课堂问答

一、转账交易时如果接收者不在线怎么办？ 这个时候不需要接收者在线，转账交易只不过是在区块链上记录一下，把一个人账户上的比特币转移到他人的账户上，他人是否当时连接在比特币网络上是没有影响的。

二、假设某个全节点收到了一个转账交易，有没有可能转账交易中接收者的收款地址是这个节点以前从来没有听说过的? 这是可能的。比特币账户在创建的时候是不需要通知其他人的，在本地产生一个公私钥对就可以了。只有在产生收款地址以后第一次收到钱时，其他节点才知道这个账户的存在。

三、如果账户的私钥丢失了，该怎么办? 私钥丢失之后是没有办法的。该账户上的钱就变成了死钱，永远取不出来了。在去中心化的系统里，是没有人可以给你重置密码的。

另外，有些加密货币交易时，一般来说交易所是中心化的机构。在交易所开办一个账户的时候，一般是要提供身份证明的。这种情况下把比特币保存在交易所里，私钥实际上是由交易所来保管的。登录这个交易所是按照登录银行差不多的程序，即一个账户名一个密码，一般来说需要二次验证，比如Google身份验证器产生一次性密码，通过二次验证然后登录。

这种情况下如果账户密码丢失了，是可以跟交易所联系的，通过身份验证之后重置密码。有一些在线钱包也提供保管私钥的功能，但比特币或加密货币的交易所处于一种缺乏监管的状态，这个跟股票交易所是很不一样的。历史上曾发生很多次加密货币的交易所被黑客攻击的情况。最著名的是日本的Mt.Gox的事件，它曾经是全世界最大的一个比特币交易所，交易量占到了全球比特币交易量的70%，后来被黑客攻击，丢失了大量的比特币。后来交易所破产了，其CEO被判刑。各种加密货币交易所出现问题的情况发生了很多次，也有内部监管不当，管理人员卷钱跑路也时常发生。相比之下，一些冷钱包和硬钱包是比较安全的。

四、如果私钥泄露了怎么办？ 比如你发现自己账户上出现一些可疑的交易，这个时候该怎么办?这时应该尽快把自己账上的钱转到另外一个安全的账户上，这个也跟我们平时的生活体验不太一样，如果在银行账户上出现一些可疑的交易，我们首先想到的是通知银行，能否把密码重置，账户冻结，免得别人把钱取走，而这些在区块链的世界里都是做不到的。

比特币账户所谓的密码是什么？就是它的私钥。公私钥对生成之后是没有办法改的。可以生成一个新的账户，但是原来账户上的私钥是改不了的。同样，也无法阻止别人发布从这个账户上转账的交易，任何有私钥的人都可以发布一个转账交易，把账户上的钱转走，这个也是没有办法冻结的。所以我们能做的就是在第一时间抢在别人之前把自己账户上的钱转到一个安全的账户上。

五、如果转账的时候写错了地址怎么办？ 这是没有办法的。如果写错了地址而转错了人，我们也没有办法取消已经发布了的交易，比特币当中转账交易一旦发布到区块链里，就没有办法取消了。当转错了地址，如果我们知道是转给了谁，可以跟对方进行联系。如果不知道转的是谁的地址，或者是不存在的地址，那就没有办法了。

什么叫不存在的地址？地址是公钥取哈希得到的。有些地址其实不是公钥的哈希得来的，比如第一节课曾讲的digital commitment的例子。你想把某项内容的哈希值发布到区块链上，证明你曾在某个时间知道某个事情。

在前面讲比特币脚本的时候，有个经典的说法，比如把哈希值放到return的后面，因为OP_RETURN后写什么都是没有人管的。但是有人会用哈希值生成一个看上去像是比特币地址的东西。比如A→B，正常情况下B是某个比特币账户公钥取哈希之后得到的地址。在这里把他要保存的那个哈希值生成一个地址，作为收款人的地址。这个地址是没有对应的私钥的，它其实是个假的地址，比特币系统并不知道这个地址的真假，你这个哈希是怎么来的，别人也看不出来。所以这样转账的钱就变成了死钱。这个转账永远不可能被取出来。

