拥有多年的区块链服务经验，为用户提供专业的服务信息，下面介绍哈希函数可以应用于，以及哈希函数的应用实例，选择可以为您随时随地解决玩币中所遇到的各种问题，让你不再为职称评级繁琐事务而烦恼。

哈希函数，又叫散列函数、散列算法，是一种从任何一种数据中创建小的数字“指纹”（也叫做摘要）的方法。什么意思呢？就是说，你输入任何长度、任何内容的数据，哈希函数输出固定长度、固定格式的结果，这个结果类似于你输入数据的指纹。只要输入发生变化，那么指纹一定会发生变化。不同的内容，通过哈希函数得到的指纹不一样。这就是哈希函数。

在分布式账本里，为了保证数据完整性，会采用哈希值进行校验。如，一笔交易、一页账本（也就是区块的概念），用了哈希之后生成摘要，意味着整个区块交易信息无法进行篡改（即无法在篡改数据之后保持摘要不变）。

区块链原始的定义或狭义的理解就是区块+链的形式，这个链是通过哈希链接起来，每一个区块可能都有很多交易，整个区块又可以通过哈希函数产生摘要信息，然后规定每一个区块都需要记录上一个区块的摘要信息，这样一来所有区块都可以连成一条链。

如果改了历史中某一个区块的数据，意味着这个区块摘要值（即哈希值）会改变，那么下一个区块中记录的上一个区块的哈希也得做相应的修改，以此类推，也就是说如果要修改历史记录的话，要从那一个点开始往后所有记录都要修改才能保证账本的合法性，哈希函数就提高了账本篡改的难度。

链乔教育在线旗下学硕创新区块链技术工作站是中国教育部学校规划建设发展中心开展的“智慧学习工场2020-学硕创新工作站”唯一获准的“区块链技术专业”试点工作站。专业站立足为学生提供多样化成长路径，推进专业学位研究生产学研结合培养模式改革，构建应用型、复合型人才培养体系。

Hash算法在信息安全方面的应用主要体现在以下的3个方面：

1）文件校验

我们比较熟悉的校验算法有奇偶校验和CRC校验，这2种校验并没有抗数据篡改的能力，它们一定程度上能检测并纠正数据传输中的信道误码，但却不能防止对数据的恶意破坏。

MD5 Hash算法的”数字指纹”特性，使它成为目前应用最广泛的一种文件完整性

校验和（Checksum）算法，不少Unix系统有提供计算md5 checksum的命令。

2）数字签名

Hash 算法也是现代密码体系中的一个重要组成部分。由于非对称算法的运算速度较慢，所以在数字签名协议中，单向散列函数扮演了一个重要的角色。对 Hash 值，又称”数字摘要”进行数字签名，在统计上可以认为与对文件本身进行数字签名是等效的。而且这样的协议还有其他的优点。

3）鉴权协议

如下的鉴权协议又被称作”挑战–认证模式：在传输信道是可被侦听，但不可被篡改的情况下，这是一种简单而安全的方法。

Hash，一般翻译做”散列”，也有直接音译为”哈希”的，就是把任意长度的输入（又叫做预映射， pre-image），通过散列算法，变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，也就是，散列值的空间通常远小于输入的空间，不同的输入可能会散列成相同的输出，而不可能从散列值来唯一的确定输入值。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

HASH主要用于信息安全领域中加密算法，他把一些不同长度的信息转化成杂乱的128位的编码里,叫做HASH值.
也可以说，hash就是找到一种数据内容和数据存放地址之间的映射关系

Hash算法在信息安全方面的应用主要体现在以下的3个方面：

1) 文件校验

我们比较熟悉的校验算法有奇偶校验和CRC校验，这2种校验并没有抗数据篡改的能力，它们一定程度上能检测并纠正数据传输中的信道误码，但却不能防止对数据的恶意破坏。

MD5 Hash算法的”数字指纹”特性，使它成为目前应用最广泛的一种文件完整性校验和(Checksum)算法，不少Unix系统有提供计算md5 checksum的命令。

2) 数字签名

Hash 算法也是现代密码体系中的一个重要组成部分。由于非对称算法的运算速度较慢，所以在数字签名协议中，单向散列函数扮演了一个重要的角色。 对 Hash 值

，又称”数字摘要”进行数字签名，在统计上可以认为与对文件本身进行数字签名是等效的。而且这样的协议还有其他的优点。

3) 鉴权协议

如下的鉴权协议又被称作”挑战–认证模式：在传输信道是可被侦听，但不可被篡改的情况下，这是一种简单而安全的方法。

哈希函数可以应用于是很多人头疼的问题，尤其是在理解和现实的冲突方面，哈希函数的应用实例也同样面临着相似的问题，关注我们，为您服务，是我们的荣幸！