**1a.2 – Função de Hash**

Hash é uma sequência de caracteres que identifica um certo documento apartir de seu conteúdo e de um algoritmo de Hash que, através dos dados do documento, gera um Hash que o identifica.

**Características da função/Algoritmo de hash**

Uma função hash é caracterizada por:

Saída de tamanho fixo: independente do valor de entrada, as saídas possuem a mesma quantidade de letras e números.

Eficiência de operação: a função não pode ser complexa ao ponto de comprometer a velocidade de processamento

Determinística: um valor de entrada sempre possuirá a mesma saída.

**Propriedades a quais uma função de Hash deve possuir**

Unidirecional: Essa propriedade diz respeito à não invertibilidade desse tipo de função. Ou seja, deve ser praticamente impossível pegar um valor de hash, aplicar uma função inversa e obter o dado de entrada.

Resistência a colisões: Pelo fato da saída (hash) ter um tamanho finito, então o número de hash’s diferentes possíveis também é finito, contudo, o número de docuentos diferentes no mundo é incontável (infinito), logo pelo princípio da casa dos pombos pode ocorrer de dois documentos diferentes terem o mesmo hash, mas é de extrema importância que probabilisticamente uma função de hash evite essas colisões.

**Principais algoritmos de hash**

Message Digest (MD): Essa função tem foco na verificação da integridade de arquivos. As versões mais comuns são: MD2, MD3, MD4 e MD5, que foi utilizada nos exemplos anteriores, lembra?

Secure Hash Function (SHA): Utilizada em transmissão de dados entre servidor e cliente

RIPEMD: É uma versão melhorada das funções MD. As saídas do RIPEMD possuem 160 bits de tamanho, enquanto as saídas MD possuem 128 bits

Whirlpool: É um algoritmo de criptografia de código livre desenvolvido por dois professores (um do Brasil e outro da Bélgica). Esse algoritmo é usado pela Organização Internacional de Padronização (ISO) e pela Comissão Eletrotécnica Internacional (IEC).

Para um aprofundamento matemático sobre algoritmos de hash:

<https://www.ime.usp.br/~pf/estruturas-de-dados/aulas/st-hash.html>

**Hash SHA256**

A função de Hash utilizada no bitcoin e utilizada fortemente no blockchain é o HASH SHA256.

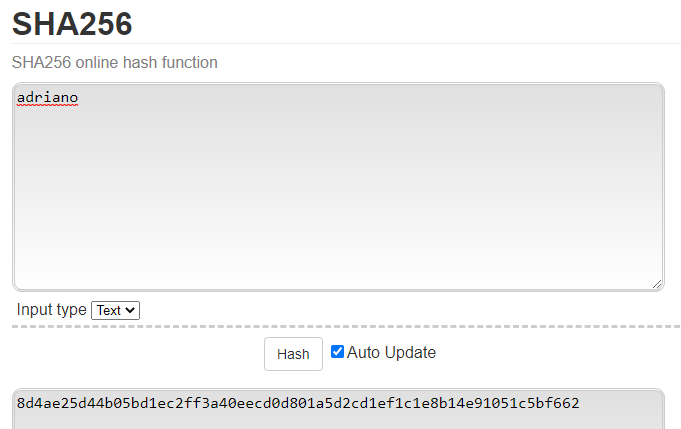
Essa função faz parte do conjunto SHA-2, criado pela NSA (National Security Agency), em português Agência de Segurança Nacional dos Estados Unidos.

E a sigla SHA significa Secure Hash Algorithm, ou em português, Algoritmo de Hash Seguro.

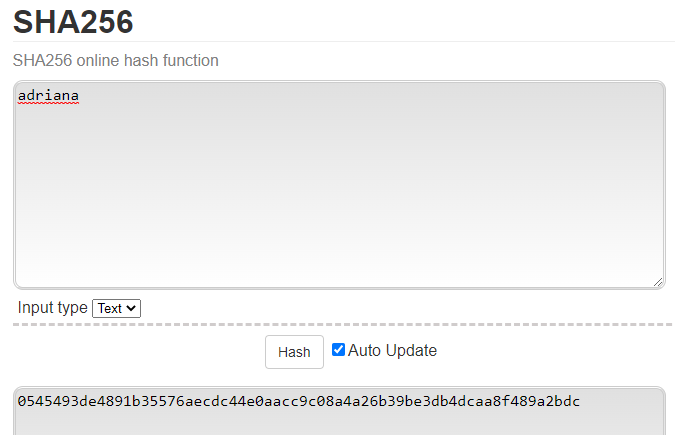
A sequência (hash) que ela gera possui 64 caracteres, sendo cada caracter um desse conjunto: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}, ou seja, a sequência é hexadecimal.

No seguinte link: <https://emn178.github.io/online-tools/sha256.html>

Podemos visualizar a saída (hash) obtida através de uma entrada de dados, no caso da função SHA256 ou de outras se desejar.



Veja se alterarmos apenas um caracter:



O Hash muda completamente, isso é uma característica desse algorítmo.

**Função de Hash no Blockchain**

Certo, já vimos o que faz uma função de Hash, e já vimos que numa cadeia Blockchain um bloco é formado por 3 campos: O conteúdo que ele armazena, o Hash do bloco anterior na cadeia, e o seu Hash.

A função Hash utiliza o conteúdo (transação) que o bloco armazena e o Hash do bloco anterior, e apartir desses dados, cria um Hash para esse bloco.

Fontes:

<https://www.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona>

<https://criptofy.com/hashing-criptomoedas/>