7.btc挖矿

全节点

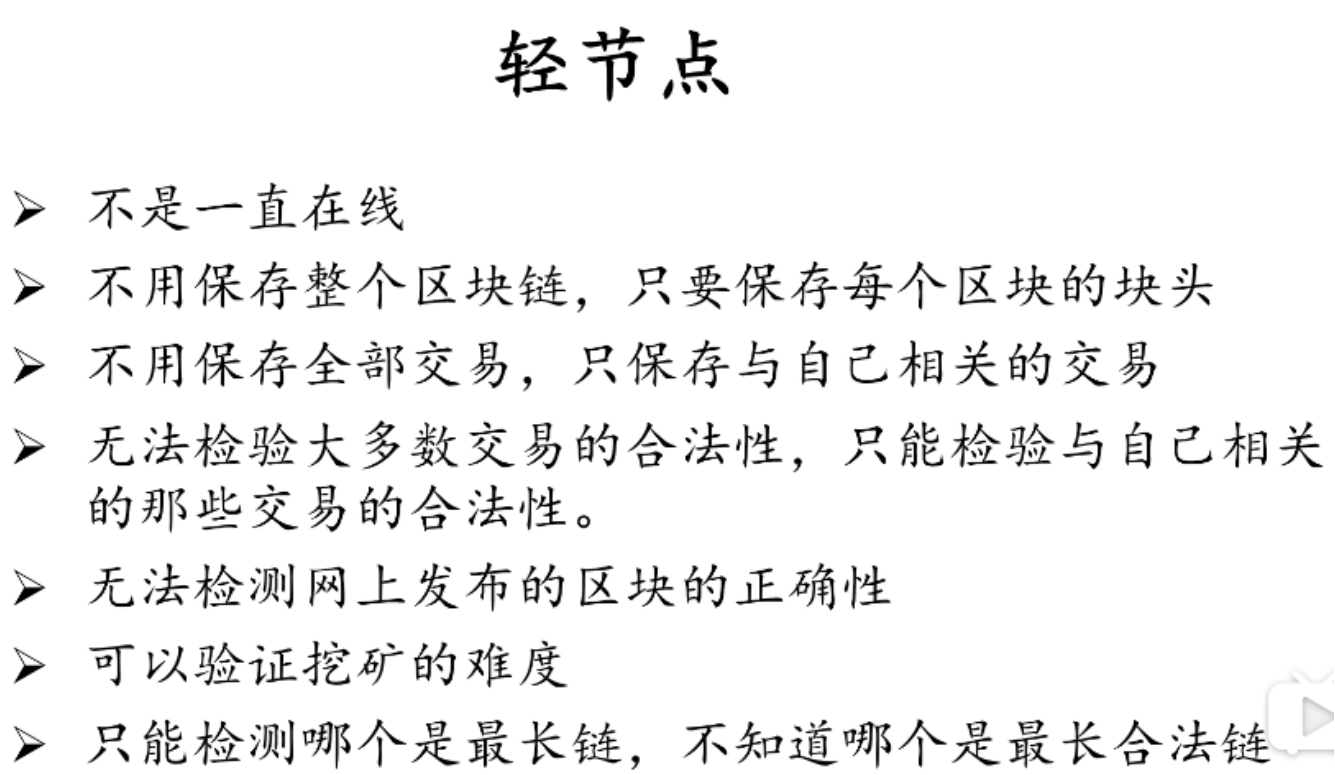
- 一直在线
- 在本地硬盘上维护完整的区块链信息
- 在内存里维护UTXO集合，以便快速检验交易的正确性
- 监听比特币网络上的交易信息，验证每个交易的合法性
- 决定哪些交易会被打包到区块里
- 监听别的矿工挖出来的区块，验证其合法性
- 挖矿
  - 决定沿着哪条链挖下去？
  - 当出现等长的分叉的时候，选择哪一个分叉？

检验交易的正确性：

1. 有无合法签名
2. 是不是double spending

监听别的矿工挖出来的区块验证3个方面：

1. coinbase reward是否正确，有没有自行提高奖励。
2. 检查blockheader里算出来的hash值是否符合target
3. target是否正确。



