Información Tecnológica
Vol. 32(3), 15-24 (2021)
http://dx.doi.org/10.4067/S0718-07642021000300015

Herramienta web con tecnología de cadena de bloques para un sistema de facturación electrónica en Colombia

Bryan García, Mario A. Sánchez y Jair Abadía
Facultad de Ingeniería, Ingeniería de Sistemas, Fundación Universitaria Católica Lumen Gentium, Cali-Colombia.
(Correo-e: bgarcia@unicatolica.edu.co; masanchez@unicatolica.edu.co; jabadia@unicatolica.edu.co)

Recibido Ago. 26, 2020; Aceptado Oct. 23, 2020; Versión final Dic. 14, 2020, Publicado Jun. 2021

Resumen

El objetivo de este estudio es usar el método inductivo para presentar el diseño e implementación de una herramienta software para un sistema de facturación electrónica usando tecnología cadena de bloques (blockchain). La facturación electrónica en Colombia es un proceso dirigido de acuerdo con los lineamientos de la DIAN (Dirección de Impuestos y Aduanas Nacionales). Dentro de los archivos de factura electrónica generados se encuentra un código de seguridad llamado CUFE (Código Único de Facturación Electrónica), el cual es el encargado de garantizar que la información contenida es única. En el presente estudio, una base de datos es diseñada usando MongoDB y la interfaz de acceso al sistema se desarrolló usando Bootstrap, HTML y JavaScript. La lectura, almacenamiento, procesamiento y creación de los bloques de la cadena fue implementada usando Flask y Python. Se obtiene como resultado una herramienta capaz de crear bloques de facturas electrónicas en 0,106 segundos. Se concluye que esta herramienta mejora la seguridad de facturación electrónica en Colombia.

Palabras clave: factura electrónica; blockchain; ciberseguridad; software; industria 4.0

Web tool with blockchain technology for an electronic invoicing system in Colombia

Abstract

The primary objective of this study is to use the inductive method to design and implement a blockchain technology software tool for electronic invoicing in Colombia. Electronic invoicing is a process managed in accordance with the guidelines of the DIAN (Dirección de Impuestos y Aduanas Nacionales). Each electronic invoice file contains a unique electronic invoice code (CUFE, in Spanish), which ensures that the information contained is unique. A database is designed by using MongoDB and the interface to access the system is developed by using Bootstrap, HTML, and JavaScript. Reading, storage, processing, and the creation of blockchains is performed by using Flask and Python. As a result, a new web tool is developed that is capable of creating electronic invoice blocks in 0.106 seconds. It is concluded that this web tool significantly improves the security of Colombian electronic invoicing systems.

Keywords: electronic invoice; blockchain; cyber security; software; industry 4.0

INTRODUCCIÓN

El proceso de facturación electrónica en Colombia está regulado por la DIAN mediante el decreto 2242 de 2015, en el cual se ampara el modelo obligatorio con fines de masificación y control fiscal de las entidades comerciales. Este decreto determinó la estructuración de un código llamado CUFE, el cual debería garantizar que para la combinación de los valores en algunos campos de la factura electrónica se obtendría un solo código de identificación (Dirección de Impuestos y Aduanas Nacionales-DIAN, 2020). Además, se define que la información debe estar contenida en un archivo XML (eXtensible Markup Language), el cual mediante etiquetas en estructura de árbol organiza los datos (De Campos et al., 2014).

La información contenida en el CUFE estaba codificada a partir del algoritmo SHA-1 (Secure Hash Algorithm, Algoritmo de Hash Seguro), el cual es una función criptográfica que toma una entrada y genera un valor hash de 160 bits, generalmente representado como un número hexadecimal de 40 dígitos (Visconti y Gorla, 2018; Sahu y Ghosh, 2017). La resolución 000042 del 05 de mayo de 2020, emitida por la Dian, presenta un cambio en el uso del algoritmo de encriptación de SHA-1 a SHA358, buscando mejorar el nivel de seguridad en los nuevos documentos debido a posibles fallas en estos. El uso de este algoritmo permite que las nuevas facturas electrónicas generadas para el sistema garanticen que la información contenida no pueda ser modificada sin cambiar el valor del código CUFE, sin embargo, no existe una trazabilidad en los cambios generados en el documento. Por otro lado, un gran número de facturas electrónicas emitidas anteriormente al decreto del año 2020 mantendrán su codificación inicial permitiendo la modificación de los datos ante intereses de terceros.

