13 比特币思考

比特币的设计当中，很多地方都用到了哈希指针。那么指针保存的是本地的地址，那么区块传输到网络当中，怎么能够生效呢？指针当中的地址只在本地有意义，那么区块链中的哈希指针是怎么进行传播的?

其实哈希指针只是一种形象的说法，其实只有存储的哈希值，没有指针。那么怎么才能找到上一个区块的内容呢？全节点一般是将整个区块链的内容存在一个key，value的数据库里。一个常用的key value数据库就是level DB。其实的链表结构，是在level DB里用哈希值攒起来的。所在实际的系统当中，只有哈希没有指针。

有一些节点没有保存所有的区块信息，只保存了最近的几千个区块，需要用的时候可以管全节点要。哈希指针的性质保证了整条链的内容是不可以被篡改的。

区块恋？据说七夕的时候，两个人一起买比特币，私钥一人保存一半。将来两个人继续好下去，钱就可以取出来，要不然就会永久封存。这样做有什么问题么？ 只要有一个人的私钥丢失了就完全没法用了。除此之外，还会降低账户安全性，因为账户的安全性和私钥的长度相关。比特币账户的私钥是256位，比如说俩人分手了，其中一个人想要取出来钱，只需要暴力尝试剩下的128位就可以了，使得暴力破解需要尝试的可能性大幅度减少。

所以多人合作应该用多重签名，而不是把私钥拆分。而且这两个人分手了，这个币花不了就会永久的保存在UTXO里面，这对矿工很不友好。UTXO中的死钱是我们想避免的。

分布式共识。关于分布式共识，有很多不可能结论。从理论上证明分布式系统中取得共识是不可能的。既然理论上不可能，为什么实际上比特币系统可以达成共识？严格地说，比特币并没有取得真正意义上的共识。比如说出现了分叉攻击，就可以回滚到前一个交易。甚至理论上可以回滚到创世纪块。按照分布式理论，一旦达成共识就不应该改了。所以比特币系统没有达到真正意义上的共识。还有就是理论和实际往往是有差距的。很多不可能结论对于实际其实是不适用的。一旦模型修改，理论可能就不存在了。

比特币的稀缺性。比特币系统中的矿工，为什么要挖矿？因为为了获得收益，收益必须比开销大，才有利可图。一个加密货币启动的时候比较难，因为货币不流通，收益可能比开销少。总量固定的东西，是不适合用来作为货币的。（比如说比特币）。以太坊就是没有上限的。稀缺的东西是不适合用来做货币的。我们总是觉得通膨是坏事，因为会让钱不值钱了。但是一个好的货币必须具备通货膨胀的能力。那黄金呢？黄金在古代是用来作为货币，但是现代社会不再用黄金作为货币了。严格来说黄金的总量不是定死的，每年都会有新的金矿发现。但是每年能挖出来的黄金远远赶不上社会创造的财富。会导致黄金变得越来越值钱，因为更多的社会财富会积累到。就像中国的房地产，买房的人就会越来越不努力，没买房的人就会买不起房。个人劳动变得不值钱，积极的社会是不应该这样的。

量子计算距离实用还有很长的距离。在比特币的有生之年，量子计算对于比特币还没有威胁。如果有一天量子计算真的可以破解现有的所有加密体系，首先冲击的还是传统的金融业。比如说网上银行，网上转账，网上支付。所以还不如担心量子计算对金融业的冲击。将来还会有量子加密算法。比特币系统中并没有把公钥直接公布，而是取哈希之后。即使将来可以通过量子计算从公钥推出私钥，对比特币系统来说问题也不大。因为得从哈希值推出公钥是什么，这个对于量

子计算来说也是不可能的。

取哈希和加密是不同的。加密的过程是不能丢失信息的，因为将来解密的时候还需要还原。但是取哈希的过程通常来说是不可逆的，一般来说过程中都有信息丢失，所以没有办法通过哈希值来反推回原来的内容。比如说比特币系统中使用的SHA256，可以将任何的内容算成一个256bits的哈希值。如果这个过程是可逆的，那么任何大小的东西都可以压缩成256bits而且不丢失任何信息，就变成了一个超级厉害的压缩算法。

即使将来有量子计算技术，一个坏人想要偷你的钱，首先需要在你取币的时候（收币的时候只需要提供公钥的哈希，也就是你的账户，所以很安全）监听你的交易，监听到你的公钥和签名，然后快速的通过你的公钥破解出来的你的私钥，并且发布一个和你竞争的交易，并且竞争胜利才可以偷钱。这个对于量子计算来说也几乎是不可能的。