轻节点只保存区块头，和全节点体积差了1000倍。

btc的安全保证有两个方面：一个是密码学上的保证，一个是共识上的保证。

挖矿的设备:挖矿设备演化趋势是越来越趋于专业化，最早的时候用的是普通的CPU挖矿，像家里计算机、笔记本电脑。但如果买一台计算机专门用来挖矿是非常不划算的，计算机当中的大部分内存都是闲置的，挖矿只用到其中很小一部分内存，CPU当中的大部分部件也是闲置的，因为挖矿当中计算哈希值的操作只用到了通用CPU当中的很少一部分指令。硬盘和其他很多资源也都是闲置的，所以随着比特币挖矿难度的提高，用CPU挖矿，用通用计算机挖矿显得性价比太低。

所以挖矿转入第二代设备:GPU。GPU效率相比CPU提高了很多，主要用于大规模的并行计算。但GPU用来挖矿还是有点浪费了，GPU是用于通用并行计算而设计的，用来挖矿的话有很多部件仍然是出于闲置状态，**比如说用于浮点数计算的部件**。这些部件对于深度学习来说是很重要的，但比特币的操作只用到了整数挖矿。所以GPU虽然效率提高了很多但仍然有不小的浪费。这些年GPU价格涨得很快，有些人归因于深度学习的火热，其实有很多GPU是用来挖矿的。不过有一个好消息，随着比特币挖矿难度的提升，用GPU挖矿已经划不来了，已经超过了GPU的算力范围，所以GPU现在可以更多的用于深度学习、游戏应用的服务。

有一些新开发的加密货币有的还在用GPU挖矿，而现在更多用**ASIC芯片挖矿**，这是专门为了挖矿而设计的芯片，上面没有多余的电动逻辑，整个芯片就是为了比特币挖矿、计算哈希值的操作而设计的。它的性价比是最高的，这个芯片除了挖矿什么事都干不了，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。除非这两个加密货币用同一个mining puzzle。

有些加密货币刚发行的时候，为了解决能启动问题，会故意用一个已有的加密货币的mining puzzle，比如说跟比特币一样的mining puzzle，这样可以吸引更多的人来挖矿，这种情况叫merge mining。除了这种情况，其他都是一个芯片只能为一个加密货币挖矿。ASIC芯片生产周期需要一年，但跟其他通用芯片相比，ASIC芯片研发速度已经是非常快的了。

在这么长的生产周期里面，如果比特币价格出现剧烈变化的话，前期投入的研发费用可能就打水漂了。从历史上看，比特币的价格变化是比较剧烈的。曾经发生好几次，比特币的价格在几个月之内，下跌了80%，然后又

慢慢恢复。

如果比特币价格大幅度下降的话，挖矿可能是赔本的，可能还抵不上电费。即使在比特币发展的黄金时期，价格不断上涨，这时挖矿是有利可图的。但是竞争也是越来越激烈的，定制的ASIC芯片可能用不了几个月就过时了。一款ASIC矿机刚上市的时候大部分的利润是在它上市的前两个月获得的，因为这个时候它的算力在同类产品中是最强的。再往后随着更强的矿机出现，它就可能被淘汰掉。所以购买ASIC矿机的时机很重要，现在都是要提前预定的。有些不良厂商，ASIC矿机生产出来之后，不是立即提供给消费者，而是自己先用来挖矿一段时间，赚取比特币，等到最赚钱的黄金时间即这前两个月过去之后，再把矿机发给用户。当比特币系统中算力突然有一个很大的提升，就说明某个大公司生产出了新一款的ASIC矿机。所以在挖矿热潮中真正赚钱的不一定是挖矿的用户，而可能是卖矿机的大厂商。

挖矿机的变化趋势，是从通用变得越来越专用，CPU是通用计算，GPU是通用并行计算，ASIC是专用计算。ASIC一旦过时就作废了，不像CPU和GPU还能做其他工作。很多人觉得这是不好的，是跟去中心化的理念是不相符的，也违背了比特币设计的初衷。最民主的情况是，大家都用家里的CPU计算机挖矿。后来改为GPU噪音是很大的。**而有些新的加密货币设计的是Alternative mining puzzle。而设计它的出发点是asic resistance(抗asic芯片化)，目的是让通用的计算机也能参与挖矿的过程。**

挖矿的另一个趋势是大型矿池的出现，单个矿工即使用了ASIC芯片，挖矿从平均收益上看是有利可图的，但是收入是非常不稳定的。比特币系统中平均每10分钟出一个区块，这是说比特币系统中所有的矿工做一个整体来看平均10min会产生一个区块。但如果具体到某一个矿工来说，他可能要挖很长时间，如果他用一个矿机可能要挖一两年。这样子就好像是买彩票，挖到了就是中了一个大奖。单矿工还有其他问题，他除了挖矿之外还要承担全节点的其他责任(就是这节课最开始介绍的那些)。

所以要引入矿池，所谓的矿池，就是把这些矿工组织起来，作为一个整体，矿池的架构一般是一个全节点会驱动很多矿机，一个矿池有一个矿主，叫pool manager。下面连了很多矿工，这些矿工只负责计算哈希值，全节点的其他职责都由矿主来承担。他负责监听网上的交易，把这些交易组织打包成区块，同时要看一看有没有其他的节点抢先发布区块，如果有的话看怎样进行调整.....

