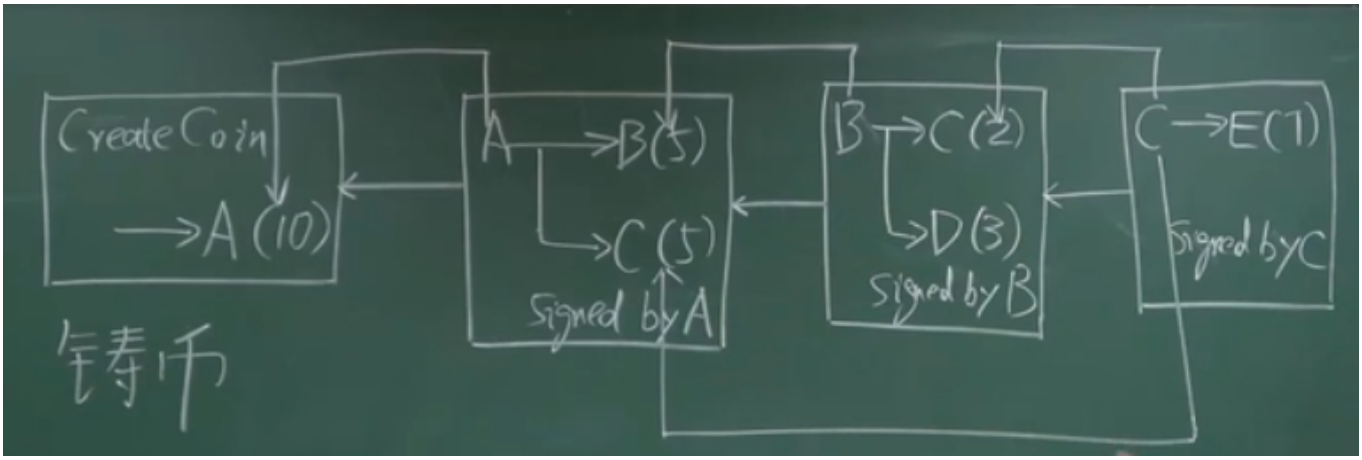
比特币的共识协议

数字货币和纸质货币区别是可以复制，叫作双花攻击 即double spending attack。 去中心化货币要解决两个问题:①数字货币的发行②怎么验证交易的有效性，防止double spending attack。

答案:①比特币的发行是由挖矿决定的 ②依靠区块链的数据结构



比特币的发行者A拥有铸币权(createcoin) 假如发行10个比特币 A(10)分别给B和C各五个 → B(5)C(5) 该交易需要有A的签名，证明经A同意。(designed by A)同时还要说明花掉的10个比特币从哪来的。 第二个方框中的钱是从第一个框内铸币交易中来的。
比特币系统中每个交易都包含输入和输出两部分。输入部分要说明币的来源，输出部分要给出收款人公钥的哈希。 有的交易部分比较复杂，如C的货币来源是第二第三个方框，要标识清楚。

图四就构成了一个小型的区块链，**这里有两种哈希指针**，一种哈希指针是连接在各个区块之间的，把它们串起来构成一个链表，前面学的就是这种哈希指针。而在该图中还有第二种哈希指针，是指向前面某个交易的指针，用来指明币的来源。为什么要说明币的来源:证明币不是凭空捏造的是有记录的，同时也是**防范double spending**。

现在来看第二个方框里A向B的转账，该交易需要A的签名和B的地址。比特币系统里收款的地址是通过公钥推算出来的。比如B的地址就是B的公钥取哈希然后经过一些转换得到的。

A如何知道B的地址?比特币系统中没有查询对方地址的功能，必须通过其他渠道。比如某个电商网站，接受比特币支付，就可以公开它的地址或公钥。

A需要知道B的地址，B需要知道A的什么信息吗?B其实也要知道 A的公钥，这代表A的身份。不仅是B，所有节点都需要知道A的公钥。而签名是用私钥签名公钥验证(注意不要跟前面知识弄混了，加密是用接收人的公钥加密私钥解密)，所以区块链上每个节点都要独立验证。

那如何才能知道A的公钥?实际上交易里就包含了。输入时不仅要输入币的来源，还要输入公钥。那就存在了安全漏洞，假如B的同伙伪造了这次交易呢?其实第一个方框里铸币交易的输出就有A的公钥的哈希，所以第二个方框交易里A的公钥要跟前面哈希对的上。