这种做法一般牺牲一点比特币，比如转很少一点钱，换取往这个区块链里写入这个哈希值的机会。这个做法是不提倡的，因为这样的话转账交易的输出会永久的保存在UTXO里面。全节点收到这样一个转账交易，它其实并不知道你的地址的真假，它不知道你的钱其实是花不出去的，所以它必须把它永久的保存起来，这样对全节点是不友好的。

接着问一个问题:proof of burn 、OP_RETURN这些实际当中是怎么操作的? 当一个全节点收到一个转账交易的时候，它首先要检查一下，这个交易的合法性，只有合法的交易才会被写入区块链里。而OP_RETURN这个语句是无条件的返回错误，既然如此，它怎么可能通过验证，怎么可能被写到区块链里呢？

验证当前交易合法性的时候，不会执行这个语句。即当前交易的输出脚本在验证交易合法性的时候，是不会被执行的。只有有人想花这笔钱，后面再有一个交易，要花这个交易的输出的时候才会执行这个交易的输出脚本。

六、挖矿时会不会有的矿工偷答案? 不会。发布的区块里有coinbase transaction，里面有一个收款人地址，是挖到矿的矿工的地址。假如A挖到了矿，里面就是A的收款地址。如果要偷答案的话，就要把A的地址换成自己的地址，而地址如果一变化，coinbase transaction的内容就发生了改变。这样会导致什么？导致merkle tree的根哈希值变化，因为这个交易和区块中所包含的其他交易是合在一起构成了merkle tree。任何一个地方发生改变，根哈希值就会变。而nonce是在块头里面，根哈希值也是在块头里面，block header的内容发生了变化之后，原来找到的nonce就作废了。所以不可能偷答案，因为每个矿工挖到的nonce是和他自己的收款地址绑定在一起的。

七、怎么判断交易费该给哪个矿工？即事先怎么知道哪个矿工会挖到矿? 事先不需要知道哪个矿工会得到这个交易费。交易费是怎么算的?total inputs>total outputs，其差额就是交易费。发布的交易里面，一个交易可以有很多个输入，也可以有很多个输出，总输入减总输出就是交易费。给谁不需要事先知道，哪个矿工挖到矿了，就可以把这个区块里所包含的交易差额收集起来，作为他自己的交易费。

下面看一下比特币的一些统计数据: 如图(第23分第30秒)显示的是比特币区块链的大小的变化情况，可以看到区块链是越来越大的。这也不奇怪，区块链只能往里面添东西，所以区块链只会越来越长。目前的size对于硬盘的容量来说，还是完全没有问题的，区块链大部分内容还是可以保存在硬盘上的。

如图(第24分第13秒)是UTXO集合的大小变化。该集合总的趋势是不断变大的，有一些波动，主要原因就是比特币交易增多后UTXO的集合会跟着一起变大。当然还有另一些方面是历史原因造成的，有一些账户私钥丢失了，所以这些账户对应的输出在UTXO里就要永久的保存下去，时间长了也会累计增多。

如图(第25分)是比特币矿池挖矿的情况。可以看出，挖矿集中化的趋势也非常严重，几个大的矿池占了系统中很大一部分。

如图(第25分第24秒)是比特币的价格变化情况。如图(第25分第30秒)是比特币市值的变化情况，跟价格变化的图几乎是一样的。这里的市值是绝对的市值，不是说在加密货币整体中占的百分比。

如图(第25分第52秒)是比特币的交易量。可以看出最后两年交易量增加的很明显，而且波动非常大，这个交易量是按照美元价格算出的，所以这些波动当中有一些是比特币本身的价格波动造成的。

如图(第26分第24秒)是每天的交易数目。总的趋势也是在不断增长。如图(第26分第46秒)是每个区块的交易数量，趋势跟前面的图很接近，因为难度调整算法要把出块时间稳定在10分钟，这样的话每天能产生多少个区块就是差不多的。交易数目的变化主要是因为每个区块里所包含的交易数目发生了变化。每个区块最多包含交易的上限差不多是4000个，图中的情况是远远没有达到这个上限。很多人说1M太小了，但真实的区块链上很多区块是没有装满的。