El algoritmo SHA-1 presentó una vulneración en su nivel de seguridad en el año 2005, donde investigadores de la universidad de Shangdong demostraron mediante 269 operaciones que el algoritmo no es óptimo. Además, el equipo formado por Google y CWI Amsterdam (Google Security, 2016), anunciaron la primera colisión del SHA-1; cambiando la información interna obteniendo el mismo código asociado. La colisión del algoritmo SHA-1 se logró mediante el uso de 110 GPUs trabajando durante un año, mostrando así las vulnerabilidades de seguridad de éste y con ello de todos los procesos que usen ese algoritmo para su seguridad interna.

En Colombia a la apropiación de la tecnología Blockchain se le presentó oposición por parte del gobierno nacional debido a relación directa con las criptomonedas. La superintendencia de comercio de Colombia, entidad encargada de la aceptación del uso de las criptomonedas, solamente reconoció al peso colombiano como única moneda válida en el país; limitando las investigaciones alrededor de este tipo de tecnologías (Vásquez et al., 2019). Una vez que el Blockchain fue usado en países como China, Estados Unidos y otras potencias mundiales, en Colombia se empezaron a desarrollar contratos inteligentes que usan esta tecnología disruptiva para disminuir la corrupción en el proceso (Téllez Ordoñez et al., 2019). El Blockchain también ha sido una herramienta útil en Colombia al servir de apoyo a los embargos judiciales, debido al control impuesto por medio de la cadena de bloques al gran número de participantes que intervienen en los procesos (Solarte-Rivera et al., 2018).

Las limitaciones del desarrollo tecnológico del Blockchain, debido a la falta de claridad en la reglamentación por parte de la legislación colombiana (Vásquez et al., 2019), evitan que procesos como el de facturar electrónicamente puedan disminuir sus riesgos de seguridad usando esta tecnología. Lo anterior se refleja en la ausencia de desarrollos para resolver el problema presentado en el método de facturación propuesto en el decreto 2242 de 2015. Por otro lado, el plan de desarrollo nacional presentado por el congreso de Colombia en el año 2018 muestra la necesidad de implementar tecnologías disruptivas que mejoren el desempeño en los procesos nacionales, siendo el Blockchain una gran alternativa de uso.

El desarrollo tecnológico actual puede ser descrito de acuerdo los lineamientos de la cuarta revolución industrial, termino introducido por Klaus Schwab (Xu et al., 2018). Esta revolución presenta un panorama donde la tecnología entra a mejorar los procesos físicos y biológicos ya existentes, mediante avances tecnológicos en áreas como la robótica (Han et al., 2013), la inteligencia artificial (Santos et al., 2020), impresión 3D, nanotecnología (Mónica et al., 2016), Blockchain (Ali Syed et al., 2019), internet de las cosas (Swamy y Kota, 2020), entre otros (Wan et al., 2016).

Las características que diferencian la cuarta revolución de las demás son su velocidad, la amplitud y profundidad de la percepción de la tecnología en los procesos y el impacto de los sistemas (Preukschat et al., 2016). La primera muestra como la evolución de los desarrollos tecnológicos aplicados bajo esta revolución se incrementan a ritmo exponencial, dando como resultado nuevas líneas de investigación a partir de las principales de la cuarta revolución. La segunda característica presenta como la tecnología no solo se percibe como algo que mejora el proceso, sino que se convierte en parte de este y finalmente, la tercera característica da a conocer el impacto de la tecnología que hoy en día la conexión a internet permite para cualquier proceso que trabaje con datos.

La cuarta revolución industrial permite mediante el uso de tecnologías emergentes intervenir procesos como la secuenciación genética, energías renovables, la computación cuántica entre otros, siendo así la oportunidad de fusionar tecnologías que interactúan entre el dominio físico, digital y biológico. Dentro de las ventajas que se le atribuyen a esta nueva revolución está la alta productividad, donde por medio del uso de la inteligencia artificial y la continua optimización de los procesos se incrementa la productividad en comparación con años anteriores (Dimitrieska et al., 2018). Por otro lado, la creación de nuevos trabajos debido a la necesidad de conocimiento avanzado y la interacción con sistemas que usan nuevas tecnologías. Además, se presentan modificaciones en procesos que eran realizados manualmente, donde ahora por medio de tecnologías como la impresión en 3D se toma menos tiempo en la implementación de estos proyectos y se mejora la calidad.

