比特币是世界上第一种成功的加密货币，之前的尝试都没有像比特币这样有效解决有关货币的各种问题。

比特币本身是密码学发展的产物，利用了密码学中的很重要的“单向散列函数”以及数字签名两大技术来构建，今天我们来集中精力讲解单向散列函数的5种重要的特性，以及比特币挖矿相关的技术原理。

下面我们先讲哈希函数的特性：

单向散列函数（one-wayhash function），也就是通俗叫的哈希函数。

第一个特点：输入可以任意长度，输出是固定长度

哈希函数不用知道输入信息代表的是什么意思，也无所谓信息的长度有多长，只要输入hash函数出来的都是固定长度的比特值。比如非常有名的SHA256
哈希函数，输入任何值出来的都是256比特的0和1. 输入一本《三国演义》或者仅仅输入一个字母a，出来的都是256位比特长度的数据。

第二个特点：计算hash值的速度比较快

这一点经常被大家所忽略，似乎是习以为常的东西就不去在意，其实这一点同样重要，因为单向哈希的计算很快，才能保证加密或者验证的速度。

第三个特点，防碰撞特性（Collisionresistance）

X≠y，H（x）=H(y) 输入空间远远大于输出空间，比如256位的哈希值指的就是输出空间是2^256这么多，输入是无限可能的，输出是固定长度。

但是，目前没有找到没有好的方法去找出一个x能得到H（x）等于右边的值。

遍历所有输入的可能能去找到这个值，叫做brute-
force暴力破解吗，也就是现在矿机所谓的“哈希碰撞”这个词的来源。

哈希防碰撞用处是保证上传和下载的数据是一样的，就是改一点点出来的结果差很多。举个例子，你输入的信息是一部《红楼梦》（当然电脑识别出来就是0和1），然后你在红楼梦的第100页的第五句话把一个逗号改成句号，然后输出的hash值就完全不同了。这就是哈希函数一个非常重要的特性。

但是collision resistance目前没有数学证明这个碰撞不会发生，MD5就是最好的例子，之前是很安全的，但是后来找到了破解方法。

第四个特点：隐藏性（Hiding）或者叫做单向性（one-way）

哈希函数的计算过程是单向不可逆的。x推出H（x），但是反推没有法子（单向性），也就是说，哈希值没有泄露输入的x的信息。也就是说x的信息被隐藏了起来，这也就就是隐藏性。

输入空间要足够大，取值是均匀的，这样就很难暴力破解。

利用第三和第四个特性可以做出很有趣的应用场景。

比如预测一个事情。
现实世界中预测和结果很多时候是有微妙的关系的，比如三国时期，曹操专门去找当时的人物品鉴专家许劭，让他看看自己是什么材料，许劭评价曹操是“治世之能臣，乱世之奸雄”，这个很难说他评的准不准，或许因为这个评语，影响了曹操的心理，他就朝这个方向发展了，就成了自我验证的预言了。所以，很难判断预测是否真的准。

更简单例子是，有影响力的股评师，今天预测一下明天的股价是不是增长，那么，他如果公开表明币价，可能会影响币价。

所以如何表明他确实很准确呢？让他把股评信息写到纸上，或者存到电脑里，但是要求是第二天开盘后，不能偷偷修改内容，这样就不用担心预测影响股价了。那么现在需要做的只是一件事儿：保证他没有篡改自己已经写好的内容。

那么，可以用hash算法，预测的结果（信息）是x，对x
哈希函数一下，公布hash值
，第二天收盘再把x放出来，如果你改了昨天的数据，hash就变了。所有人都可以用hash算一下这个x和昨天公布的hash值进行对比。

实际情况下，实际的输入空间不是很大，输入不够随机，担心有人对上升下跌这样的词汇语句进行组合排列，找到这个x，为了保证安全性，会加入一个nonce随机数，公式表达如下。

