UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Redes de Ingeniería

https://revistas.udistrital.edu.co/index.php/REDES

RΣDES DE INGENIERÍA

ARTÍCULO DE REVISIÓN

Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos

Analysis of the Cryptographic Hash function in block chains and its impact on the security of data transactions

Yesid Díaz Gutiérrez[1]
Juan Manuel Cueva Lovelle[2]

Para citar: Díaz, Y., y Cueva, J. (2018). Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos. *Redes de Ingeniería*, *9*(2), 82-87, doi: https://doi.org/10.14483/2248762X.14383.

Recibido: 4-febrero-2019 / Aprobado: 22-mayo-2019

Resumen

Un *hash*, como se conoce comúnmente a las funciones criptográficas, se puede definir como un algoritmo matemático capaz de convertir un bloque de datos cualquiera en una colección nueva de caracteres con un tamaño específico, sin importar la cantidad de caracteres de los datos iniciales; en ese orden de ideas los elementos funcionales para el tratamiento de la información y las transformaciones que el hash permite y proporciona pueden ser aplicados como mecanismos de seguridad en cadenas de bloques, facilitando la protección de la información en tareas de autenticación de usuarios, envío de datos entre bloques o resguardo de información relevante. Este documento presenta de forma detallada la aplicación de la función hash criptográfica SHA-256 para el uso de apuntadores de longitud fija de 256 bit, con el objetivo de mapear cada una de las cadenas de bloques dentro de las transacciones de datos.

Palabras clave: blockchain, criptografia, hash, seguridad, transactions.

Abstract

A hash, as cryptographic functions are commonly known - can be defined as a mathematical algorithm capable of converting any data block into a new collection of characters with a specific size, regardless of the number of characters of the initial data; in that order of ideas the functional elements for the treatment of information and the transformations that the hash allows and provides; they can be applied as security mechanisms in block chains, facilitating the protection of information in user authentication tasks, sending data between blocks or safeguarding relevant information. This document presents in detail the application of the SHA-256 cryptographic hash function for the use of 256-bit fixed-length pointers in order to map each of the block chains within the data transactions. The use of 256-bit fixed-length pointers in order to map each of the block chains within the data transactions.

Keywords: blockchain, cryptography, hash, security, transactions.

1. Magíster en Dirección estratégica en tecnologías de la información, Universidad Internacional Iberoamericana, Puerto Rico; director Nacional del Programa Ingeniería de sistemas, Corporación Unificada Nacional de Educación Superior, CUN, Colombia. Correo electrónico: yesid_diaz@cun.edu.co
2. Doctor en Informática, Universidad Politécnica de Madrid, España. Docente del Departamento de Informática, Universidad de Oviedo. Correo electrónico: cueva@uniovi.es

INTRODUCCIÓN

Una de las principales dificultades relacionadas con el riesgo e integridad de los datos es la facilidad para modificar o eliminarlos, una vez se han superado los controles de autenticación de usuarios en los protocolos de seguridad. El Blockchain, por su concepción de distribución de la información en cadenas de bloques, permite identificar claramente la ubicación de la información, generando una marca específica de cada uno de los datos y su trayectoria dentro de la cadena; sin embargo en los procesos de transacciones de datos es necesario disponer de una protección adicional que permita encriptar la información, sin importar el tamaño de caracteres.

De acuerdo con lo anterior y con base en las características funcionales de elementos criptográficos del blockchain, como el hash y el nonce y la interacción de elementos adicionales, es posible diseñar una estructura capaz de encriptar tanto la información que ingresa a la cadena, como la que se procesa en cada una de las transacciones. Esta encriptación se centra fundamentalmente en la capacidad del hash SHA-256 para convertir un bloque de datos cualquiera en una nueva colección de datos, que por medio del número único generado por el nonce facilita el proceso de minado.

En la Figura 1 se muestra de forma general la estructura de cadena de bloques propuesta para implementar un protocolo de seguridad en las transacciones de datos por medio del hash.

Con el objetivo de comprender un poco más la funcionalidad del hash 256, a continuación se muestran en la Figura 2 los resultados de aplicar el algoritmo matemático del hash 256, al convertir cualquier boque de datos, en una colección de 64 caracteres, sin importar el tamaño original.

