04 比特币的协议

先考虑中心化管理的情况（拥有类似于央行这种大家都信任的中心机构）

我们最先考虑的想法就是，央行发行一张100元的数字货币，然后用央行的私钥进行签名，大家可以通过央行的公钥来验证真伪。

但是这样的设计只利用的非对称加密的公私钥对，并没有使用区块链的技术。所以问题在于，虽然我没有办法修改数字货币的面值（因为已经被央行签名），但是我可以复制多份出来，可以把一张100元复制成好多100元。从而在购买东西的时候，一张货币可以重复多次使用。

这种攻击被称之为double spending attack。数字货币的一大重要内容，就是防止double spending attack。

另外一种方案是央行需要有一张表来记录每一张数字货币的所属权，这样进行每一笔交易的时候，不仅需要验证货币是否是央行发行的，还需要向央行进行确认这张货币的所属权是否正确。发生交易之后，货币的所属权就需要更改成对应的用户。这样的方案是可行的，但是实际操作起来的复杂性很高，并且是中心化的管理。而比特币是去中心化的设计。

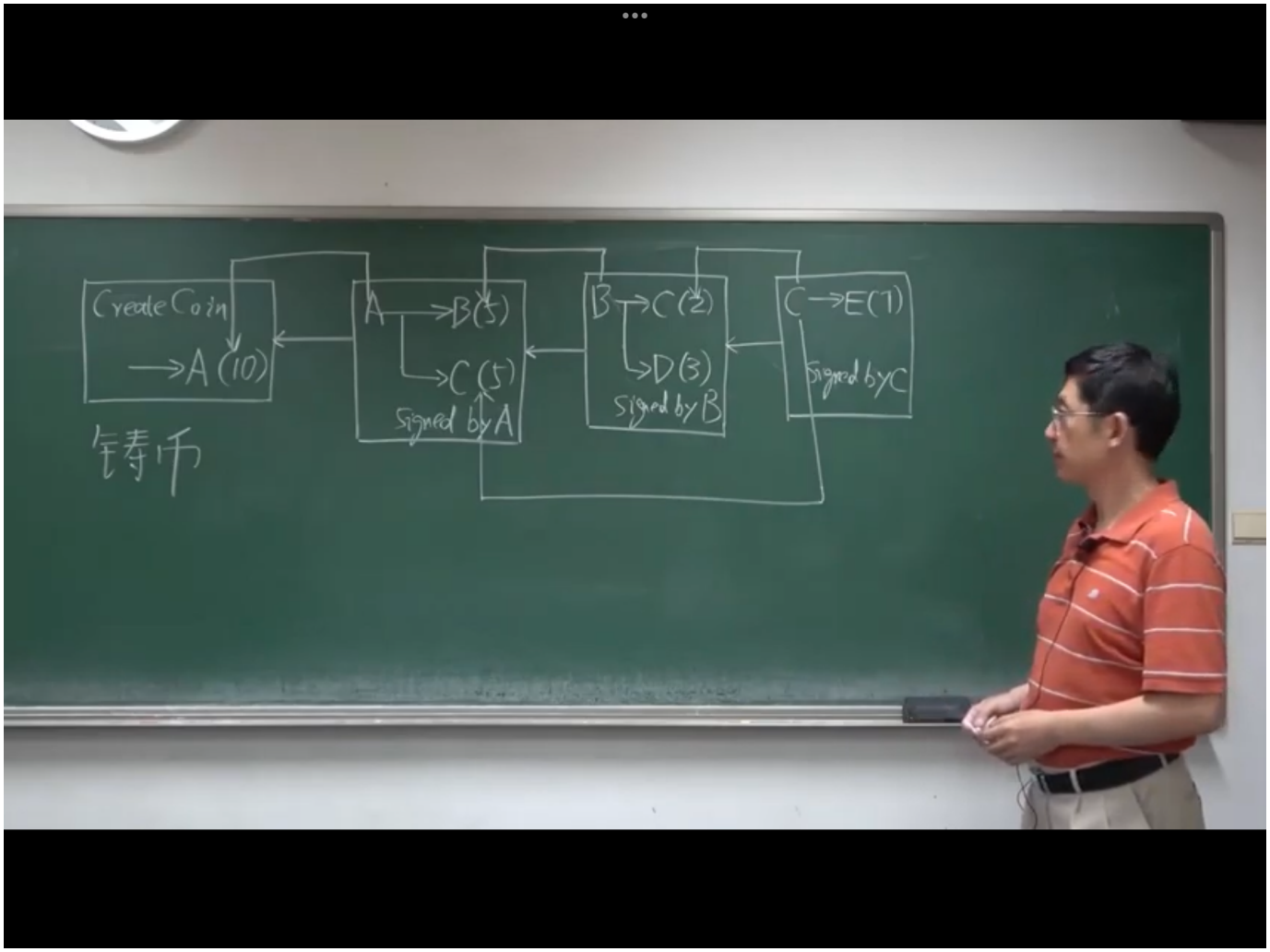
去中心化的问题：

1. 如何来确定什么时候发行货币，谁来决定什么时候发行货币

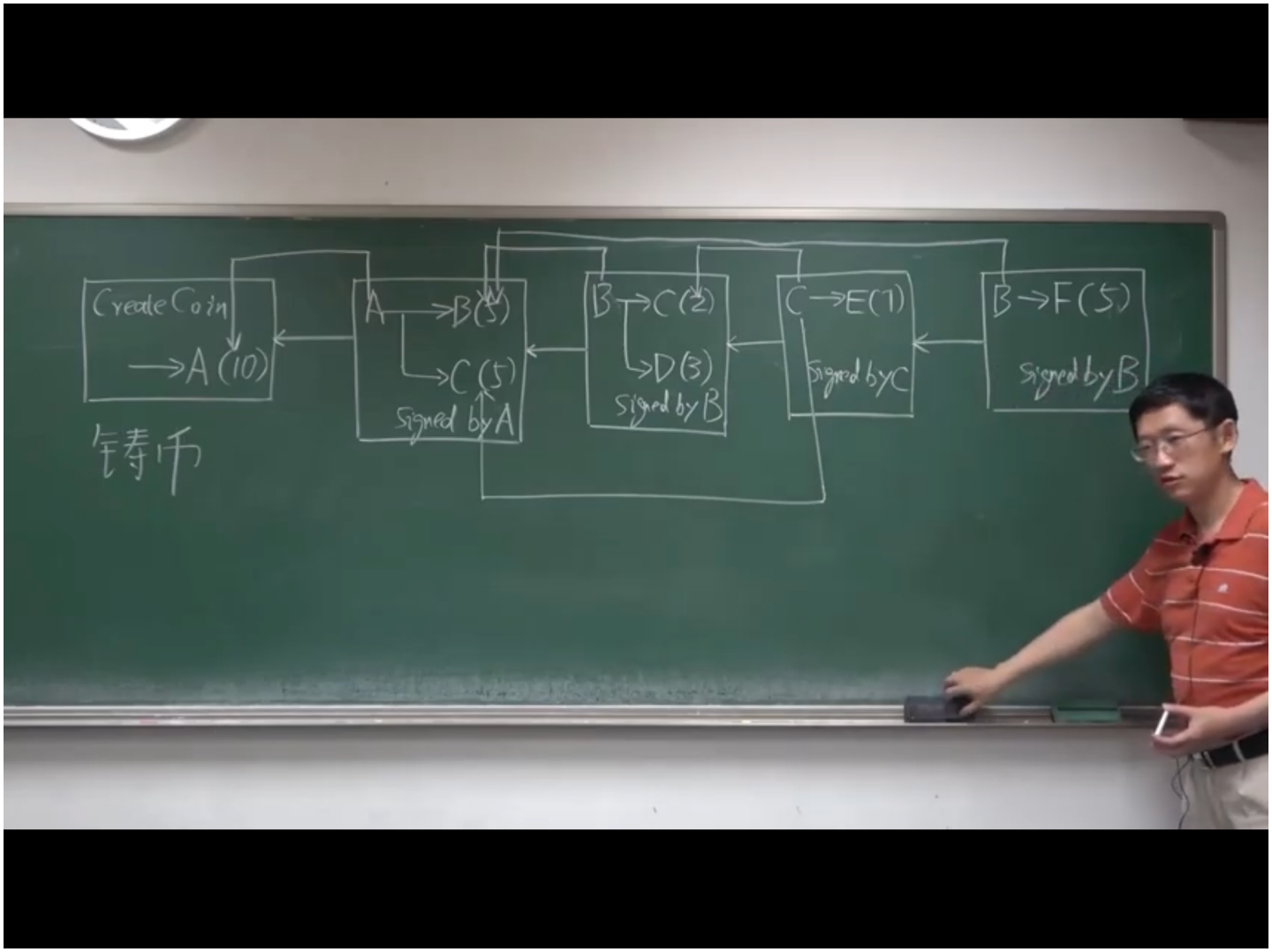
   在比特币中由挖矿来决定

2. 如何验证货币所有权的正确性

