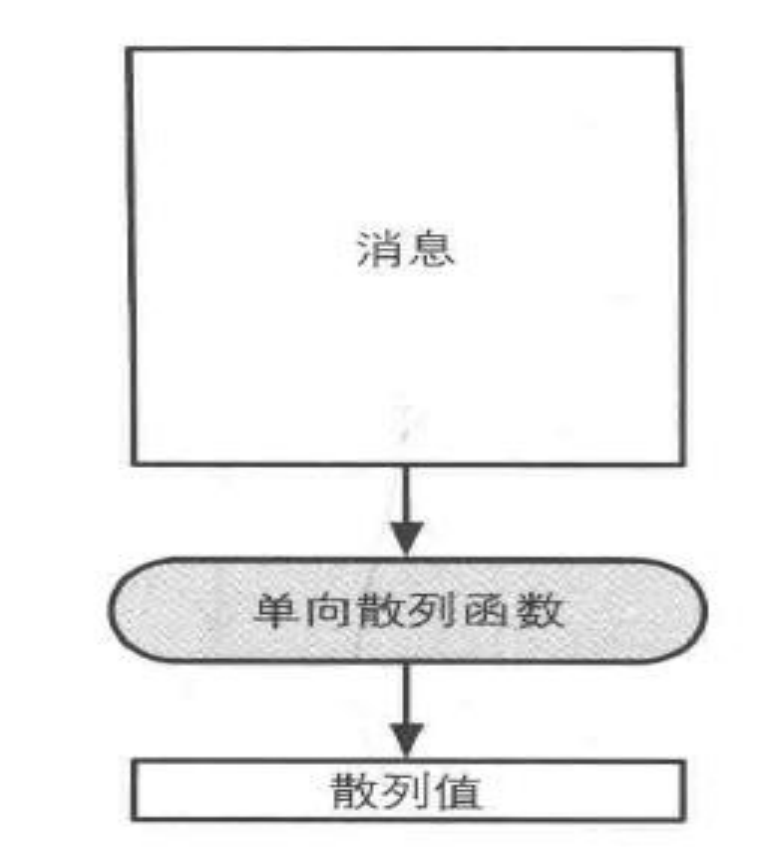
2.4 哈希运算与神奇的难以篡改

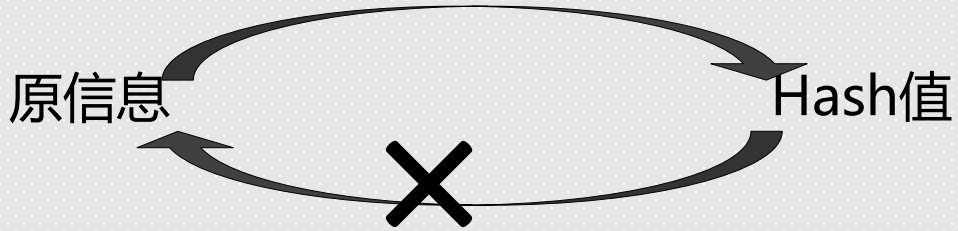
01 区块链之密码算法------哈希算法

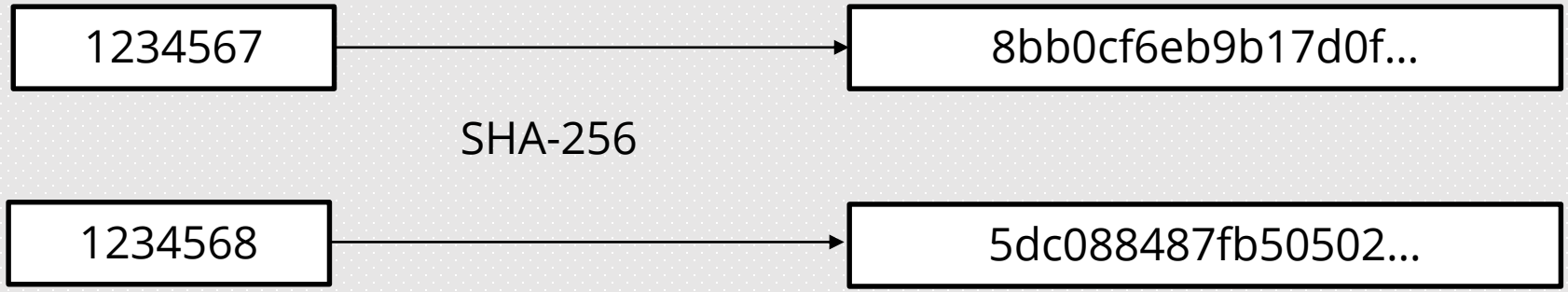
哈希加密算法，SHA256，是由美国国家安全局研发，由美国国家标准与技术研究院（NIST）在2001年发布。将任何一串数据输入到SHA256将得到一个256位的Hash值（散列值）。其特点：**相同的数据输入将得到相同的结果。**输入数据只要稍有变化（比如一个1变成了0）则将得到一个千差万别的结果，且结果无法事先预知。具体来说就是哈希算法将数据打乱混合，压缩成摘要，使得数据量变小，重新创建一个叫做哈希值的指纹。