ASIC芯片只能负责计算哈希值，它不能干全节点的其他功能。矿池的出现还为了解决另一个问题:收入不稳定。单个矿工的收入是不稳定的，所以大家一起干，有了收益再进行分配。

那么收益该如何分配?矿池一般有两种组织形式，一种是像大型数据中心那样，有的互联网公司，有成千上万个服务器，大的矿池里面也有成千上万的矿机，这些矿机如果是属于同一个机构的话，那么收入怎么分配就不重要了。

但也有矿机是来自不同机构的，即第二种组织方式:分布式的。矿工和矿主不在同一个地方，可能分散在世界各地，那么矿工要加入一个矿池，就是按照矿池规定的通讯协议跟矿主进行联系。矿主把计算哈希值的任务分配给他，矿工计算完之后，把结果反馈给矿主，将来获得出块奖励时一起分配。

如果矿工是来自五湖四海的，不是属于同一个机构的，那么利益该怎么分配?平均分配行不行?比如每个矿工挖到一个区块，得到了出块奖励，然后平分给其他矿工，这样行吗?不行，因为会有矿工偷懒。因此要按矿工的贡献大小进行分配，也就是这里同样需要工作量证明。那该怎么证明每个矿工做了多少工作呢？

为什么矿工的收入不稳定，因为挖矿太难了，如果把挖矿的难度降低之后，挖矿就会变得稳定了。怎么降低难度呢?以前的要求是，矿工要找到一个nonce，用nonce计算block header 的哈希值，前面至少有70个0才是合法的区块。降低挖矿难度之后，比如说前面只要有60个0就行了，这样挖到的叫作一个share，这个share叫做almost valid block。矿工挖到share或almost valid block之后，把它提交给矿主。矿主拿到这个区块有什么用呢？用来证明矿工所做的工作量，而没有其他用途。矿主无法得到区块奖励以及任何好处。所以矿主就统计每个矿工提交了多少这样的share，将来等到某个矿工真正挖到了合法的区块之后，再将出块奖励按照每个矿工所做的工作量，提交的share数目进行分配。

这样做为什么是可行的?每个矿工挖到矿的概率取决于他尝试的nonce数目，尝试的nonce越多，能找到的share就越多。

有没有可能一个矿工挖到一个合法的区块之后，不把它提交给矿主，而是自己偷偷摸摸发布出去，得到出块奖励?即平时挖到的share提交，但挖到了合法区块就不提交?不可能，因为每个矿工的任务是由矿主分配的，矿主负责组装好一个区块，然后交给矿工去尝试各种nonce，而且挖矿仅仅调nonce是不够的，还需要调整coinbase parameter。所以矿主会把不同的coinbase parameter所对应的nonce值的范围交给不同的矿工去尝试。那么这个区块里包含什么?coinbase transaction里面有收款人的地址，这个地址填的是矿主的地址，即pool manager的地址，所以矿工挖到区块之后，如果他不提交给矿主自己发不出去是没有用的。里面的收款地址是矿主的，他取不出钱来。所以只要是当初按矿主给分配的任务进行挖矿的，就不可能偷区块奖励。

如果他一开始就不管矿主的任务，自己组装一个区块，偷偷把收款地址改成自己地址，会怎样?那样他提交share给矿主的话，矿主是不认的，因为里面交易列表被改过了，coinbase transaction里面的内容发生了变化，算出的merkle tree 的根哈希值也是不一样的。这种情况下矿主是不会给他工作量证明的。那就相当于矿工一开始就单干，跟矿池是没关系的。

虽然不可能偷区块奖励，但会不会有人捣乱，比如平时挖到一个share，提交给矿主，作为工作量证明。等他挖到一个真正合法的区块之后，把它扔掉。这是有可能的，虽然没有经济好处，但有可能是别的矿池派来的卧底，不想让这个矿池得到区块奖励。这些矿工还是会分红，分的是别的矿工挖出来的区块奖励。