Para implementar las tecnologías de la cuarta revolución es necesario tomar en cuenta los alcances de acuerdo con una serie de desventajas que conlleva el uso de estas tecnologías (Dimitrieska et al., 2018). Dentro de estos se presenta la desaparición de empleos que no posean habilidades alineadas con la industria 4.0 a causa de la automatización al usar inteligencia artificial. Además, la aparición de nuevas tecnologías debe respetar los problemas éticos presentes, ya que, en caso de no tener precedentes, como el caso del uso de la inteligencia artificial o los vehículos autónomos, antes de proponer la tecnología es necesario definir estos lineamientos éticos. La conexión de todos los procesos a la red conlleva el mejoramiento de la seguridad ante ciberataques, donde dentro de las líneas que propone la cuarta revolución industrial se propone como solución el Blockchain.

Esta tecnología disruptiva fue propuesta en el año 2008 por un autor anónimo conocido como Satochi Nakamoto (Nakamoto, 2008), el cual presentó la tecnología aplicada a un proceso de compra y venta de criptomonedas. En (Wang et al., 2021) se presenta la tecnología Blockchain como una alternativa para mejorar el sistema de generación de contratos, mejorando su nivel de seguridad a través del lenguaje Ethereum. La generación de este tipo de documentos, conocidos como contratos inteligentes permite manejar la información de forma descentralizada, eficiente, transparente y con una trazabilidad de acuerdo con el historial del documento. En (Tanwar et al., 2020) se usa la tecnología Blockchain para realizar el seguimiento en un esquema de compra y venta de energía eléctrica. El área financiera es intervenida por esta tecnología dejando a un lado problemas como hackeo en transacciones monetarias, tarifas de transacción, fraude, entre otros (Tapscott y Tapscott, 2017). Por otro lado, el Blockchain puede ser aplicado a procesos médicos (Daraghmi et al., 2019), sistemas de votación (Shahzad y Crowcroft, 2019), certificados académicos (Jirgensons y Kapenieks, 2018), agricultura (Wu y Tsai, 2019), etc.

El Blockchain se presenta como una tecnología disruptiva capaz de mejorar los niveles de seguridad en un proceso, esto mediante la construcción de una cadena de bloques que contienen información específica (Choo et al., 2020). Cada uno de los bloques de la cadena tienen un elemento llamado hash, el cual es un código de encriptación a partir el algoritmo SHA-256. El hash es creado usando información contenida en el bloque, por otro lado, se establece una relación entre todos los bloques construyendo los códigos propios a partir del código hash en el bloque en el eslabón anterior. Esta relación entre los bloques es la que le brinda a la tecnología Blockchain la capacidad de detectar un intento de ataque a la seguridad de la cadena en sus diferentes puntos, ya que la modificación en algún bloque se verá reflejada tanto en el cambio del hash como en el cambio del hash alrededor de este.

De acuerdo con (Preukschat et al., 2016), los elementos básicos que componen la tecnología Blockchain son el nodo, el protocolo estándar de comunicación, la red entre pares y un sistema descentralizado. El primer elemento hace referencia a un ordenador con el software y hardware necesario para comunicarse con los otros dispositivos de la cadena. Por otro lado, el protocolo de comunicación son las reglas usadas por todos los nodos que comparten información de la red, donde en caso de existir una conexión directa entre dos ordenadores se le llama red entre pares.

Otra característica importante de esta tecnología es el funcionamiento descentralizado, donde, si el atacante decide modificar el proceso, el funcionamiento de este no depende de un solo nodo, sino que está distribuido en varios puntos (Preukschat et al., 2016). Finalmente, el sistema Blockchain debe estar supervisado por varias entidades, las cuales se encargan de verificar que el sistema no es modificado sin ser detectado. Los problemas de seguridad en los sistemas de facturación electrónica en Colombia debido al uso del algoritmo SHA-1 presentado en el decreto del 2015 pueden ser afrontados mediante la implementación de la tecnología Blockchain en el proceso, sin embargo, es necesario determinar en qué parte del proceso se implementa la tecnología. Es necesario diseñar e implementar herramientas que permitan aplicar esta tecnología disruptiva al proceso de manera efectiva, buscando eliminar los problemas de seguridad tecnológicos presentes en los procesos iniciales.

METODOLOGÍA

La metodología usada en este desarrollo es inductiva con un tipo de investigación aplicada y con alcance exploratorio, donde se busca desarrollar una aplicación para detectar un ataque en el sistema de Blockchain desarrollado y el tiempo usado en la creación de un bloque del sistema. La primera parte corresponde al diseño e implementación de la herramienta de acuerdo con los requisitos propuestos en la literatura. La segunda parte presenta el funcionamiento del sistema ante la detección de modificaciones de la información contenida en la factura electrónica. Finalmente, se presentan los tiempos resultantes al ejecutar la herramienta para crear un nuevo bloque del sistema.