02 哈希算法的特征

- 单向性
- 根据任意长度的消息计算出固定长度的散列
- 不同的输入就有不同的输出
- 算法效率高，计算哈希值的时间短





03 典型的Hash算法

- Hash算法中比较著名的是MD系列和SHA系列。
  - **MD系列**是在上个世纪90年代初由Mit laboratory for computer science和RSA data security inc的Rivest设计的，MD代表消息摘要（Message Digest），MD2(1989)、MD4(1990)和MD5(1991)都产生一个128位的信息摘要。
  - **SHA系列**算法是NIST根据Rivest设计的MD4和MD5开发的算法，国家安全局发布SHA作为美国政府标准，SHA（Secure Hash Algorithm）表示安全散列算法。

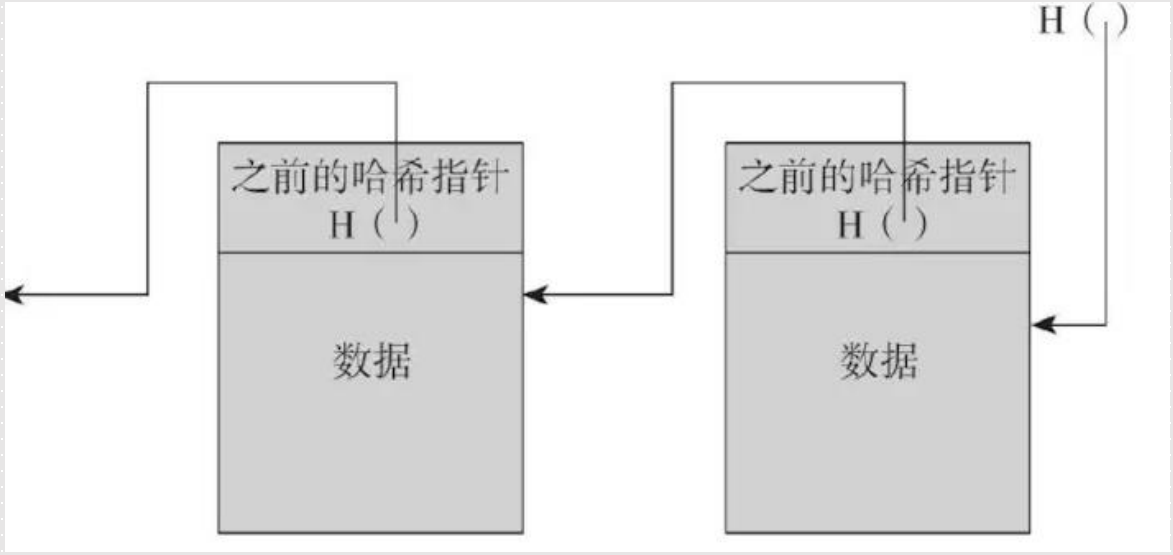
04 Hash函数的基本概念和原理

- Hash函数必须具有以下性质：
  - **H可以用于“任意”长度的消息。**“任意”是指实际存在的。
  - **H产生的Hash值是固定长度的。**这是Hash函数的基本性质。
  - **对于任意给定的消息M，容易计算H(M)值。**这是要求Hash函数的可用性。
  - **单向性（抗原像性）**：对于给定的Hash值h，要找到M使得H(M) = h在计算上是不可行的。

