COLOMBIA POTENCIA DE LA VIDA

TIC

Módulo 1

LECCIÓN 2

Funciones de hash

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Función de hash

Tiempo de ejecución: 2 horas

Planteamiento de la sesión:

En la segunda sesión se estudiarán las funciones de hash y su importancia en la seguridad e integridad de los datos en una blockchain. Se expondrán sus principales características y algunas de las funciones más usadas.

Desarrollo de la sesión: 2 horas

Algoritmo de hashing

Los algoritmos de hashing son herramientas esenciales en el mundo de la criptografía, y son una pieza clave en el blockchain con sus aplicaciones de firma electrónica. Con estos algoritmos se pueden generar y crear firmas digitales para comprobar la integridad y no alteración de documentos firmados.

Características fundamentales:

Se puede describir el código hash como una serie alfanumérica con una longitud fija, la cual identifica o representa un conjunto específico de datos, como un documento de texto, una imagen o un video. Un ejemplo de un código hash podría ser algo similar a esto:

10f4acae93252afb8fdca2845bb6017b.

Estos códigos alfanuméricos se generan mediante lo que se conoce como función hash, que es básicamente un algoritmo matemático que transforma el conjunto de datos de entrada en una expresión alfanumérica con una longitud específica, el código hash en sí.

Sus características fundamentales son las siguientes:

Se plantea realizar la siguiente actividad con los estudiantes:

Haga el pseudocódigo y el diagrama de flujo de los siguientes algoritmos:

1. El código hash sirve para identificar de manera inequívoca un documento o los datos que representa. Si una entrada sufre una alteración, el código hash resultante va a tener variaciones importantes que permiten identificar la discrepancia. Es muy difícil encontrar dos entradas que puedan generar el mismo hash.
2. Son resistentes a colisiones. Como el hash cambia con cada entrada o variación, permite que los códigos generados sean únicos.
3. Son funciones unidireccionales. Los datos de entrada generan un código hash único, pero partiendo del código resultante no es posible descifrar cuál fue la entrada que produjo el hash. Esta es una de las características clave para garantizar la seguridad en una red blockchain.

Algoritmos hash más usados:

MD **SHA** **BLAKE**

En los inicios de la criptografía, los algoritmos de cifrado consisten en sustituciones o desplazamientos de letras en el alfabeto o en los números. Este método fue efectivo en su momento, pero actualmente este tipo de algoritmos se pueden descifrar usando fuerza bruta, es decir, probando todas las combinaciones posibles hasta obtener el mensaje original.

A lo largo del tiempo, gracias a la evolución de la tecnología se han desarrollado diversos protocolos y algoritmos para la generación de códigos hash y cifrados fuertes, buscando constantemente mejorar la seguridad y la utilidad de esta herramienta criptográfica esencial. Los algoritmos de hashing desempeñan un papel crucial en diversas aplicaciones, desde la verificación de integridad de archivos hasta la gestión de contraseñas

Entre los algoritmos hash más notables se encuentran:

MD5

Desarrollado en el año 1991, el MD5 surgió como una mejora de su predecesor, el MD4. Sin embargo, con el tiempo se descubrieron vulnerabilidades que compromete su integridad y seguridad, lo que llevó a su desuso en contextos sensibles, por lo cual este algoritmo no es útil en el contexto de blockchain.

SHA-1, SHA-2, SHA-3

La NSA estadounidense (National Security Agency) desarrolló estos algoritmos hash entre los años 1993 y 2015. Aunque el SHA-1 ha demostrado vulnerabilidades a lo largo del tiempo, SHA-2 y SHA-3 siguen siendo ampliamente utilizados en la actualidad. Estos algoritmos se emplean para garantizar la integridad y autenticidad de los datos en diversas aplicaciones, incluyendo la firma digital y la seguridad en transacciones.

BLAKE 2 Y BLAKE 3

Estos son algoritmos de hashing más recientes que han ganado reconocimiento por su eficiencia y velocidad en la generación de códigos hash. Ofrecen mejoras respecto a funciones hash anteriores, convirtiéndose en buenas opciones para aplicaciones donde el rendimiento es crítico debido a las grandes cantidades de datos de entrada.

SHA-256 (PARTE DE SHA-2)

El SHA-256 es una variante de la familia SHA-2 y se utiliza ampliamente en la actualidad. Ofrece un espacio de salida de 256 bits y es conocido por su resistencia a ataques criptográficos. Este algoritmo se utiliza en muchas implementaciones de blockchain para garantizar la integridad de los bloques y la seguridad de las transacciones. Su robustez y amplio uso lo convierten en una elección común en aplicaciones que requieren una alta seguridad.