La Figura 1 presenta la estructura de la herramienta propuesta para la implementación en la primera parte. Se observa como la etapa 1 corresponde a la base de datos, diseñada usando Mongo dB. La selección de este tipo de base de datos se debe a sus características como lo son la escalabilidad, la descentralización y la flexibilidad de la estructura de datos almacenados. La configuración de la base de datos se realiza mediante su aplicación nativa llamada Mongo DB Compass, donde se establecen los parámetros de interés y las colecciones a usar. Cada uno de los documentos almacenados deberán ser en formato JSON, ya que solo se maneja este tipo de estructura en esta base de datos.

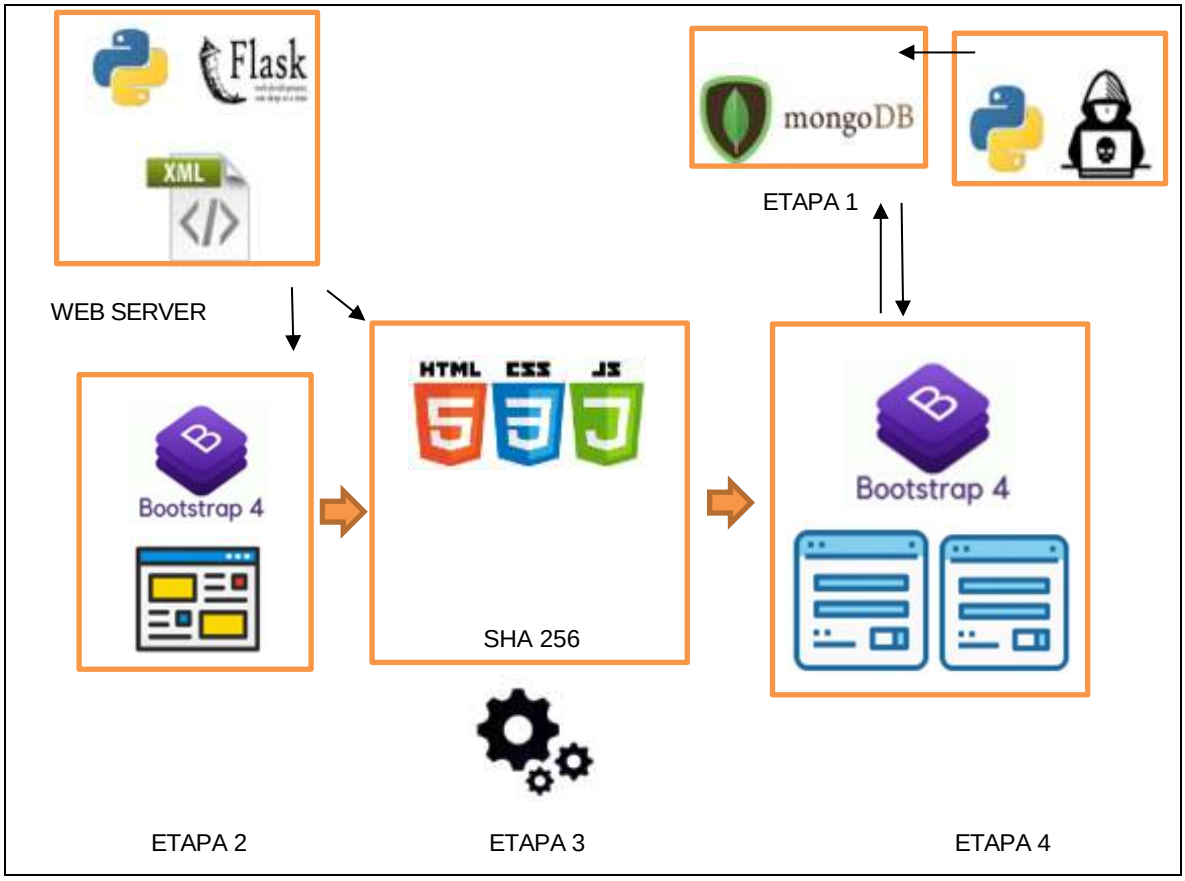

Fig. 1: Diseño estructural del software de facturación electrónica que usa tecnología Blockchain

