**Bitcoin and Crytocurrency technology**

**Chapter 1: Introduction crypto ( mã hóa ) and Cryptocurrencies ( tiền điện tử )**

* 1. Cryptographic hash function

Hash function là một hàm toán học gồm 3 thuộc tính sau:

+ input any string, any size.( dữ liệu đầu vào của hash funtion có thể là bất cứ một chuỗi nào với bất cứ một kích thước nào, không giời hạn dung lượng của dữ liệu đầu vào).

+ fixed size output.( với input là tùy ý, thì output sẽ được mặc định là một chuỗi gồm 256 bit).

+ Efficiently computable.( với input đã cho thì chúng ta có thể thấy được output của hashfunction trong một khoảng thời gian hợp lý, thời gian ở đây có thể tính bằng hàm O(n) với n là số bit của input ).

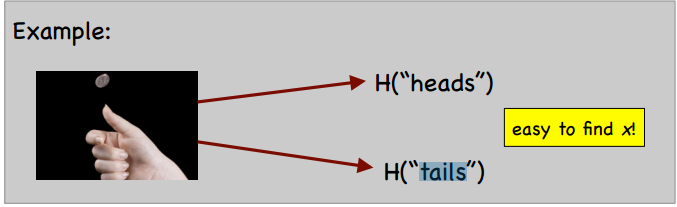
Ba thuộc tính quan trong để tạo nên một hash function bảo mật về mặt mã hóa.

+ Collision Resistance ( không đụng độ ): ở đây có nghĩa là với mỗi input x!=y thì qua hash funtion chúng ta không thể tìm thấy H(x)=H(y).

+ Hiding properties ( ẩn các giá trị của input ):

Điều mà chúng ta muốn là: cho H(x), mà không thể tìm thấy được x.

Ví dụ: Khi chúng ta tung đồng xu thì sẽ luôn có 2 trường hợp ( hình và số), tương ứng với hai trường hợp này thì sẽ có hai hash function tương ứng H( “heads”) và H(“tails”), việc để tìm input tương ứng với 2 hash function thì rất rễ bởi vì tập dữ liệu đầu vào thì không trải rộng mà chỉ có 2 giá trị là “hình” và “số”.



Hiding: để ẩn input thì chúng ta sẽ chọn secret value r ( giá trị bí mật r) từ tập phân bố xác suất có “high min-entropy” sau đó H(r||x) , từ đó tìm x là điều không thể.

* R||x: là nối chuỗi x với giá trị r
* High min-entropy: có nghĩa là phân bố rộng, do đó không có giá trị cụ thể nào được chọn với xác suất lớn.

+ Puzzle-friendliness:

**Chapter 2:**

**Chapter 3:**

**Chapter 4:**

**Chapter 5:**

**Chapter 6:**

**Chapter 7:**

**Chapter 8:**

**Chapter 9:**

**Chapter 10:**

**Chapter 11:**