1

Funções de Hash

Segurança da Informação

Segurança da Informação

Funções de Hash

Definição, funcionamento e aplicações do Hash, função popular da criptografia

O assunto sobre as funções criptográficas pode ser complexo para algumas pessoas. Contudo, é fundamental que você entenda sobre o principal pilar da segurança de informação: a confidencialidade.

Qualquer falha nos servidores podem gerar problemas gravíssimos! Imagine o que poderia acontecer caso as senhas de usuários do principal portal de criptomoedas, como o Binance, fossem vazadas?

Segurança da Informação

Funções de Hash

Definição, funcionamento e aplicações do Hash, função popular da criptografia

É justamente por isso que o hash existe! Neste artigo, você vai entender como funciona o hashing, conhecer as aplicações dessa função e outros assuntos envolvendo a criptografia. Confira os tópicos a seguir:

- O que é a Função Hash?
- Como funciona o Algoritmo Hash?
- Características da Função Hash;
- Propriedades de uma Função Criptográfica;
- Principais algoritmos das Funções Hash;
- A relação entre Hash e o Blockchain;
- Aplicações da Função Hash.

Segurança da Informação

Funções de Hash

O que é a Função *Hash*?

A Função Hash é um algoritmo matemático para a criptografia, na qual ocorre uma transformação do dado (como um arquivo, senha ou informações) em um conjunto alfanumérico com comprimento fixo de caracteres.

Para você ter uma noção, o hash da palavra "voitto" utilizando a função MD5 é: **494009d6ad36e1caa1b05e7cc98ab48f**.

Segurança da Informação

Funções de Hash

Como funciona o Algoritmo *Hash*?

O algoritmo hash é conhecido como uma função matemática criptográfica, na qual você possui dados de entrada e, após passar pela criptografia, eles apresentam valores de saída "padronizados", ou seja, as saídas devem possuir o mesmo tamanho (geralmente entre 128 e 512 bits) e o mesmo número de caracteres alfanuméricos.

A função hash criptográfica é utilizada, principalmente, para resumir uma grande quantidade de informações em arquivos.

Segurança da Informação

Funções de Hash

Como funciona o Algoritmo *Hash*?

Imagine um banco de dados com muitas informações podendo ser resumido em uma única sequência de letras e números! Isso traz uma praticidade gigantesca dentro do mundo digital e da tecnologia da informação.

No início do artigo, você viu que o hash da palavra "voitto" é: **494009d6ad36e1caa1b05e7cc98ab48f**. Não parece que essa informação foi resumida, certo?

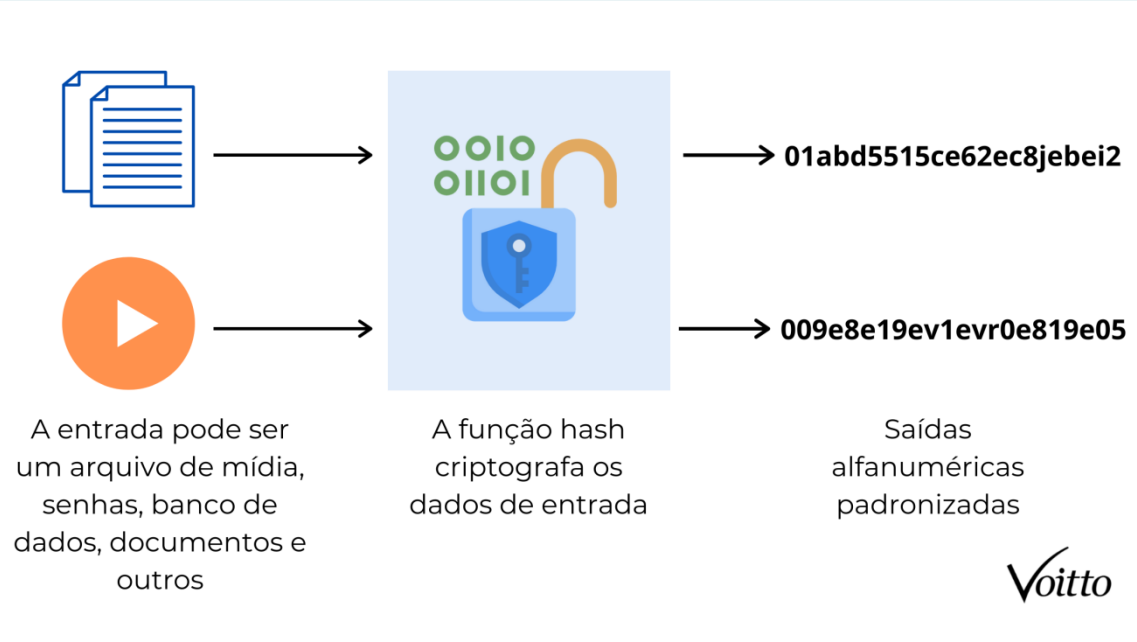
Porém, outro artigo sobre blockchain possuia aproximadamente 2000 palavras.