Por otro lado, la etapa 2 corresponde a la interfaz de acceso al sistema, la cual se desarrolló usando Bootstrap, HTML y Javascript. La etapa 3 corresponde a la lectura, almacenamiento, procesamiento y creación de los bloques de la cadena. Cada una de estas funciones fue implementada usando Flask y Python, mediante el uso de un servicio web. Cada función que se desee ejecutar desde la interfaz de usuario será solicitada mediante una petición al servicio implementado en este lenguaje de programación. En esta etapa se implementarán funciones en Python que leerán mediante el uso de librerías la información contenida en los archivos XML de las facturas electrónicas y extraerán la información de forma automática para crear el bloque de la cadena, almacenándolo finalmente en la base datos creada. Finalmente, la etapa 4 corresponde a todas las interfaces de la herramienta que mediante Javascript presentan la información de la cadena de Blockchain aplicada a este proceso.

La herramienta web desarrollada presenta el esquema mostrado en la Figura 2. La navegación de la interfaz se realiza mediante el uso de pestañas, y en el archivo index.html presentará la página de acceso al sistema desarrollado. Al igual que la interfaz de acceso, todas las pestañas de la aplicación son implementadas

usando las mismas herramientas, HTML, Bootstrap y Javascript, donde está última también se encarga de realizar las respectivas solicitudes al servicio y de capturar la información en formato JSON que este le envía para mostrar la información en cada pestaña.

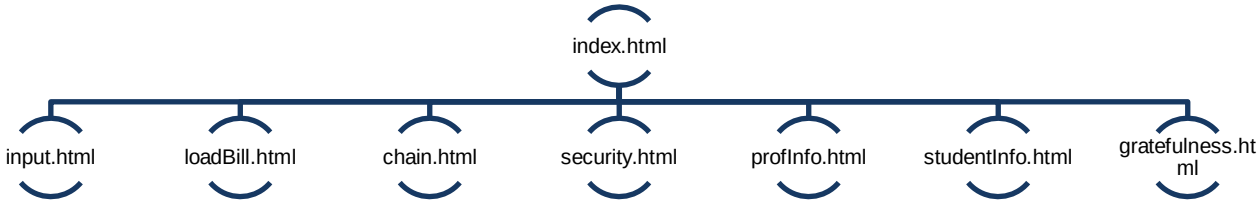

Fig. 2: Estructura de la interfaz propuesta en Bootstrap y HTML

Por otro lado, el servicio web desarrollado en Python debe ser ejecutado y puesto en funcionamiento con su respectiva dirección ip para solicitar la ejecución de sus tareas. Para el desarrollo de este documento se usó un servidor propio y un enlace a una dirección ip externa para simular la ejecución en un servidor privado. Sin embargo, en caso de utilizar la herramienta para fines comerciales será necesario establecer los respectivos protocolos de seguridad que garanticen el manejo de la información sin riesgos adicionales.

En la segunda parte se prueba el nivel de seguridad del sistema desarrollando un script en Python que accediera a la base de datos creada y modificara la información, de forma automática, contenida en algunos bloques de la cadena. Este script se ejecuta de forma local, donde se establecerá el número de bloque a intervenir y el cambio que se desea realizar en este, buscando emular la intervención en el sistema desarrollado. Finalmente, para medir la velocidad de creación de cada bloque de la cadena, se hicieron 10000 pruebas con cinco facturas electrónicas diferentes, donde se comprobó que en cada creación del bloque se obtuviera el mismo hash para el mismo grupo de datos.

RESULTADOS Y DISCUSIÓN

De acuerdo con los lineamientos de la metodología propuesta se diseñó una base de datos en Mongo dB para almacenar los datos de la herramienta. Lo anterior debido a que se debe contar con una base de datos para almacenar la información de los bloques de la cadena, los hashes creados y la información de los usuarios que acceden a ella. Por otro lado, la base de datos debe ser escalable y con características suficientes para el manejo de un gran volumen de datos en caso de ser necesario. La estructura de la base de datos la conforman las colecciones llamadas Bloque, BloqueHash, NameFile y Users. La primera colección se creó para almacenar la información de cada bloque del Blockchain, mientras que la segunda almacena los hashes de cada uno en orden. Por otro lado, la tercera colección guarda los nombres de los archivos XML correspondientes a las facturas electrónicas almacenadas en el sistema. Finalmente, la última colección almacena los datos de acceso de los usuarios que usaran la herramienta.

La interfaz de acceso se presenta en la Figura 3, donde una vez registrados los datos y al presionar el botón de envío se ejecuta una petición al servicio implementado en Python. Se comparan tanto los datos enviados desde la interfaz como los almacenados en la colección Users, donde al ser iguales se dirige a la siguiente pestaña del software. En caso de que los datos no sean correctos, la interfaz no permite el acceso al uso de la herramienta hasta realizar la respectiva corrección de los mismos.