   使用区块链来记录所有交易记录



在这个区块链中存在两种哈希指针，一种是上节课中讲到的链接区块链之间的哈希指针，另外一种是用来说明币的来源的哈希指针。



当我进行double spending attack的时候，B的币来源还是之前A给的5个币，但是在向前查验交易记录的时候发现B的五个比特币已经花出去了，所以B的交易是不合法的。所以这个区块是不会被接受到区块链中的。

在A给B转账的过程中：

A需要知道B的地址（在比特币系统中是通过B的公钥经过一系列变化推算出来的）。但是和实际生活中类似，接受转款的人需要主动提供自己的银行账户（也就是比特币中的地址），银行（比特币系统）并不会提供类似的查询服务。

B需要知道A的公钥，从而验证签名是否是A的公钥。除此之外，所有的节点都需要知道A的公钥，因为每个节点之间需要独立验证，并不能依赖彼此（因为有的节点可能是有恶意的）。但问题是如何让所有节点都能知道A的公钥。为了解决这个问题，我们可以要求A在转账的过程中自己主动提供自己的公钥是什么。但是安全漏洞在于可能有B的同伙B'，用B'的公私钥对来伪造A的身份信息，从而将A的钱偷走。为了防止这样的事情发生，铸币交易（或者A的币的来源交易）中会输出A的公钥哈希，在A给B转账的交易中，A提供的公钥哈希必须和之前交易中输出的A的哈希匹配的上。如果匹配不上，说明是有人在冒充A，从而证明是非法交易。

在我们的例子中，每个区块只包含一个交易。但实际过程中，每个区块都包含很多的交易，以merkle tree的形式存储起来。

每个区块包含Block Header 和 Block Body两部分

Block Header：

包含的是一些宏观的信息（用的是比特币哪个版本的协议version，区块链中指向前一个区块的指针hash of previous block header（取哈希的时候是将整个块头取哈希，不包含body的部分），整个merkle tree的根哈希值merkle root hash，挖矿的难度目标阈值target，随机数nonce）

Block Body:

包含交易列表transaction list

我们上述的讨论中，假设所有的节点都需要验证交易的正确性。

但是实际中分为全节点和轻节点，full node(fully validating) and light node

一般来说light node没有办法独立验证交易的合法性，系统中实际上full node的数量非常少

但我们只考虑full node因为light node对于比特币系统的维护并没有帮助，只是利用了一些区块链的信息

当一个全节点验证合法的交易后需要写入交易的时候，如果每一个节点自己来决定写入的顺序，会导致每个节点的信息可能是不一致的。这个时候我们需要Distributed Consensus。