在比特币系统当中，前面这些验证过程，是通过执行脚本来实现的。每个交易的输入提一段脚本，包括给出公钥的过程，公钥也是在输入的脚本里指定的。每个交易的输出也是一段脚本，验证其的合法性，就需要把当前交易的输入脚本跟前面交易(提供币来源的交易)的输出脚本拼在一起，然后看看能不能顺利执行，如果能执行说明是合法的。比特币脚本(BitCoin Script)

该图对交易系统进行了简化，实际上每个区块(对应图中的每个方框)可以有很多交易，这些交易就组成merkle tree。每个区块分为块头和块身。

块头包含的是区块的宏观信息，比如:用的是比特币哪个版本(version)的协议，区块链当中指向前一个区块的指针(hash of previous block **header**)，整颗merkle tree 的根哈希值(merkle root hash)，还有两个域是跟挖矿相关的，一个是挖矿的难度目标预值(target)，另一个是随机数nonce。

这里的target，就是前面讲到的，整个块头的哈希要小于这个预值，即H(block header)≤target。block header里存的就是这个目标预值的编码(nBits)。这里需要注意，前一个区块的哈希只算的是前一个区块的块头，所以前面画的，一个区块引出一个箭头指向另一个区块中间，是不正确的，所以有的书中箭头是指向一个区块的上面。**取哈希时是把块头的部分取哈希。**

块身里面有交易列表(transaction list)。

前面还有一个内容讲的时候简化了:每个节点都需要验证所有的交易，实际上系统中的节点分全节点(full node)和轻节点(light node)，全节点是保存区块链所有的信息的，验证每一个交易，所以全节点又叫fully validating node。轻节点只保存block header的信息，一般来说轻节点没法独立验证交易的合法性。

比如一个交易是不是double spending，轻节点没有存以前的交易信息所以它没法验证。系统中大多数节点是轻节点，这节课内容主要针对全节点，因为轻节点没有参与区块链的构造和维护，只是利用了区块链的一些信息做一些查询。

区块链里的内容是如何写到区块链里面的呢:每个节点，每个账户都可以发布交易，交易是广播给所有节点的。有些交易是合法的，有些是非法的。谁来决定哪些交易应该被写入下一个区块中呢?按照什么顺序写呢?如果每个节点自己决定可以吗?如果每个人在本地维护一个区块链，那区块链的统一性得不到保证，而账本的内容是要取得分布式的共识(distributed consensus)。

分布式共识

分布式的共识一个简单的例子就是分布式的哈希表(distributed hash table)，比如系统里有很多台机器，共同维护一个全局的哈希表。

这里需要取得共识的内容是什么？哈希表中包含了哪些键值对key valve pair。假如有人在自己电脑上插入一个键值对，'xiao'这个pair对应的是12345，即'xiao'→12345。那么别人在另一台读的时候也要能把这个读出来，这就叫一个全局的哈希表。

关于分布式系统有很多不可能结论(impossibility result)，其中最著名的是FLP。这三个字母是三个专家的名字缩写，他们的结论是:在一个异步的(asynchronous)系统里，(网络传输迟延没有上限就叫异步系统)，即使只有一个成员是有问题的(faulty)，也不可能取得共识。

还有一个著名结论:CAP Theorem。(CAP是指分布式系统的三个我们想要的性质，Consistency【系统状态的一致性】 Availability【别人都可以用】 Partition tolerance)。该理论内容是:任何一个分布式系统，比如分布式哈希表，这三个性质中，最多只能满足两个，假如想要前两个性质，那么就不会得到第三个性质。

分布式共识一个著名的协议是Paxos，该协议能够保证一致性，即第一个性质。如果该协议打成了共识，那么这个共识一定是一致的，即每个成员所认为的共识都是相同的。但是，某些情况下，该协议可能永远无法达成共识，这种可能性比较小但是客观存在的。

比特币中的共识协议(consensus in BitCoin):

比特币中共识要解决的一个问题是，有些节点可能是有恶意的。我们假设系统中大多数节点是好的，那么该如何取得共识协议?