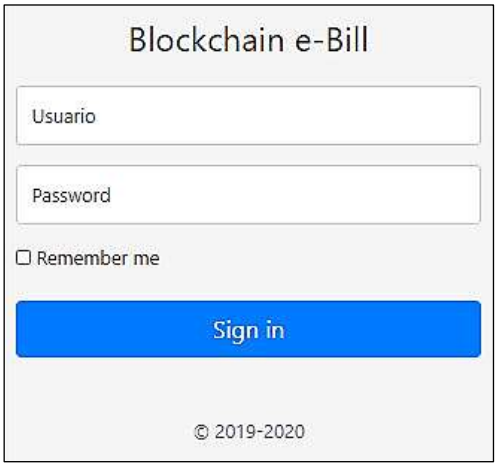

Fig. 3: Interfaz de acceso a la herramienta

La pestaña Cargar Factura Electrónica de la interfaz, mostrada en la Figura 4, permite almacenar la factura electrónica seleccionada contenida en un archivo XML, donde el nombre del archivo seleccionado se agrega a la colección respectiva. En caso de no existir el archivo seleccionado se procede a guardarlo en una carpeta interna de la herramienta, en caso contrario se emite una alerta diciendo que el documento ya existe.

Fig. 4: Interfaz para cargar la factura electrónica

La interfaz de creación de bloque se presenta en la Figura 5. Se observa como los datos son leídos a partir de un archivo almacenado en pasos anteriores, y presentados en una tabla que permite revisar la información de interés. Para crear un bloque a partir de la información de la factura electrónica escogida se presiona el botón Enviar a la cadena, el cual, mediante una petición al servicio creado en Python, solicita la encriptación de la información y la concatena a la cadena de la herramienta. La información usada para la creación del bloque se extrae automáticamente del archivo XML seleccionado para el proceso, donde se almacenan los datos de interés en una sola cadena de texto para someterla a la encriptación.

Fig. 5: Interfaz para seleccionar la factura electrónica, procesar la información y crear el bloque de la cadena

La implementación del algoritmo de encriptación SHA-256 implementado en el servicio de Python presentará un solo código de encriptación para un mismo conjunto de datos, sin embargo, si alguno de los datos cambia en solo un valor se obtendrá otro código completamente diferente. Lo anterior se presenta en la Figura 6.

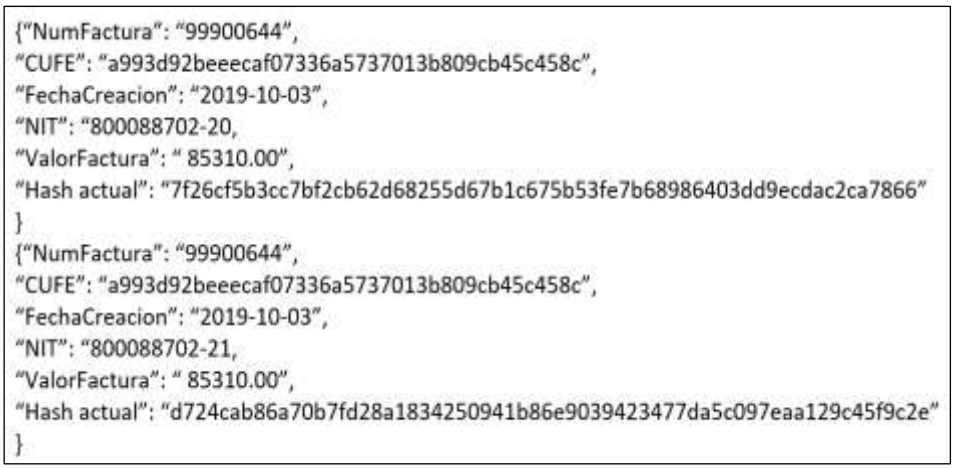

Fig. 6: Cambio en el hash al variar la información de los datos usados para el bloque de la cadena

La selección y procesamiento de diferentes facturas electrónicas darán forma a la cadena de la herramienta Blockchain, donde al seleccionar un archivo se dará origen a un bloque. En la pestaña Cadena de Bloques se presenta la información contenida en la base de datos a partir de los archivos procesados. Se presenta cada bloque en orden con la información contenida en cada uno de ellos. Se observa como la conexión entre bloques se realiza mediante la información contenida en los hashes de cada eslabón. Lo anterior se presenta en la Figura 7.