在分布式系统中，存在FLP Impossibility Result：

在一个异步系统中(asynchronous system)，假设网络的时延没有上限，那么只要有一个用户是不认同的-faulty，那么整个系统就会不认同。

CAP Theorem（分布式系统想要满足的三大性质）：

Consistency

Availability

Partition Tolerance

但是现在的分布式系统最多只能满足其中的两条。

Paxos协议有可能会有永远达不成共识，虽然可能性很小但是理论存在。

比特币中的共识协议 Consensus in BitCoin

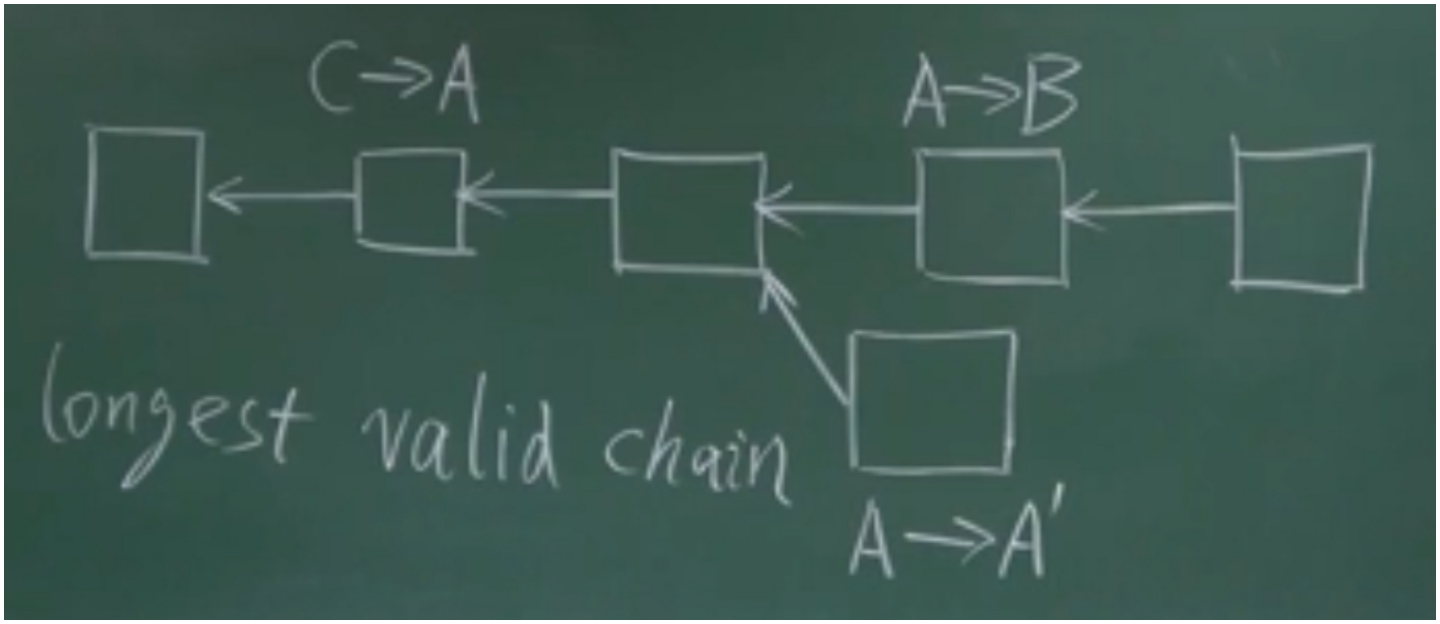
基于投票的共识协议（由一个节点提出需要写入区块的交易，其他节点验证通过就投支持票，不同意就投反对票）

