区块链原理与技术 作业1

> 姓名：TRY
>
> 专业：计算机科学与技术
>
> 学号：

一、密码学概况

在维基百科中，**密码学**是在第三方存在下的安全通信技术的研究与实践，其研究内容主要包括：公钥加密、数字签名、私钥加密、hash函数、伪随机数、安全协议（承诺）等等。其中，**哈希函数、数字签名**等都在区块链技术中有着非常重要的应用。

二、Hash Function

2.1 Introduction of hash function

Hash Function（哈希函数）是将**任意长度的消息**映射成一个**较短的定长输出消息**的函数，目的在于为文件、消息或其他的分组数据产生"数字指纹"。而在密码学中用到的hash被称为**密码散列函数**（cryptographic hash function），具有以下三个特性：**碰撞阻力**，**隐秘性**，**谜题友好。**

2.2 Collision-resistance

collision resistance是**碰撞阻力。"collision"**是指使用hash的过程中无法避免的hash冲突，即指假设有输入`x`,`y`以及hash函数`h`,当 $x \neq y$时，有 $h(x) = h(y)$。而**"collision resistance"** 是指无法找到collision。值得注意的是，"找不到碰撞不代表碰撞不存在"。可以用**"随机碰撞检测"**来检测一个密码散列函数的安全性。

利用碰撞阻力的特性，可以实现**信息摘要**（message digest）。比如，可将一个文件进行hash，并将hash值保存在本地，然后将文件上传到网盘保存；当下次从网盘下载回文件时，只需要对下载文件计算hash值，比较这两次的hash值是否一致，即可判断出文件是否被修改。

2.3 Hiding

hiding是**隐秘性。**简单的说，指hash的过程是不可逆的，即不可通过输出 $y = H(x)$推得输入 x。要实现hiding的这一特性，**要求**`x`需要取值自一个很广泛的集合（不然需通过与另一个较为分散的输入进行结合，如级联上一连串的随机数）。

hiding的应用是**承诺**（commitment）。**承诺**协议包括两个算法：**commit算法**和**verify算法。**其中，前者将信息`msg`和一个临时随机数`nonce`作为输入，输出"承诺"`com`；后者将某个`com`、`nonce`及`msg`作为输入，当利用`msg`和`nonce`进行commit结果为`com`时返回`true`，否则返回`false`。使用承诺协议，要求满足**"隐秘性"**和**"约束性"**（分别对应hiding和collision-resistance）。

2.4 Puzzle friendliness

puzzle friendliness是**谜题友好性。简单来讲**，如果有一个人想找到`y`值对应的输入，假定在输入集合中，有一部分是非常随机的，则除了简单随机遍历，将非常难以求得`y`值对应的输入。

利用puzzle friendliness这一特点，可以为**比特币**设计**谜题搜索**，来保证所有参与者的**公平性。**具体而言，对于"比特币挖矿mining"来讲，miner就是要求解一个长随机数`n`，这个`n`和区块链中的区块的块头`header`组成输入信息`x`，使`x`的hash值`h(x)`落在某个指定的范围`target`内。由于puzzle friendliness的原因，只能通过一个个**遍历**输入的方式去寻找这个`n`，而这个寻找随机数的过程正保证了参与者的公平性。

三、Digital signatures

比特币不同于银行中心化账户管理，是用户自己开账户的。用户生成**<公钥`pk`，私钥`sk`>**，并利用这两个keys来进行签名和验证。**签名**属于**非对称加密**，允许每个个体都拥有一对密钥，私钥保存在本地，公钥向全体公开。而**签名算法**把一段消息message和私钥`sk`作为输入，返回签名sig。而**验证算法**通过把一段消息、签名消息与公钥`pk`作为输入，返回验证结果。

在实践中，比特币使用的签名算法是随机的，需要良好**随机源**（保证不会产生相同的<公钥，私钥>对）；且需要通过**Hash Function**对信息进行处理，限制信息大小。在比特币中的签名，就是要证明信息是本人发送的，**发送方**每发起一笔`Tx`就对所发送的信息使用**私钥**`sk`进行加密，**接受方**使用**公钥**`pk`进行解密来验证`Tx`的合法性。在比特币中，"公钥即身份"，用户可以随时定值新的随机身份，并且一个用户可以有多个身份。