05 哈希运算在区块链中的使用—数据加密

- 哈希指针：不仅要保存结构体在内存中的位置还要保存结构体的哈希值

- 区块链和普通链表的主要区别就在于用哈希指针代替了普通的指针



06 哈希运算在区块链中的使用—数据加密

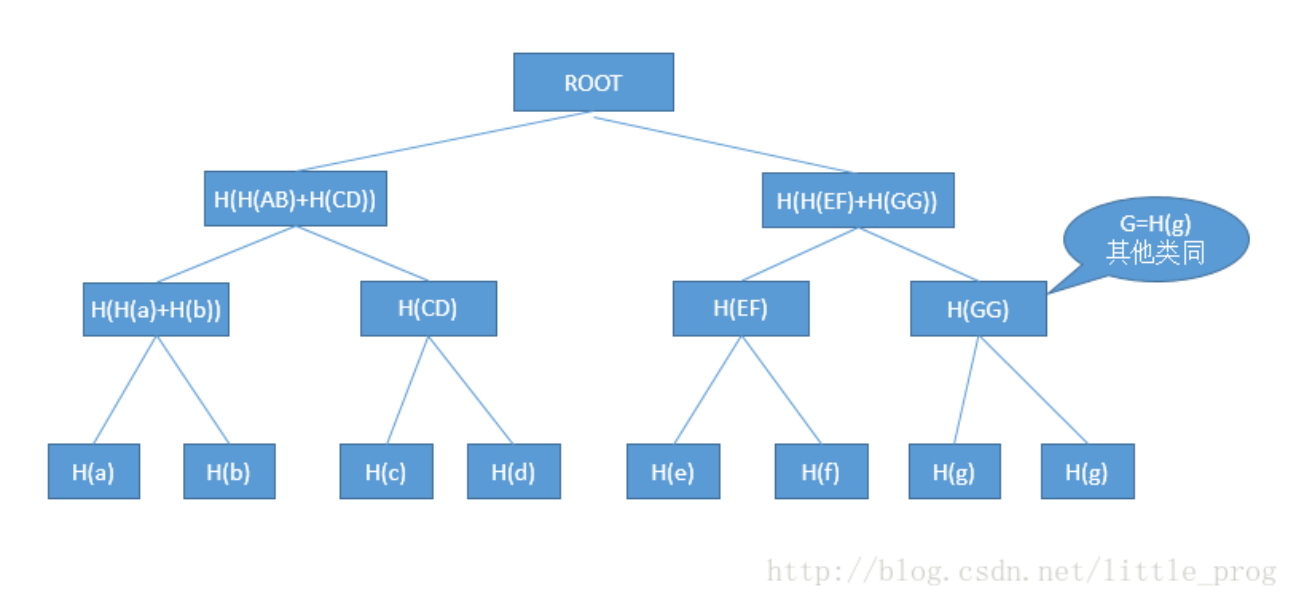
- **识别区块数据是否被篡改**：区块链的哈希值能够唯一而精准地标识一个区块
- **把各个区块串联成区块链**：每个区块都包含上一个区块的哈希值和下一个区块的值

07 哈希运算在区块链中的使用—加密交易地址

它使用的是单向哈希。哈希树的顶部为顶部哈希（top hash），亦称根哈希（root hash）或主哈希（master hash）。它是通过并联两个子哈希来往树上爬直到找到根哈希。

作用：1.快速定位每笔交易

2.核实交易数据是否被篡改



08 哈希运算在区块链中的使用—挖矿

- 挖矿：区块头中有个参数叫随机数Nonce，寻找这个随机数的过程就叫做“挖矿
- 比特币挖矿过程使用SHA256哈希函数不断运算。挖矿就是重复计算区块头的哈希值，不断修改Nonce值，直到符合目标哈希值过程。哈希函数的结果无法预知，也没有特定模式快速算出哈希值。

09 小作业

思考：假如给你一个交易的哈希值，你怎么判断这个交易的正确性和存在性呢?