Como se puede observar en la Figura 2, a pesar del tamaño del texto original, el resultado de aplicación del hash 256, siempre será una encriptación única de 64 caracteres totalmente diferente. Este modelo de encriptación facilita la manipulación de datos, toda vez que sin importar el tamaño del texto recibido, puede ser manejado con un tamaño de almacenamiento estándar de 64 caracteres en cada una de las transacciones realizadas.

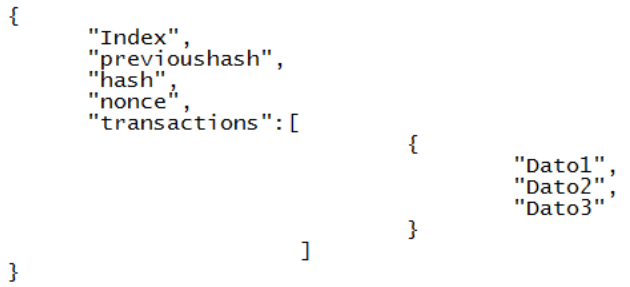

Figura 1. Estructura de cadena de bloques para seguridad en las transacciones de datos, por medio del hash SHA-256.
Fuente: elaboración propia.

Texto	Hash criptográfico 256
Comprobando	81d2aa6e f5e99328 881f95c3 1a27f7ae a51099cf bcb5e0ed daf4b6a4 a264eb9c
Comprobando la Funcionalidad	d96ce280 9a2f5a03 fbbaef79 c6868fdd 48557fac 2464fc2b 840706b4 a22edad6
Comprobando la funcionalidad del hash 256	32f27710 dd3449ca f6307f9a 7e21b13f 3392eb28 d16bdbc6 2bc1974c 1f740159

Figura 2. Conversión de bloques de datos por medio del hash 256 en cadenas de 64 caracteres.
Fuente: elaboración propia.

ISSN: 2248–762X • Vol. 9, No. 2 (julio-diciembre 2018). 82-87

MÉTODOS

El desarrollo metodológico del proceso se orientó desde tres fases específicas: Apropiación; Modelamiento; y Desarrollo lógico.

Apropiación

Durante esta fase se procedió a analizar en detalle cuatro de los elementos del blockchian, con el objetivo de verificar su funcionalidad a fin de determinar el esquema en el cual brindan una mayor productividad, frente al reto de mejorar la seguridad de la información en los procesos de transmisión de datos.

De acuerdo con lo anterior, a continuación se describen los elementos que intervienen en el proceso y que permiten vulnerar la información.

Función hash Criptográfica SHA 256: este algoritmo matemático es el eje fundamental del proceso de seguridad de la información, ya que permite tomar una cadena de valores alfanuméricos de cualquier tamaño, para convertirlo en una cadena de valores de 64 caracteres. Dentro de los beneficios de implementar esta función se encuentran:

- Capacidad de almacenamiento limitada a 64 caracteres.
- Procesamiento estándar de acuerdo al tamaño de la cadena.
- Encriptación de los valores originales.
- Transacciones de datos soportadas a 64 caracteres.

Las siglas Sha hacen referencia a *Secure hash Algorithm* que traduce algoritmo de hash seguro y están estrechamente relacionadas con su fortaleza en la protección de datos.

Index: este elemento facilita la identificación y el conteo de cada una de las cadenas de bloques, permitiendo identificar el número de cadenas de bloques que intervienen en un proceso y la posición que actualmente se está validando. Por sus características funcionales, facilita la búsqueda de algún tipo de datos dentro de la cadena y permite el rastreo de la información dentro de varias cadenas.

Previoushash: facilita el enlazamiento de las cadenas de bloques, identificando plenamente la cadena anterior, con el objetivo de enlazarla con la nueva cadena. Es importante resaltar que en Blockchain es fundamental identificar las cadenas previas cuando se procede con la creación de una nueva cadena. Sumado a lo anterior, su uso determina el tope de la cadena de bloques identificando el final de la misma, de esta manera y con la articulación con el ***index***, no solamente se puede determinar cuántas cadenas han sido creadas sino cuál es el inicio y el final, facilitando la navegación y recorrido para proceso de búsqueda.

