区块链原理与技术作业

密码学在比特币中的应用

第 1 次作业

姓名：郝裕玮
班级：计科 1 班
学号：18329015

问题：描述您对如何在比特币中使用密码学的理解？

答：首先我将把课上所学的比特币密码学总结为以下 5 个知识点：

（1）哈希函数：在比特币中使用的哈希函数算法为 SHA256，它的功能为可将任意长度的输入转化为 256 位的定长 0-1 字符串。同时如果想达到密码学安全，则需要（2）—（4）这 3 个附加特性。

（2）碰撞阻力：首先碰撞的定义为：可以找到两个值 x 和 y 满足 $x!=y$，但 $H(x) = H(y)$。同理，碰撞阻力的定义则为：只要 $x!=y$，则必有 $H(x)!=H(y)$。

对于 SHA256，诚然函数结果是有限的，为2^{256}。而由抽屉原理可知，只要我们的输入有$2^{256}+1$个，则必然存在两个不同输入的输出相同。但是2^{256}约为10^{80}，而宇宙中的原子个数也才10^{77}个，所以我们可以直接将这微乎其微的碰撞可能性默认为 0，这也证明了比特币交易的安全性。

（3）隐秘性：隐秘性的定义为：无法通过哈希函数的输出 y 得出输入 x，即计算过程是单向不可逆的。这里的原理就是碰撞阻力，由于输入和输出空间足够大，所以导致通过某种特殊方法寻找到两个输入 x 碰撞的可能性几乎为 0，最佳的办法只有暴力遍历来破解。所以隐秘性同样证明了比特币交易的安全性

（4）谜题友好：通过哈希函数计算出的 y 值是不可预测的，无法通过某种可行的办法来缩短寻找到输入 x 的时间。也就是说最佳的办法只有暴力遍历来寻找输入 x。这也就是比特币中“挖矿”一词的由来。

挖矿的意思就是：所有的矿工都需要不停地计算

$$H(\text{header} \,||\, \text{TXs} \,||\, \text{nonce}) \leq \text{target}$$

这个不等式，其中 header 是该区块所包含的头部信息，TXs 是账单，随机数是 nonce。结合之前提到的碰撞阻力和隐秘性，矿工的唯一办法就是除了从 0 开始暴力遍历随机数，使得其哈希值落在 target 范围内。当尝试成功时，该矿工就会获得记账权并获得奖励（得到比特币，同时记录一个区块的奖励，也是比特币发行的唯一方式）。当某记账节点率先找到解，则立刻向全网公布。其他节点验证无误后，就会在其他的新区块重新开始新一轮的计算。该方式被称为 POW，也就是挖矿的学术称呼：工作量证明（Proof of Work）。

（5）非对称加密：首先在对称加密中，通信双方使用的是相同的密钥，虽然该种方法可以保证双方在传播消息时不会被他人窃听（因为仅有双方知道该私钥，无第三者）。但是在传播消息前，如何将该私钥传递给对方呢？一旦该私钥在传播过程中被第三者窃取，则安全性立刻失效。

在此情况下，比特币交易采用了非对称加密的方式：用户本人可自行生成一组私钥-公钥，并将公钥公布到全网，后续与他人交易时，用户将消息和私钥作为输入，生成签名。而对方只需将消息，公钥，

和签名作为输入进行验证，若为 True，则证明签名和消息属实。这样就使得信息接收者可以确认消息发送方的身份信息且保证签名不可伪造。

同时结合碰撞阻力可知，在随机源良好的情况下，几乎不可能发生随机生成的私钥与某个陌生人之前生成的私钥相同，即你的所有私钥只会被你一个人拥有，而不可能被他人窃取（除非你自己没有保存好个人私钥）。