比特币引发的思考

哈希指针:

指针保存的是本地内存的地址，那么只是在本地这台计算机上才有意义，发送到其他计算机上就没有意义了。那么在发布区块的时候哈希指针是怎么能够通过网络进行传输呢？

所谓的哈希指针只是一种形象的说法，实际系统中用的时候只有哈希，没有指针。回顾一下之前看到的block header的数据结构，如图(第1分第39秒)。第25行就是指向前一个区块的哈希，没有指针。block header里只有哈希值，没有指针。

那么怎么才能找到前一个区块的内容呢？全节点一般是把这些区块存储在一个(key，value)数据库里面。key是区块的哈希，value就是区块的内容。一个常用的key value数据库是level DB。所谓的区块链这种链表结构实际上是在level DB里面用哈希值算出来的。只要你掌握了最后一个区块的哈希值，那么你通过level DB的查找，哈希值key对应的value就可以把最后一个区块的内容取出来。然后这个区块块头里面，又有指向前一个区块的哈希值。那么再去查找key和value，可以找到前一个区块的内容，以此类推，一步一步往前找，最终能够把整个区块链都找出来。

所以说在实际系统当中，所谓的哈希指针，只有哈希，没有指针，或者也可以认为哈希值的本身就是指针。

有一些节点没有保存完整的区块链的信息，只保存了最近的几千个区块，如果需要用到前面的区块的信息可以问其他的全节点要。哈希指针的性质保证了整个区块链的内容是不可篡改的。

区块恋: 就是指，把一个私钥分成几份，有几个人各自保管，只有最终大家都拿出自己的部分私钥，才能合成完整的私钥。

这样存在的问题是:这些人中任何一个人把私钥丢了钱就取不出来了。还有更大一个问题:这种截断私钥的做法会降低账户的安全性。因为比特币系统中每个账户的安全性跟所用的私钥的长度是相关的。

为什么要用256位的私钥?因为这个长度的私钥用暴力破解的方法是不可行的。就算把全世界的计算机集中起来破解256位的私钥，也是不可能成功的。但是如果从中截断，一对情侣中一个人分手之后想把钱取出来，他已经知道了其中一半的私钥，只要把剩下的128位私钥猜出来就行了。私钥长度减少一半并不意味着难度降低一半，难度由2的256次方降到了2的128次方，前者远远大于后者，破解难度降了很多。如果是四个合伙人的例子，有三个人瞒着另一个人要把钱取出来，那么他们只需要尝试2的64次方就可以了。

因此对于多个人的共享账户，不要用截断私钥的方法，而最好采用多重签名，多重签名中用到的每一个私钥都是独立产生的。而且多重签名也提供一些别的灵活性，比如可以要求N个人当中任意给出M个签名就可以了。

在区块恋例子中，如果一对情侣分手了，那么他们的比特币将永久的保存在UTXO里面，这对矿工是不友好的。矿工是不知道这笔钱永远取不出来的，所以矿工要把这笔钱永久的保存在UTXO里面，造成这个集合的膨胀。

分布式共识:

前面已经讲过，从理论上实现分布式系统的共识是不可能的，但实际当中又怎么变的可能了呢?为什么比特币系统能够绕过分布式共识中的那些不可能结论?严格来说，比特币并没有取得真正意义上的共识，因为取得的共识随时有可能被推翻，比如出现了分叉攻击。你以为已经取得了一个共识，分叉攻击后系统会回滚到前一个状态，从理论上说甚至有可能回滚到创世纪块。

按照分布式系统理论的要求，共识一旦达成之后，就不应该再改了，所以从这方面来说比特币并没有绕过分布式系统那些不可能的结论，因为它并没有达到真正意义上的共识。这说明理论和实际往往是有区别的。很多理

论上的不可能结论对于实际当中是并不适用的，因为这种不可能结论只是对某种特定的模型下是不可能的，实际当中把模型稍微改一改不可能结论就不成立了。

比特币的稀缺性:

矿工挖矿的原因是为了获得收益，挖矿的收益要大于开销才是有利可图的。要吸引别人来挖矿，要么增加挖矿的收益，要么降低挖矿开销。任何一个新发行的加密货币，都有一个能启动的问题。早期为了吸引矿工来挖矿，可以给矿工更多的收益。比特币的做法是:①早期难度设置的比较低。②早期的出块奖励比较高。

实际上，比特币这种总量恒定的性质是不适合用来做货币的。后面讲的以太坊就没有出块奖励定期减半的做法，一些新型的货币甚至要自带通胀的功能，每年要把货币的通行量提高一定的比例。因为稀缺的东西是不适合用来做货币的，通货膨胀会导致钱变得更不值钱了，但一个好的货币是要有通货膨胀的功能的。

量子计算:

随着量子计算的发展，量子计算机计算力变得越来越强大，加密货币会不会变得不安全了? 这种担心是没必要的:①量子计算技术离实用还有很长一段距离，在比特币的有生之年不一定能产生实质性的联系。如果量子计算在将来能强大到破坏加密体系的话，首先会冲击的是传统金融业。比如我们在网上进行的很多金融活动:网上银行、网上转账、网上支付，都会变得不安全了。所以与其担心量子计算对比特币的冲击，还不如担心量子计算对传统金融业的冲击，因为大多数的钱还是放在传统金融业里面的，加密货币的市值只占了现代金融体系当中的很小一部分。

②比特币当中没有把账户的公钥直接暴露出来，而是用公钥取哈希之后得到一个地址。比特币当中用的非对称加密体系，从私钥是可以推导出公钥的。所以只要把私钥保管好，公钥其实丢了也没有关系。从公钥显然是不能推出私钥的，否则就麻烦了。

假设将来量子计算技术发达了，能够从公钥中推出私钥，那怎么办呢？比特币在设计的时候又加了一层保护，没有用公钥本身，而是用公钥的哈希。所以如果有人想偷你账户上的钱的话，首先是要用地址推导出你的公钥，相当于把公钥的哈希值进行逆运算，而这一点即使是用量子计算机也是没有办法完成的。

加密和取哈希是两个不同性质的操作，加密的目的是为了将来能够解密，所以加密算法要保证信息的完整性，加密过程是不能丢失信息的，这样解密的时候才能够还原原来的输入。但是取哈希的过程一般是会造成信息的损失的，哈希函数一般都是不可逆的，因为有些信息在取哈希的过程中就已经丢失了。

比特币系统中用的哈希算法是SHA-256，算出的哈希值是256位，无论输入有多大，即使有几个T，算出来的哈希值也是256位。这样的运算过程显然是不可逆的。如果可逆那可就变成了一个超级压缩算法。

所以在比特币系统中，如果要收款就没必要把公钥暴露出来，只暴露公钥的哈希生成的地址就行了。将来要取钱的时候才需要公钥和私钥产生的签名。假如一个坏人在网上监听到了你取钱的交易，知道了你的公钥，他要偷你的钱，就必须实时的从公钥推导出私钥来，然后要产生一个跟你竞争的交易。你要把钱转你账户，他要把你钱转给他账户，即使这个坏人拥有量子计算机也很难几分钟内把你的私钥破解了，而且他发布的交易要抢在你交易的前面。

所以安全起见，一个地址用过之后就不要再用了，每次取钱最好把钱一次取走，即使取不完，也最好把钱转给另一个安全的账户。后面会讲到，以太坊中的地址也是从公钥当中推导出来的，但也不是公钥本身，也是公钥取哈希之后进行的转换。