Nonce (Numbre That Can Only used Once): "El número que solo puedes usar una vez", es un número aleatorio utilizado en procesos criptográficos como parte del protocolo de seguridad en el proceso de autenticación de usuarios; su interrelación con el hash genera un esquema de control que vulnera la información contenida en cada uno de los bloques de posibles ataques, garantizando la integridad de la información, sobre todo durante la transmisión de los datos.

Modelamiento

A fin de comprender el modelamiento del esquema que se propone para garantizar la seguridad de la información en el proceso de transmisión de datos, con la aplicación de la función hash criptográfica, es necesario identificar claramente cómo se comunica cada cadena de bloques por medio del hash. En la Figura 3 se puede observar el modelo de comunicación de cadenas de bloques por medio del hash.

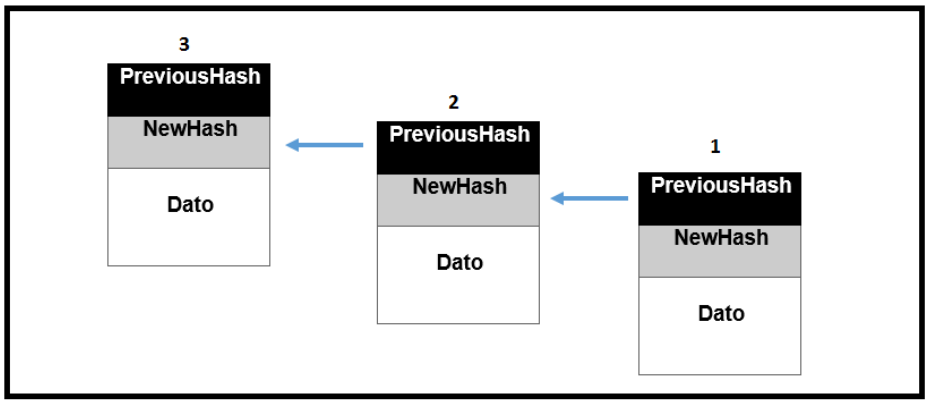

Figura 3. Modelo de comunicación de cadenas de bloques por medio del hash.
Fuente: elaboración propia.

En el modelo de comunicación de cadenas de bloques, representado en la Figura 3, se puede observar que todo el proceso se desarrolla a través de los hash; el PreviousHash en el bloque 1, se comunica con el NewHash del bloque 2; una vez establecida esta comunicación, el NewHash del bloque 2, se convierte en PreviousHash, lo anterior para conectarse con el Bloque 3 a través del NewHash de este Bloque, repitiendo este proceso de manera reiterativa de acuerdo con el número de bloques que se vayan creando. Para este esquema cada bloque es una transacción y la información de dicha transacción se replica en un nodo, dichos nodos hacen un papel muy similar al de un computador en una red, es decir almacenan la información de la transacción; sin embargo las características funcionales del esquema propuesto en el marco de las cadenas de bloques garantizan que si un nodo es violentado o eliminado, la información se regenera en un nuevo nodo evitando la pérdida o alteración de información.

Desarrollo lógico

Tomando como base fundamental el modelamiento del esquema propuesto y con el objetivo de generar el insumo para el futuro desarrollo de una aplicación de software que lo automatice, a continuación se formulan los procesos que hacen parte del desarrollo lógico de dicho esquema.

Proceso de inicialización

El proceso de inicialización permite la creación de cada uno de los nodos que harán parte de la cadena de bloques, una vez creados deberán ser inicializados para garantizar que se puedan acceder; lo anterior teniendo en cuenta que es en los nodos donde se replican todas y cada una de las transacciones, (Figura 4).

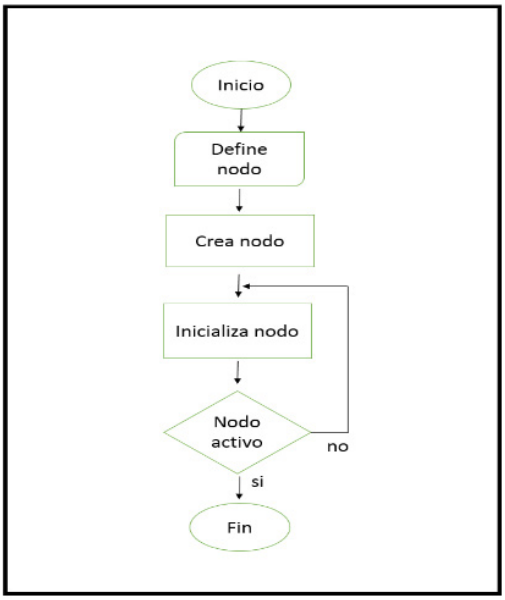

Figura 4. Desarrollo lógico del proceso de inicialización.
Fuente: elaboración propia.