Fig. 7: Cadena de bloques de las facturas electrónicas almacenadas en el sistema de facturación

Finalmente, mediante el script desarrollado en Python se modificaron algunos datos en la cadena almacenada en la base de datos de Mongo dB, emulando un ataque al sistema. Se observa como en la pestaña Seguridad de la Cadena (Figura 8) se presenta el ataque a algunos bloques del sistema, mediante el cambio de color de azul a rosado, presentando de esta manera que la información contenida en el bloque es alterada debido a que los hash alrededor del bloque no concuerdan. La interconexión de bloques por medio del hash de cada uno dificultad realizar un ataque a este tipo de procesos con tecnología Blockchain, sin ser detectados por el sistema, ya que para modificar un solo bloque sería necesario modificar toda la cadena. Por otro lado, la descentralización de la aplicación y su cuidado a partir de varios nodos hacen aún más difícil la tarea de hacking.

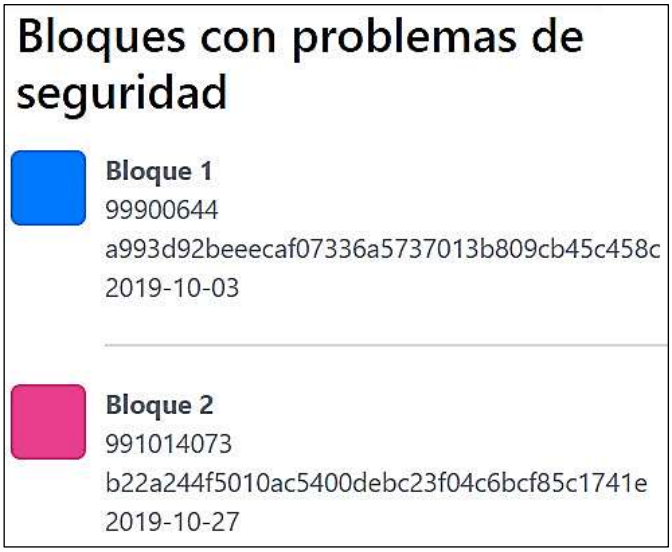

Fig. 8: Identificación de los bloques del sistema que fueron modificados por un ciberataque

Los resultados de las pruebas realizadas con cada factura electrónica son presentados en la Tabla 1, donde se reporta el número de bloques creados por factura, el tiempo promedio de creación de bloque y la desviación estándar de estos. El valor promedio de creación de los bloques de la cadena es de 0,106 segundos. Además, se observa que la desviación estándar en cada caso presenta poca dispersión de los tiempos en cada prueba, mostrando así que los tiempos de creación entre bloques son similares en cada uno de los casos donde la herramienta se ejecuta.

Tabla 1: Tiempo para la creación de bloques en el sistema de facturación electrónica

Archivo	*Bloques creados*	*Promedio creación bloque [s]*	*Desviación estandar*
factura1.xml	10000	0,102	0,039
factura2.xml	10000	0,101	0,061
factura3.xml	10000	0,111	0,084
factura4.xml	10000	0,103	0,056
factura5.xml	10000	0,112	0,109

El diseño e implementación del software propuesto en este documento permitió aplicar tecnología Blockchain a un sistema de facturación electrónica usando los requisitos propuestos por la DIAN, entidad encargada de regular estos procesos en Colombia. Esta herramienta permite comprender el proceso paso a paso de la generación de una cadena de información usando tecnología Blockchain buscando con esto que los lectores puedan replicar esta tecnología en otros procesos.

El tiempo empleado en la creación de cada uno de los bloques de facturación electrónica de 0,106 segundos se encuentra en un rango similar al de herramientas con tecnología Blockchain reportadas. Este es el caso de Hyperledger Fabric, donde se implementa un framework para medir la latencia y escalabilidad de un sistema con tecnología Blockchain (Kuzlu et al., 2019), obteniendo transacciones de hasta 0,01 segundos por medio de peticiones internas y de 0,13 segundos para transacciones abiertas. Por otro lado, plataformas como Ethereum, presentan velocidades de creación de bloques de hasta 0,2 segundos, mostrando así la eficiencia de estas herramientas en cuanto al manejo de información (Alrubei et al., 2020). Por otro lado, en (Misra et al., 2020) se realizó la simulación de un sistema en Ethereum para la generación de bloques aplicados a un sistema con tecnología IoT, reportando tiempos de generación de bloque de 5 segundos. Lo anterior permite comparar el sistema desarrollado con los presentados actualmente, mostrando un rendimiento competitivo en la creación de bloques con la herramienta generada, sin embargo, es necesario implementar pruebas de creación de bloques en paralelo y usar computadoras con mayores prestaciones para obtener mejor desempeño del software.