H（x||nonce） nonce是一个随机数

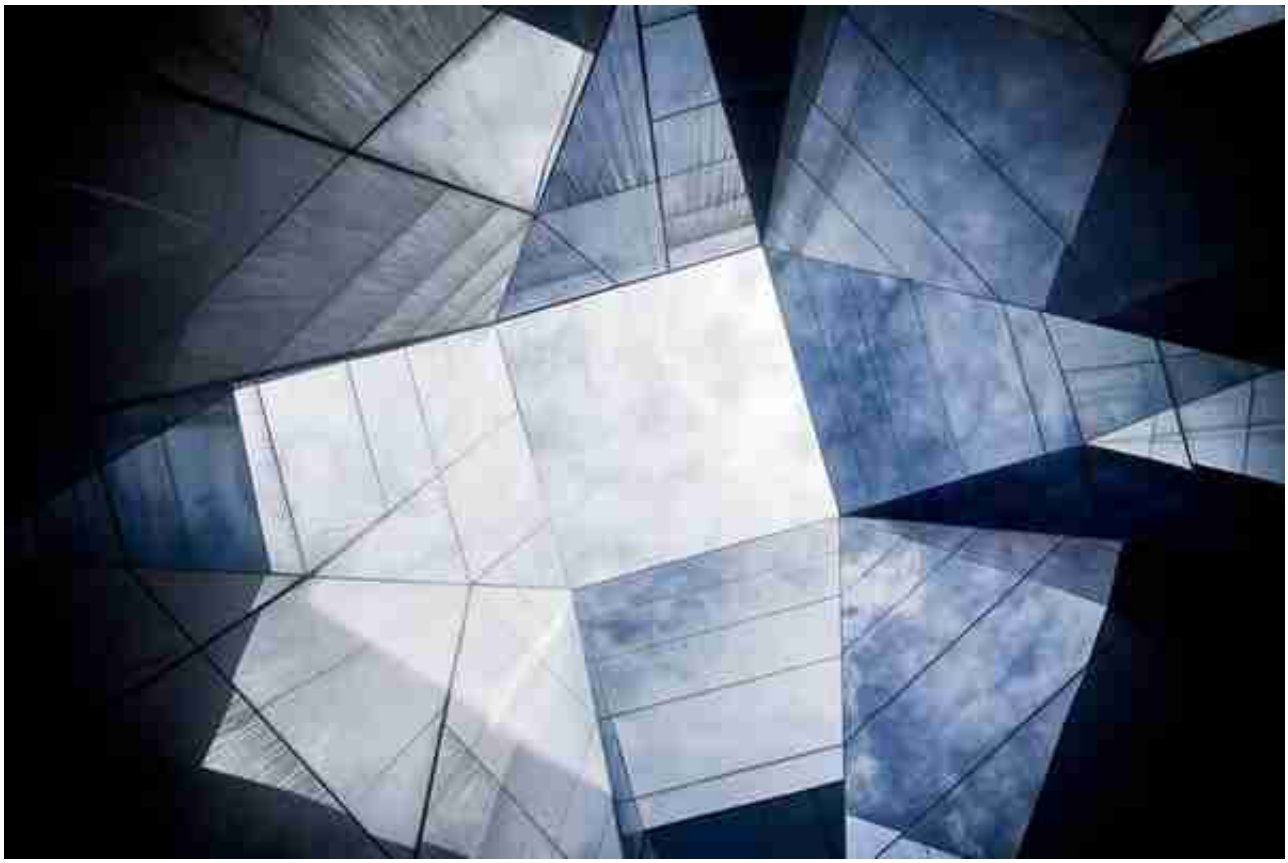
意思就是预测的结果信息x后面加个随机数，一起得到hash。

第五点：谜题友好（puzzlefriendly）

就是说看x不知道H（x）是什么？这个无法从输入数据，判断到底输出是什么样子。就是说，知道输入的信息，无法一眼看出来输出的hash值是什么，谜题友好性值得就是这一点：你无法通过控制输入值x来获得想要的输出值H（x）

所以，综合隐藏性和谜题友好性两个特点，知道输入信息也不知道哈希值是什么，可以很快算出来，但是无法预先判断；知道哈希值也不能知道输入值是什么，反向计算是非常非常困难的，只能暴力破解。

所以如果你想要输出的值落在某一个范围里，比如小于某个数值，计算机只能一个一个去试去猜答案，看哪个输入算出来的输出值正好是落在你想要的范围内。



目前世界上所谓的区块链落地应用，其实有时候用的是比特币的数据结构（默克尔树等），有时候用的是UTXO模型来结算。有的时候说是溯源，有的时候说是合约。很多的应用出来，不管是什么样的概念，多数都要用到哈希函数，利用哈希函数5种特性中的一部分。

随着文章讲解的深入，关于比特币，关于行业的信息都在展开，慢慢的大家更能明白，为什么说哈希函数是比特币和区块链行业的基础了。