第一种方案是投票，首先应该确定哪些区块有投票权，有些membership是有严格要求的，这种情况下基于投票的方案是可行的。但比特币系统创建账户是很容易的，甚至一个人产生了公私钥对别人都无法得知，只有转账时别人才知道。所以有些人可以不停的创建账户，当超过账户总数的一半时就有了控制权，这种称为女巫攻击(sybil attack)。因此投票方法不可取。

比特币账户巧妙的解决了这个问题，不是按照账户数目投票，而是按照计算力来投票。每个节点都可以在本地组装出一个候选区块，把它认为合法的交易放在里面，然后开始尝试各种nonce值(***占4 byte***)，看哪一个能满足不等式H(block header)≤target的要求。如果某个节点找到了符合要求的nonce，它就获得了记账权。

所谓的记账权，就是往比特币账本里写入下一个区块的权利。只有找到这个nonce，获得记账权的节点才有权利发布下一个区块。其他节点收到这个区块之后，要验证这个区块的合法性。

比如括号里block header的内容填的对不对；block header里面有一个域，叫nBits域，实际上它是目标预值的一个编码检查一下nBits域设置的是不是符合比特币协议中规定的难度要求；该不等式是否成立。假设都符合要求，然后检查block body 里面的交易列表，验证一下每个交易都是合法的:①要有合法的签名②以前没有被花过。如果有一项不符合要求，这个区块就是不能被接受的。如果所有条件都符合，也不一定接受。

假如生成了一个新区块，怎么知道新区块插在了哪里呢?根据生成区块的指针。有可能就存在一个问题，如图5(第四个视频第65分钟) ，这两个交易指A转账给B，以及A转账给自己。这种情况不是double spending，判断一个交易是不是double spending ，是看这个区块所在的分支上币又没有被花掉。如图，一直到第三个区块，币都没有花过，所以这个交易是合法的。虽然该交易是合法的，但是它不在最长合法链(longest valid chain)上。这种称为分叉攻击(forking attack)。所以接收的区块应该是扩展最长合法链。

区块链在正常情况下也可能出现分岔:两个节点同时获得记账权。每个节点在本地自己组装一个它认为合适的区块，然后去试各种nonce，如果两个节点在差不多同一个时间找到了符合要求的nonce，就都可以把区块发布，这时会出现两个等长的分岔。这两条都是最长合法链，那该接受那条呢?比特币协议当中，在缺省(默认的意思)情况下，每个节点是接受它最早收到的那个。所以不同节点根据在网络上的位置不同，有的节点先听到新生成的其中一个区块，那就接受这个区块；有些节点先听到另一个区块，那就接受另一个区块。

如何判断接收了一个区块?比特币协议中用到了implicit consign，如果沿着这个区块往下继续扩展，就算认可了这个发布的区块。比如在新生成的其中一个区块后面又拓展一个区块，表明就认可了这个新区块。

等长的临时性的分岔会维持一段时间，直到一个分岔胜出。也就是哪一个链抢先一步生成了新的区块，哪一条就是最长合法链。另一个作废的就叫orphan block。这两个新区块有可能会各自拉拢，两个区块链看谁的算力强，有时候也是看谁的运气好，就会胜出。

竞争记账权的好处:首先获得记账权的节点本身有一定的权力，可以决定哪些交易写到下一个区块里。但这些不应该被设定为竞争记账权的动力，所以巧妙地建立了一个机制:区块奖励(block reward)。

比特币协议中规定获得记账权的节点在发布的区块里可以有一个特殊的交易:铸币交易。在这个交易里可以发布一定数量的比特币。

货币的发行

这里要回到前面的问题①，谁来决定货币的发行?coinbase transaction币基交易是比特币系统中发行新的比特币的唯一方法，后面的交易都是比特币的转移。这个交易不用指出币的来源。

那么能造多少币呢?开始时比特币刚上线的时候，每一个发布的区块可以产生50BTC(BTC就是比特币的符号)。协议中规定，21万个区块以后，初块奖励就要减半，就变成了25BTC。再过21万个区块，又要减半。

因此当一个区块胜出后，另一个作废的区块得到的比特币是没有作用的，其他诚实的区块是不会承认的。

比特币系统中要取得什么共识?去中心化的账本要取得共识。谁又能决定账本的内容呢?只有获得记账权的节点才能写东西。怎么获得记账权呢?就是解pow(挖矿)。按照算力记票，算力可以用每秒能试多少nonce数值表示。那怎样防范女巫攻击呢?按算力记票，即使创建再多的账户，也无法使算力增强。

比特币争夺记账权的过程叫作挖矿(mining)，比特币被称为数字黄金(digital gold)，争夺记账权的节点被称为矿工(miner)。