北京大学肖臻老师《区块链技术与应用》公开课笔记

> 比特币密码学原理篇，对应肖老师视频：click here 全系列笔记请见：click here **About Me:**点击进入我的Personal Page

比特币属于加密货币，可见其中必然会涉及到密码学的知识。而比特币本身开放，其交易记录、交易金额、交易内容甚至源代码都面向全网开放，加密又使用在哪里呢？在比特币中，正是加密确保了信息的不可篡改，保证了区块链本身的优势——不可篡改。

在比特币系统中，加密主要涉及两个内容：

hash（哈希）

> 关于什么是哈希，请自行百度学习。简单理解为对某一事物的投影操作，即A——>Hash(A) 在密码学中，采用的哈希函数称为名cryptographic hash function，其两个重要性质分别为collision resistance（对哈希碰撞具有抗拒性）和hiding(隐藏性) [注：自行翻译，可能与实际有差异，请仅关注其具体含义即可]

- **哈希碰撞:** 给定x和y，且有x!=y，但给定一个哈希函数Hash(),可以得到Hash(x)=Hash(y)，则称为hash碰撞。collision resistance保证,如果有Hash(x)!=Hash(y)，必然可以得到x!=y（当然，这是理想状态。有兴趣的可以了解针对哈希碰撞出现后如何处理，如：开放定址法、公共溢出区等）。在实际应用中，哈希碰撞基本上难以避免，我们只要保证给定x，很难找到一个y，能够在x!=y的前提下，使得Hash(x)=Hash(y)就认为其是collision resistance的【目前并不存在一个hash函数可以从数学上证明具有collision resistance的性质】。
- **collision resistance用处：** 如果我们自己有一条信息x，我们希望别人知道我有x但不想让别人知道x具体是什么，就可以通过告诉其Hash(x)，由于该性质，保证了x!=y时，Hash(x)和Hash(y)是不相等的。我们只需要告诉别人Hash(x)即可，对方可以通过Hash(x)知道你确实知道x这个信息，但他无法（很难）通过Hash(x)反推出x。
- **hiding：** 我们认为，给定x和Hash(),可以很容易得到Hash(x),但没有办法在已知Hash(x)和Hash()的情况下，反推出x的具体取值，当然这也是一个理想的情况。
- **collision resistance和hiding结合实现digital commitment(数据保证)：** 在视频中，肖老师提到关于股市预测的案例，某个人对某个股票进行涨停预测，我们如何保证能够知晓其预测是否准确？最简单的是提前公布，等待实际结果出现后验证。但实际中，当提前发布预测后，可能会由于预测者本身对股市实际结果造成影响。所以，应该将提前将其写于纸上并密封，交给第三方机构保管，等到实际结果出现后开启密封与实际对比，这就是digital commitment。而第三方机构需要能够使人信服，在实际生活中，有很多场景并不存在一个这样的第三方机构，而区块链技术正为此提供了一个很好的解决方法。 我们把预测结果看作x，提前公布Hash(x)，等到预测结果发生时间来临后，公布x，如果根据x可以得到公布的Hash(x)，则说明公布的x确实为所预先预测的内容。从而，我们可以实际进行判断预测是否准确。实际使用中，为了x足够大，会对x进行“加盐”，对x拼接一个nonce，对其整体取Hash。
- **Puzzle friendly** 在比特币系统中，还需要第三个性质Puzzle friendly。该性质要求哈希值计算事先不可预测，仅仅根据输入很难预测出输出。例如：我们需要一个哈希值，存在于某一个范围内，只能通过不停运算查找出来。该性质保证了比特币系统中，只能通过“挖矿”获得比特币。也就是说，该性质保证了工作量证明(POW)机制可以运行下去【“挖矿难，但验证易”】。 在比特币系统中采用SHA-256哈希函数

签名

- 比特币中账户管理 在第三方中心化系统中，账户开通依赖于第三方。但去中心化的比特币系统中，很明显不能进行“申请账户”。在比特币系统中，申请账户是用户自己来处理的，即自己创建一个公钥-私钥对。（关于公私

钥请自行了解非对称加密体系和对称加密体系） 公钥和私钥的应用保证了“签名”的应用。当在比特币网络中进行转账时，通过“签名”可以明确是由哪个账户转出的，从而防止不良分子对其他账户比特币的盗取。 在发布交易时，通过自己私钥签名，其他人可以根据公钥进行验证，从而保证该交易由自己发起。也就是说，只有拥有私钥，才能将该账户中的比特币转走。 【注意：比特币系统中，很难通过生成大量公私钥对来获取他人私钥】