如图(第八节视频 第38分处)是矿池在各个国家的分布比例，中国矿池占世界81%，远远超过其他国家，所以按矿池比例来看的话，中国的总算力是有绝对优势的。

如图(第八节视频 第38分第24秒)如果按照单个矿池来看，在2014年，曾经有叫GHash.IO的矿池，这个矿池的算力，占到了全球算力的一半以上。在当时曾引起一些恐慌，这一个矿石的算力就已经足以发动51%的攻击了。这个事情公布之后，该矿池主动把算力占比大幅度的减少，以免动摇大家对比特币的信心。

如图(第八节视频 第38分第56秒)是2018年的各矿池的算力分布，看上去没有那么集中了，GHash.IO矿池早已停止运营。当然，挖矿集中化的程度仍然是比较大的，几个大型矿池占了相当大的比重，但没有矿池占50%以上。这样看算比较安全了，但可能只是一个表面现象。假如一个机构有一半以上的算力，他不一定要把算力集中在一个矿池里，而可以把算力分散隐藏在很多矿池里，真正需要发动攻击的时候再集中起来发动攻击。

矿工转换矿池是很容易的，加入一个矿池就是按照这个矿池的协议跟这个矿主联系，矿池把组装好的区块信息发给矿工，矿工来尝试各种nonce值就可以了。

所以这就是矿池带来的危害，如果没有矿池，想要发动51%的攻击，攻击者要投入大量的成本来购买到足够的矿机，能够达到系统中半数以上的算力。有了矿池之后，他可能只占很小一部分比例的算力，只要能够吸引到足够多的矿工，足够多的不明真相的群众加入到他的矿池里来就行了。

一般来说，矿池的矿主要收取一定比例的出块奖励作为管理费。矿主也要按照比例收取管理费，有的是按照出块奖励的比例，也有的是抽取交易费。有的一些有恶意的矿池在发动攻击之前，可能故意把管理费降得特别低，甚至是赔本赚吆喝，吸引足够多的矿工加入之后就可以发动攻击了。这是大型矿池的一个弊端，使得51%的攻击更加容易了。

假如某个矿池占到了半数以上的算力，他具体能够发动哪些攻击呢?一个最常见的就是分岔攻击。假如一个区块链，其中一个区块包含了一个大笔的交易，又等了几个确认区块之后，自认为已经安全了。然后这时就可能有人在该交易前面的区块发动分岔攻击。

看上去好像追赶的道路是很漫长的，但如果拥有51%的算力，最终还是可以成功攻击。另外，不要把51%当成绝对的门槛，有可能不到51%就可以。算力都是估计的，而且算力还在不断变化。

攻击者还能做什么坏事?还可以做boycott(封锁境域)。比如说攻击者不喜欢某个账户，怀疑某个账户参与非法交易，想把这个账户封锁掉，所有跟这个账户相关的交易都不让上链。假如A把某个交易A→B发布到区块链上，攻击者就会马上进行分岔，产生一个不包含这个交易的区块，所有跟A有关的交易也都不包含进去。

这种攻击跟分岔攻击区别是什么?他没必要等后面几个确认区块。这时候如果攻击者等待确认区块，是为了让B放心，B以为后面有六个确认区块，已经没事了，然后攻击者再发动分岔攻击。而如果目的是为了boycott的话，就没有必要等后面区块生成。A→B交易一上链马上进行分岔，越早越好，因为攻击者是希望别人沿着他的链往下挖的。

前面讲过，有些有恶意的节点故意不把某些交易写入区块里，是可以的。但没有关系，后面的区块还是会包含的。但是如果这个坏人拥有51%的算力的话，他可能仗着自己算力强，公开抵制他想抵制的交易。这样别的矿工也不敢随便把交易打包进去了。

那么攻击者有没有可能掌握51%的算力后，把别人账上的钱转走。这是不可能的。因为他没有别人账户的私钥，没有办法伪造签名。如果他仗着算力强，强行把一个没有合法签名的交易发布到区块链上，会有什么样的结果?会造成分岔。因为诚实的矿工会沿着另外一个分岔去挖，不会沿着他发布的区块往下挖。所以盗币是不可能的。

总结:矿池的出现减轻了矿工的负担，矿工只需要挖矿，计算哈希值就行了，别的事情都由矿主来完成。矿工的收入分配也更加稳定。但矿池的出现也有危害，发动51%的攻击变得容易了。他不一定自己有这么强的算力，只要动员召集这些算力就可以了。

这有点类似于云计算中的on demand computing。平时不需要维护很大的计算机群，需要用的时候可以随时召回来。而矿池的情况，是on demand mining。