ISSN: 2248–762X • Vol. 9, No. 2 (julio-diciembre 2018). 82-87

Proceso de sincronización

La sincronización es el proceso complementario a las actividades desarrolladas en inicialización, consiste en verificar los nodos creados e inicializados para hacerlos visibles con el fin de asignarlos a la cadena de bloques (Figura 5).

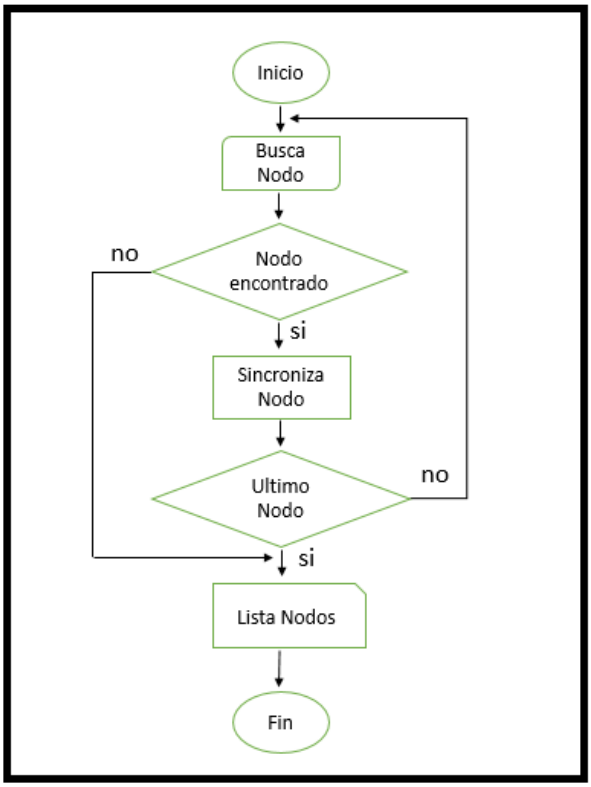

Figura 5. Desarrollo lógico del proceso de sincronización.
Fuente: elaboración propia.

Proceso de cargue

El proceso de cargue es el encargado de la creación de la cadena de bloques, por medio de la generación de un índex que para esta primera instancia quedará en cero, indicando que es el primer bloque de la cadena, el previoushah de partida o inicial, un hash criptográfico SH-256 para este primer bloque, un nonce aleatorio de minado y la transacción en blanco. Esta estructura garantiza que la cadena de bloque cumpla con el esquema funcional de seguridad de la propuesta desde la perspectiva de los elementos esenciales (Index, previoushash, hash y el nonce), Figura 6.

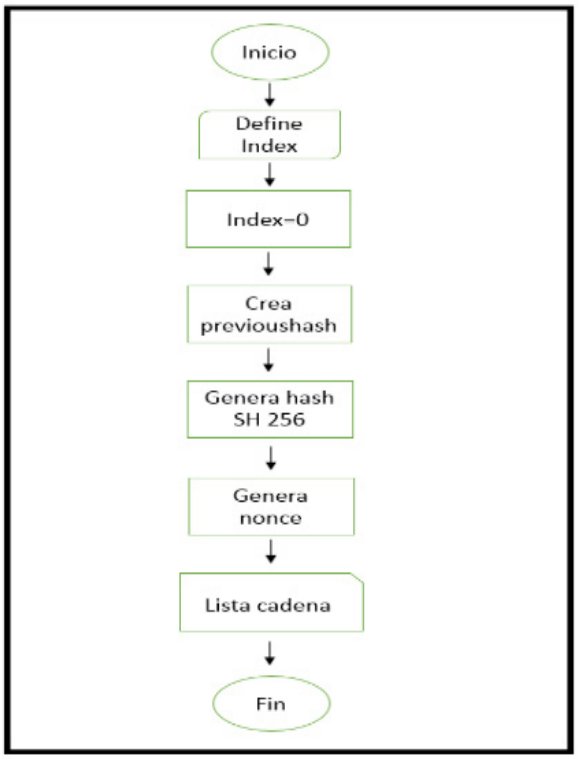

Figura 6. Desarrollo lógico del proceso de cargue.
Fuente: elaboración propia.

