Introduction

15 August 2017 01:16 PM

Hash Function :

- Input - String (Any Size)
- Output - Fixed Size (256 bits - Bitcoins)
- Efficiently computable (Real Time)

Security Properties of Hash Function :

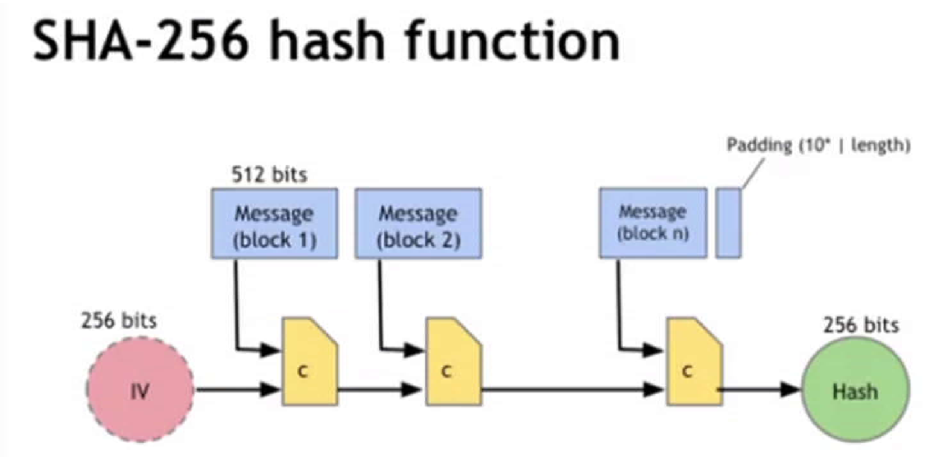
- Collision Free --> x!=y and H(x) = H(y) Collisions do exist

To find a collision -- Try 2**130 random inputs their is 99.8% probability that 2 inputs collide
(No matter what hash function is ...)
No Hash function is collision free but the people have found that it is very hard to find collision and hence proved to be collision free.

Application : 1. Message Digest (Compare Files)

- Hiding --> Given H(x) no way to figure what is x -- X has to be from a set that should be spread out (Not like Heads and Tails)
  Solution to this problem is to choose r from a probability distribution that has high min-entropy, then given H(r|x), it is infeasible to find x.
  high min-entropy --> spread out
  Security Properties :
    - Hiding : Given commitment H(key | msg) unable to find msg
    - Binding: msg!=msg such that H(key | msg) = H(key | msg)
- Puzzle Friendly: For every possible Y, if K is chosen from a distribution that has high min-entropy then it is infeasible to find x such that H(k | x) = y
  Application : Search Puzzle (Bit coin mining) No way to find solution other than searching for solution

Hash Function that BIT COIN Uses : SHA - 256



C is called compression function
IV is standard value that we look up
No collisions ever found