Segurança da Informação

Funções de Hash

Como funciona o Algoritmo *Hash*?

Usando a mesma função do exemplo anterior, o funcionamento do hash pode ser visualizado na imagem abaixo:



Segurança da Informação

Funções de Hash

Características da Função *Hash*

Saber identificar uma função hash é fundamental! Normalmente, para possuírem utilidade criptográfica, elas são caracterizadas por três pontos de distinção:

- **Saída de tamanho fixo**: independente do valor de entrada, as saídas possuem a mesma quantidade de letras e números. Lembre dos exemplos acima da palavra "voitto" e do artigo de blockchain, as saídas dos dois possuíam 32 caracteres alfanuméricos;

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

Segurança da Informação

Funções de Hash

Características da Função *Hash*

- **Determinística**: o valor de entrada (input) sempre possuirá equivalência ao valor da saída (output).

Além disso, é interessante você saber que existem vários tipos de funções hash e outros atributos da criptografia. Vamos falar sobre isso no tópico a seguir.

Segurança da Informação

Funções de Hash

Propriedades de uma Função Criptográfica

As três propriedades essenciais em uma função criptográfica, independente do tipo de função, serão detalhadas a seguir:

Segurança da Informação

Funções de Hash

Propriedades de uma Função Criptográfica

As três propriedades essenciais em uma função criptográfica, independente do tipo de função, serão detalhadas a seguir:

Segurança da Informação

Funções de Hash

Propriedades de uma Função Criptográfica

1 - 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**.

Dizemos que é praticamente impossível porque pode haver a possibilidade de se encontrar o dado de entrada, porém a probabilidade deve ser muito pequena.

Segurança da Informação

Funções de Hash

Propriedades de uma Função Criptográfica

1 - Unidirecional

Se eu lhe pedir a sequência de números cuja a divisão por 10 resulta na seguinte sequência: 1-7-2, você poderia dizer: 11-17-12 o leitor seguinte: 21-17-42 o outro leitor uma sequência diferente e no final a resposta será, na verdade: 1901-1017-22.

Percebeu que existem infinitas possibilidades de responder a esse pequeno desafio?

A mesma ideia acontece com as funções que tentam descriptografar um hash. Elas tentam achar o valor de entrada, mas se torna um trabalho muito árduo à medida que a complexidade da criptografia aumenta, o que torna a função praticamente invertível.

Segurança da Informação

Funções de Hash

Propriedades de uma Função Criptográfica

2 - Resistência à segunda pré-imagem

A resistência à segunda pré-imagem significa **que não podem existir dois valores de entrada com a mesma saída**. Mesmo em dados "semelhantes" isso não ocorre. Observe o hash dessas duas palavras:

***voitto**: 494009d6ad36e1caa1b05e7cc98ab48f.*
***Voitto**: 9c316fd682936ef2b7a7a8716e44eecf.*

Mesmo a informação sendo "igual", as saídas apresentam diferentes valores de hash.

Segurança da Informação

Funções de Hash

Propriedades de uma Função Criptográfica

3 - Resistência à colisão

Esta propriedade é basicamente uma redundância da propriedade anterior. A colisão ocorre quando duas entradas diferentes possuem o mesmo hash. Quanto mais criteriosa uma análise é feita na função para verificar se dados distintos geram uma saída igual, mais podemos afirmar que a função é resistente à colisão.

