08 比特币挖矿

全节点：

一直在线

在本地硬盘上维护完整的区块信息

在内存里维护UTXO集合，以便快速检验交易的正确性

监听比特币网络上的交易信息，验证每个交易的合法性

决定哪些交易会被打包的区块里

监听别的矿工挖出来的区块，验证其合法性

挖矿：

决定沿着那条链挖下去

当出现等长的分叉的时候，选择哪一个分叉？（缺省的情况下，选择最先听到的）

轻节点：（SPV client，simplified payment verification）

不是一直都在线

不用保存整个区块链，只要保存每个区块的块头 （大概差一千倍）

不用保存全部交易，要保存与自己相关的交易

无法验证大多数交易的合法性，只能检验与自己相关的那些交易的合法性

无法检测网上发布的区块的正确性

可以验证挖矿的难度

只能检测哪个是最长链，不知道哪个是最长合法链（因为没有办法验证交易的合法性）

轻节点假设矿工是合理的，因为挖矿的代价是非常大，所以假设全节点不会去造假。

比特币网络中大部分的节点都是轻节点（只需要转账，不需要挖矿）。当你监听到一个新发布的区块的时候，如果这个区块是合法的，那么我应该停止当前的挖矿，然后重新组装一个候选的区块。因为区块里包含的交易信息，以及包含前一个区块的哈希指针都会发生变化。

重新开始挖，看起来很可惜，但实际上是不可惜的，因为挖矿的过程是memoryless，或者叫progress free。无论挖原来的区块，还是重新挖一个新的区块，挖到的概率都是一样的。即使挖到了合法的区块，发布了出去，也不是代表着就成功了。因为很有可能最后没有在最长合法链上。

比特币是怎么保证安全性的?

一方面是密码学上的保证。别人没有你的私钥，所以就没有办法转走你账上的钱。这个能成功的前提是系统里拥有大部分算力的矿工都是好的。如果没有这个保证的话，那么密码学上的保证就没有效果了。

比如说你去银行取钱，光自己有合法证件是不够的，银行的工作人员也得遵守规定，不能把你的钱给不是你的人。

一方面是共识协议保证的。

一开始的时候挖矿，就是用自己的电脑进行挖矿。随着难度的提升，用CPU通用计算机进行挖矿就变得无利可图，因为性价比太低了。GPU的挖矿效率比CPU提升了很多。GPU用来挖矿的话，里面很多的部件也是很浪费的，一直闲置没有用。现在比特币的难度，已经超过了GPU的算力范围，一些新开发的货币还可以用GPU进行挖矿。比特币现在用ASIC(Application Specific Integrated Circuit)芯片来进行挖矿，整个芯片没有多余的逻辑，只能用来挖矿。为了某一种加密货币设计的ASIC，不能用来挖别的加密货币。除非两种加密货币用的是同样的mining puzzle。很多新发布的货币，在一开始的时候会故意使用已有的mining puzzle从而吸引更多的人。ASIC芯片的生成周期是非常长的，比特币需要一年的时间，很漫长，但是相比于其他的芯片来说已经是非常快了。即使是在比特币的黄金时期，定制的ASIC芯片可能用不了几个月就过时了，还得买新的（军备竞赛）。一款定制的ASIC矿机，可能在使用的前两个月里能够收获整个生命周期里一半以上的利润。在比特币真正赚钱的可能是卖矿机的。给客户生产的矿机可以自己先用几个月，挖的差不多了再交付给用户。这个在比特币的系统中可以发现端倪，因为算力突然提升的时候往往就是一个大的生产厂商突然发布了一款新的矿机。

有些新的加密货币，设计的叫做alternative mining puzzle。设计这些mining puzzle的出发点就是ASIC resistance。能够抵抗ASIC，目的是让通用的计算机也可以进行挖矿。

挖矿的另外一个趋势是大型矿池的出现。单个矿工的问题就是比如说你只有一台ASIC矿机，那么可能挖一两年才能挖到，那么这就和买彩票一样了，突然中了大奖，收益会很高。当个矿工的另外一个问题就是还是要担任全节点的任务。

所以就出现了矿池。一个矿池会有一个矿主，pool manager，下面连接着很多的矿工miner。Miner只负责算哈希值，矿主负责全节点的所有功能。ASIC芯片只能计算哈希值，不能担任其他的工作。单个矿工的收益是非常少的，所以矿池可以给大家集中到一起，这样挖到了之后大家可以一起来分配这个收益。那么问题就是该如何来分配这个收益呢？矿池一般来说，会有两种组织形式。一种就是像互联网中的服务器中心，就是来源于同样的一个机构，那么就无所谓了。第二种形式就是分布式系统，矿工需要按照协议加入矿主的组织，然后有了收益之后大家一起分工。

可以平均分配么？ 明显的问题是会吃大锅饭，就是干好干坏都一个样。

因此分配收益，需要按照每个矿工的contribution进行分配，就需要工作量证明。一个矿工挖矿太难了，所以可以降低挖矿的难度，比如说以前找nonce需要保证算出来的哈希一开始有70个零，现在可以要求每个矿工找nonce需要保证算出来的哈希一开始有60个零就行。这种可能的nonce我们称之为share，就是almost valid block。矿工挖到了一个share，就提交给矿主，作为工作量的证明。将来真的有一个矿工挖到了满足70个零的，就可以按照每个矿工挖到share的比重（工作量）来进行分红。

有没有可能一个矿工挖到了一个块后，不提交给矿主，而是自己偷偷的发布出去了？挖到share的话提交给矿主，挖到真的矿就自己提交了。但这是不可能的。因为每个矿工的任务是矿主分配的，只有矿主才能组装预备的区块。而且区块里需要有收款人，就是矿主的信息，所以矿工自己是取不出来钱的。那么矿工一开始就不管矿主的任务，自己预备一个区块怎么办。这个时候矿主是不会认同这个工作量，因为里面的交易信息的根哈希值对应不上。

第二个问题就是矿工有没有可能捣乱，就是平常正常提交share，但是挖到了真正的矿之后直接扔了。这个是有可能的，但是对矿工来说并没有任何经济上的好处。如果直接扔了就谁也得不到了，好像是损人不利己。但是矿池之间是竞争关系，可以派矿工卧底到对面矿池进行捣乱。

一般来说，矿主会按照一定比例来收取管理费。一些有恶意的节点，可能收取很低的管理费来赔钱赚吆喝，吸引更多的矿工加入，然后发动恶意攻击。这是大型矿池的弊端，就是让51% attack更容易达成。

假设有某个矿池，占到了51%以上的算力， 具体能发动哪些攻击呢?

最常见的就是forking attack。可以通过算力算出来一个更长的合法链，将当前的最长合法链覆盖掉。因为矿工只负责进行计算哈希，所以并不知道比特币网络中的交易信息。不明所以的吃瓜群众，只知道干活。

还可以进行Boycott，就是封锁交易，比如说矿主不喜欢某些账户（怀疑某些账户进行非法交易），比如说不喜欢账户A。那么涉及到账户A的交易信息，只要一上链，矿主就立马进行分叉，从而不让包含账户A交易的区块在最长的合法链上。