也可能落在有恶意的节点手里，它完全可以不发布某些交易，但在那种情形下总有诚实的节点愿意发布这些交易，所以是没关系的。但当在这种情况下，即有恶意的节点算力很大时，却可以始终让某些交易不上链。即完全可以公开抵制某些交易，这样一来别的矿工也不敢随便打包这些交易了，因为很可能自己辛苦挖的矿最后沦为丢弃的区块。

**[3]无法进行盗币**

不论算力再强，因为没法伪造别人账户的签名（除非获得其私钥），所以没法伪造交易将别人账户上的BTC转走。即便是仗着自己算力强，强行将不合法的区块发布到区块链上并沿着这条链继续延伸，诚实的节点依然不会沿着这条不合法的长链延伸，所以还是没用的。