但最大的问题就是membership，谁能够拥有投票权？如果大部分节点都是好的，这个方案大体上没问题（技术细节有问题）

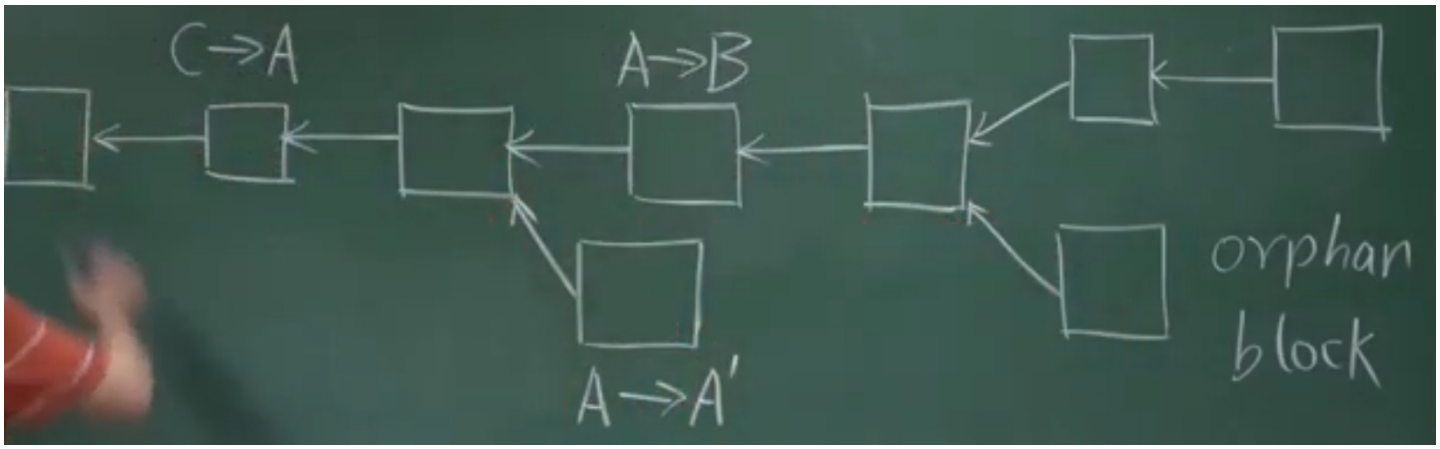
但是针对于投票机制，可以搞一个超级计算机不断生成恶意节点，保证超过总数的一半就会拥有控制权，这被称为女巫攻击Sybil Attack

比特币的机制是每个节点都可以提出需要写入的区块，但是由算力最强的节点获得记账权（通过算H(block header + nonce) <= target的速度来决定）。获得记账权的节点提出区块之后，其他的节点需要验证提出的区块中的header信息来看看是否真的获得了记账权，并且需要验证body中的交易信息是否都是合法的。别的节点可以通过新的区块的header中的hash of prev block来知道新的区块在整条区块链中插入的位置是哪里。

但问题是，在验证是否存在double spending的情况的时候，我们只会查这个区块所在的branch，不会查到别的branch上去。在下面这个图的例子中，A->B和A->A'都会被验证为合法的交易，但是这种情况应该被避免，因为我实际上是通过插入一个区块的方法来回滚了已经发生的交易。所以比特币的协议要求我们接受的区块必须是加在最长合法链上的（也就是只能加在整个区块链的最后）



但还有一种可能的情况就是，两个节点同时获得了记账权，这个时候会出现两个等长的分支。这种情况会维持一段实际时间，直到其中一个分支的算力更强找到了下一个可以写入的区块，这样的话更短的那个分支的区块就会被抛弃，被称为orphan block.



但问题是节点为什么要通过算力竞争记账权?

一个原因是可以写入合法交易，但是这不是主要目的，因为我们希望所有合法的交易都被写入。

更主要的原因是，新发布的区块中包含一个block reward，这是一个特殊交易就是coinbase transaction。这就是我们一开始提到的铸币权，这是比特币中唯一不需要指明来源就可以发布比特币的合法来源。一开始的时候区块奖励是50个比特币，每隔21万个区块后，奖励减半成25个比特币，现在已经减半到12.5个比特币。

共识协议存在意义就是保证整个区块链（账本）的内容是受到大家的认同的。