Aplicaciones:

El código hash desempeña un papel fundamental en el ámbito de la criptografía y la firma electrónica, así como en diversas aplicaciones prácticas. En el campo de la tecnología blockchain, los códigos hash son esenciales para identificar de manera única archivos o documentos que residen en los bloques, asegurando que no hayan sufrido modificaciones después de ser firmados. Cualquier cambio en los datos de entrada generaría un hash completamente diferente, evidenciando alteraciones en el documento. Además, el hash se utiliza para verificar la autenticidad de la firma a través de claves públicas y privadas en sistemas blockchain.

En el ámbito de las criptomonedas, los códigos hash son un componente clave en el proceso de minado y verificación de transacciones. En el caso de la gestión de contraseñas en servicios en línea, estas se almacenan en formato hash en lugar de texto, garantizando mayor privacidad y seguridad. Durante la recuperación de contraseñas, se utilizan estos códigos en lugar de expresiones de texto plano.

Esta tecnología versátil ha permitido implementar avances significativos en seguridad digital, siendo fundamental en diversas transacciones y gestiones en línea tanto en el ámbito público como privado.

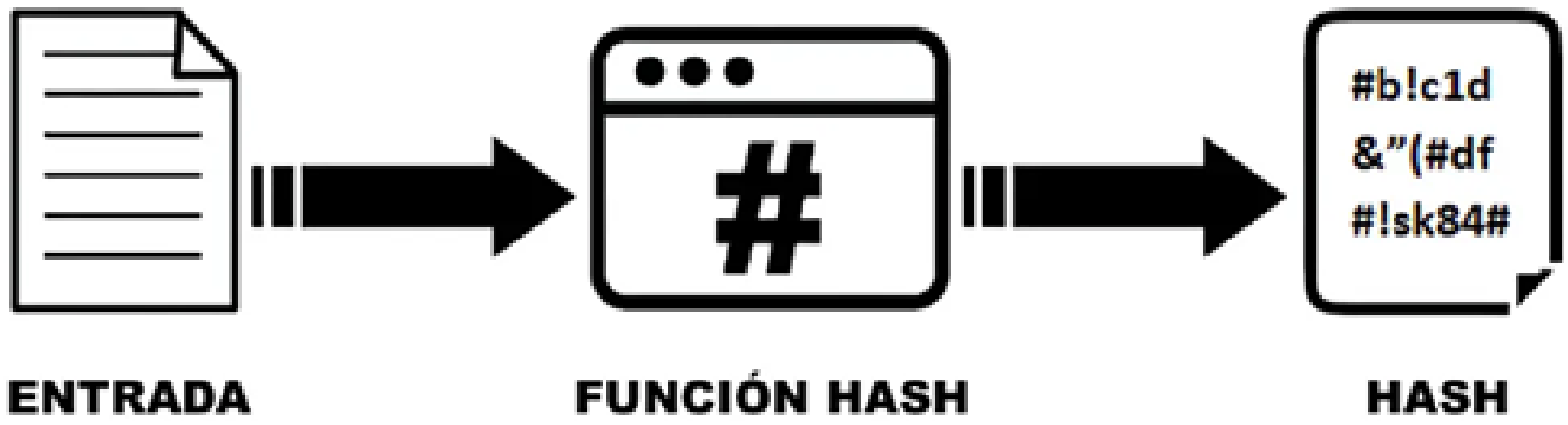

Figura 4: Función hash en un documento de texto.

En la figura 4 se puede ver una representación gráfica de un fichero de texto cualquiera, al cual se le aplica una función hash para cifrar su contenido. Si un atacante obtiene el documento con el hash, va a tener un archivo con caracteres aleatorios y al no ser un proceso reversible, no podría obtener los valores reales del documento de entrada.

Figura 4.1: Imagen a hash.

En la figura 4.1 se observa un archivo .jpg al cual se le aplica la función SHA-256. Como se mencionó anteriormente, los algoritmos de hashing son aplicables a cualquier tipo de documento. En este caso, el algoritmo toma la entrada (en este caso, los bytes de una imagen) y produce un valor hash de longitud fija de 256 bits. Este valor hash es esencialmente una representación única y fija de los datos de entrada. La imagen, al ser un archivo binario, se procesa byte por byte y cada bloque de datos pasa por las operaciones matemáticas necesarias para poder general el resultado. Si se ingresara una imagen diferente a la de la figura 4.1, el valor hash generado va a ser otro.