Segurança da Informação

Funções de Hash

Principais algoritmos da Função Criptográfica *Hash*

Os algoritmos mais populares e utilizados atualmente são:

- **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, já as saídas MD possuem 128 bits;

Segurança da Informação

Funções de Hash

A relação entre *Hash* e *Blockchain*

Blockchain é uma tecnologia aplicada principalmente no registro de transações envolvendo moedas digitais, como o bitcoin.

O blockchain é uma cadeia de blocos de dados criptografados. E adivinha quem é a função envolvida na criptografia desses dados? Isso mesmo, o hash!

Dentro da rede dessa cadeia de blocos, existem pessoas que fornecem capacidade computacional para que as transações financeiras sejam registradas e validadas, ou seja, verificar o nível de honestidade das informações dentro do bloco, evitando fraudes.

Segurança da Informação

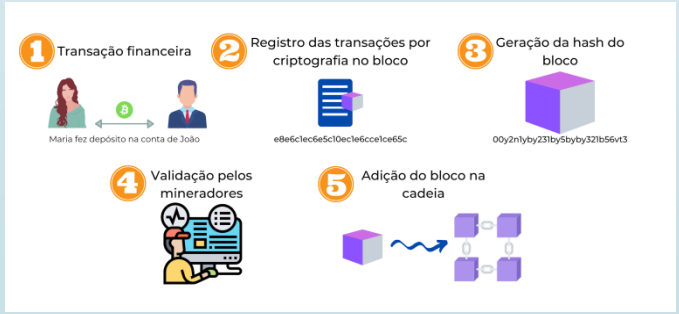
Funções de Hash

A relação entre *Hash* e *Blockchain*

Os usuários mineram a rede, registrando as transações e gerando um hash seguro.

Um detalhe interessante: um bloco recebe informações durante um tempo de aproximadamente 10 minutos. Depois disso, ele é criptografado utilizando o hash de um bloco validado na rede. Dessa forma, os novos blocos estão "ligados" aos blocos antigos, formando a cadeia.

.



Segurança da Informação

Funções de Hash

Aplicações da Função *Hash*

O hash nosso de cada dia...

Quando falamos de hash, blockchain e criptografia, achamos que tudo isso pode estar muito distante de nós, o que não é verdade.

Lembra das três principais utilidades dessa função citadas no início do artigo? Se não, vou lhe lembrar aqui:

- Resumir dados;
- Verificar integridade de arquivos;
- Segurança de senhas em servidores.

Segurança da Informação

Funções de Hash

Aplicações da Função *Hash*

Download de um arquivo

Quando você está baixando algum arquivo na rede, seu telefone ou computador está solicitando do banco de dados do servidor um arquivo que possui um hash associado.

Geralmente, a solicitação do download é rápida, certo? Isso ocorre porque o armazenamento desses arquivos dentro do servidor é feito por meio de funções criptográficas. Então, o servidor consegue procurar rapidamente no banco de dados o arquivo que está sendo solicitado.

Segurança da Informação

Funções de Hash

Aplicações da Função *Hash*

Antivírus

O principal trabalho de um antivírus, dentro de um computador ou telefone, é verificar a integridade de um arquivo por meio do hash.

Quando você solicita um download, o antivírus verifica se o arquivo que está chegando ao seu dispositivo possui o mesmo hash que o servidor forneceu. Se sim, o download é seguro. Caso contrário, pode indicar que algum invasor corrompeu o arquivo e por isso o hash foi alterado.

Segurança da Informação

Funções de Hash

Aplicações da Função *Hash*

Recuperação de Senhas

A segurança de dados é um aspecto fundamental da função hash. Os servidores mais seguros armazenam as senhas dos usuários de modo criptografado. Então, sua senha "doguinho2020" não fica explícita dentro do banco de dados.

Quando você solicita a recuperação, por exemplo, é difícil o servidor descriptografar o hash da sua senha e, por isso, ele lhe manda um código para criar uma nova.

Se você já tentou recuperar uma senha e recebeu um código no e-mail para criar uma senha nova, sabe do que estamos falando.

Referências

- Voitto

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