# 区块链原理与技术 第一次作业

**19335286 郑有为**

题目：阐述自己对比特币所使用的密码学的理解。

比特币是一种基于去中心化，采用点对点网络与共识主动性，开放源代码，以区块链作为底层技术的加密货币[1]。密码学的主要研究内容包括：公私钥加密、数字签名、哈希函数、伪随机数、安全协议、零知识证明、多方计算等。

比特币所使用的密码学原理有哈希和数字签名。哈希表示大量数据的唯一摘要值，可以作为数据的验证凭据，来保证数据的完整性和正确性；数字签名是信息发送者产生的一种无法伪造的数字串，他人可通过发送者的公钥来对信息来源进行验证，实现所有者确权。

哈希函数能将任意长度的消息应生成一个较短、定长字符串的函数，它的形式为：$h = H(M)$，同时，哈希函数要求有效计算——即能在合理的时间内输出。现今使用的哈希函数有：MD5（不适用于安全性认证）、SHA-2、SHA-3等。

达到密码学安全的哈希函数需要具备以下特性：碰撞阻力、隐秘性和谜题友好。

- 碰撞阻力 Collision-resistance：如果无法找到$x, y$，满足 $x! = y$ 且 $H(x) = H(y)$，则称哈希函数 $H$ 具有碰撞阻力。

  具有碰撞阻力的哈希函数可以生成信息摘要，信息摘要均有防止信息被篡改的作用，因为被非法修改后的信息无法通过信息接收者的哈希测试。

- 隐秘性 Hiding：如果输入$r$选自一个符合高阶最小熵的概率分布，通过给定的$r$与$x$连接的串的哈希值$H(r||x)$无法确定$x$的值。

  隐秘性能够保证哈希函数的计算过程是单向不可逆的，在实际应用上，考虑到输入空间不够大（容易被暴力破解），会引入一个不重数（nonce），这个不重数就处于概念中$r$的位置。

- 谜题友好 Puzzle-friendliness：对于任意$n$位输出值 $y$，$k$选自高阶最小熵分布，如果无法找到一个方法，在比 $2^n$ 小很多的时间内找到 $x$，保证 $H(k||x) = y$, 则称 $H$ 为谜题友好。

  它能够为比特币挖矿提供公平性，即所有人只能通过暴力求解。比特币挖矿，即谜题搜索，是一个给定目标集合$Y$，寻找合格的解$x, H(id||x) \in Y$的过程，所有人无法通过控制输入值$x$来获得想要的输出值 $H(x)$。

数字签名基于非对称加密体系，每个比特币用户都用一对密钥：<pk, sk>（公钥和私钥），公钥公布给所有人，而私钥私人保存。一个用户通过将私钥和消息内容生成数字签名，其余用户可以通过该用户的公钥对数字签名进行认证。在比特币交易过程中，每笔交易记录的发起方使用它的私钥对信息进行签名，其他人通过公钥验证，来验证该交易的合法性。

考虑到公钥密钥进行数字签名时加密解密的代价昂贵，往往将散列函数引入数字签名：通过散列函数生成一个报文m固定长度的数据指纹H(m)，B对报文的散列签名而不是对报文本身签名，因为H(m)比较短所以计算会快一些。

# 引用

[1] 维基百科：比特币 https://zh.wikipedia.org/wiki/%E6%AF%94%E7%89%B9%E5%B8%81