Proceso de transacción

Facilita el registro de la información (Figura 1), una vez se localiza el previoushash, creando el nuevo hash para la encriptación del dato o los datos que se desean proteger. Una vez enlazados con el previoushash, se envía la información a la transacción, garantizando que la información encriptada junto con sus complementos sean registrados en el bloque, Figura 7.

El proceso de transacción se repite cada vez que se registran nuevos datos en la aplicación, los datos son protegidos por el sistema de encriptación del hash SH-256 y los bloques se entrelazan por medio de los previoushash de cada bloque.

CONCLUSIONES

Los elementos utilizados en el esquema hacen parte de las características funcionales de las cadenas de bloques y su interacción garantiza la integridad de los datos en procesos de transmisión de información.

El control del index sobre el hash y el previous-hash, facilita la identificación de los datos almacenados en la cadena de bloques, permitiendo su protección y tratamiento.

La publicación de la información de cada una de las transacciones en los nodos genera respaldo a los datos ingresados a la cadena de bloques.

La automatización del proceso, a través de la construcción de un software diseñado sobre la propuesta de desarrollo lógico del esquema, permitirá el manejo de la información en cadenas de bloque de forma segura.

REFERENCIAS

[1] Sánchez, S., Domínguez, P., y Velásquez, L. Hashing, *Técnicas y hash para la protección de datos*.

[2] Escalona, S. B., y Inclán, L. V. "Funciones resúmenes o hash". *Revista Telemática,* 2012.

[3] Agulló, D., Guerra, M. C., Silva, F., y Vivanco, R. "Seguridad e integridad de la transferencia de datos", 2012.

[4] Cabrera Aldaya, A., y Cabrera Sarmiento, A. J. "Diseño e integración de algoritmos criptográficos en sistemas empotrados sobre FPGA", *Ingeniería Electrónica, Automática y Comunicaciones,* 2013.

[5] Donado, S. A., Vidal, L. Á. Q., y Meneses, E. M. Y. "Colisiones en el algoritmo de ciframiento SHA-1", *Generación Digital,* 2011.

[6] Navarro, B. Y., "Blockchain y sus aplicaciones". *Universidad Católica Nuestra Señora de La Asunción,* 2017.

[7] Nieto Ramírez, N., y Nieto Londoño, R. D., "Diseño asíncrono de las funciones de transformación del algoritmo Threefish-256". *Journal of Research of the University of Quindio,* 2013. https://doi.org/10.33975/riuq.vol25n1.164

[8] Aguirre, F., Alpago, O., Atencio, J., Furfaro, A., y Pazos, S., "Diseño, síntesis, fabricación y prueba de un Hasher SHA-256 en tecnología CMOS de 180 nm". *Proyecciones,* 2015.

[9] López, C. J. R., y Audelo, L. H. *Diseño e Implementación de una Función Hash Basada en Caos*.

[10] Salazar-Hernández, R., Díaz-Verdejo, J., García-Teodoro, P., Maciá-Fernández, G., y De Toro, F. *Uso de funciones compendio en la detección de anomalías mediante*.

[11] Fúster, A., de la Guía, D., Hernández, L., Montoya, F., y Muñoz, J. *Técnicas criptográficas de protección de datos*. Bogotá D.C.: Alfaomega, Grupo Editor, 2012.

[12] Tapscott, D., y Tapscott, A., *La revolución blockchain. Descubre cómo esta nueva tecnología transformará la economía global*. España: Ediciones deusco. séptima edición, 2017.

[13] Beck, R., Czepluch, J. S., Lollike, N., and Malone, S. "Blockchain-the Gateway to Trust-Free Cryptographic Transactions", *ECIS*, vol. 153, 2016, May.

[14] Shrier, D., Wu, W., and Pentland, A., "Blockchain & infrastructure (identity, data security)". *Massachusetts Institute of Technology-Connection Science,* 2016.

[15] Pradilla, J., Mora, J., & Capmany, J., "Amplification of the Bit Rate for Quantum Key Distribution Based on Cryptographic Hash Functions". *Network,* 2005.