CONCLUSIONES

Los riesgos de seguridad en los sistemas de facturación electrónica son disminuidos al usar la tecnología Blockchain como herramienta. Por otro lado, es necesario realizar un análisis previo del proceso para verificar la utilidad de esta tecnología disruptiva, ya que para ciertos casos el uso de estas técnicas no es necesario ya que el proceso como tal cuenta con la seguridad suficiente.

Se desarrolló una herramienta web que usa tecnología Blockchain para disminuir los problemas de seguridad en el sistema de facturación electrónica en Colombia cumpliendo con los requisitos solicitados por las entidades de control. Además, el diseño presentado permite ajustarse al manejo de gran volumen de información al usar técnicas de Big Data como el map reduce mediante el uso de apis desarrolladas en lenguajes de programación como Python o Javascript.

Se realizaron 50000 pruebas de creación de bloques con tecnología Blockchain aplicadas a un sistema de facturación electrónica, obteniendo como resultado para el 100% de los casos el mismo hash de cada factura, mientras que el tiempo promedio de creación y almacenamiento de un bloque a partir de un documento fue de 0,106 segundos. Al comparar este desempeño con herramientas desarrolladas en otro frameworks, como lo son Etherum y Hyperledger Fabric, la herramienta propuesta presenta tiempos de creación de bloques dentro de los rangos estimados por estos desarrollos.

El uso del algoritmo SHA-1 para brindar protección en los sistemas de facturación electrónica presenta vulnerabilidades de seguridad importantes a la hora de confiar en esta herramienta, como fue demostrado por el equipo formado por Google y CWI Amsterdam. El uso de esta técnica en países como Colombia en facturas electrónicas, anteriores a la actualización del año 2020, exige que se implementen tecnologías que puedan

mejorar estos niveles de seguridad, como lo es el caso de la tecnología Blockchain. Se debe recalcar que, aunque las actualizaciones para las nuevas facturas electrónicas emitidas en el país utilicen un nuevo tipo de algoritmo de encriptación es necesario mejorar el nivel de seguridad en los archivos almacenados previamente. Aunque la actualización del decreto en el año 2020 disminuye la vulnerabilidad de seguridad al usar el SHA-358 no se garantiza la trazabilidad en la modificación de los documentos, propiedad que brinda el Blockchain.

AGRADECIMIENTOS

Se agradece a la fundación universitaria Católica Lumen Gentium (Unicatólica) por el apoyo en el desarrollo del proyecto de nombre “Aplicación de la tecnología Blockchain para disminuir los riesgos de seguridad tecnológicos en los sistemas de facturación electrónica”. Además, se agradece a todos los profesores del grupo de investigación KHIMERA que participaron en el desarrollo de la herramienta propuesta por medio de sus aportes.

REFERENCIAS

Alrubei, S.M., Ball, E.A., y otros dos autores, Latency and performance analyses of real-world wireless IoT-Blockchain application, https://doi.org/10.1109/JSEN.2020.2979031, IEEE Sensors Journal, 20(13), 7372–7383 (2020)

Choo, K.K.R., Yan, Z., y Meng, W., Blockchain in industrial IoT applications: security and privacy advances, challenges, and opportunities, https://doi.org/10.1109/TII.2020.2966068, IEEE Transactions on Industrial Informatics, 16(6), 4119–4121 (2020)

Daraghmi, E.Y., Daraghmi, Y.A., y Yuan, S.M., MedChain: a design of blockchain-based system for medical records access and permissions management, https://doi.org/10.1109/ACCESS.2019.2952942, IEEE Access, 7, 164595–164613 (2019)

De Campos, L.M., Fernández-Luna, J.M., y otros dos autores, Using personalization to improve XML retrieval, https://doi.org/10.1109/TKDE.2013.75, IEEE Transactions on Knowledge and Data Engineering, 26(5), 1280–1292 (2014)

Dimitrieska, S., Stankovska, A., y Efremova, T., The fourth industrial revolution: advantages and disadvantages, Economics and Management, 15(2), 182–187 (2018)

Google Security., SHA-1 Certificates in Chrome, t.ly/7KVH, acceso Diciembre (2020)

Han, M.J., Lin, C.H., y Song, K.T., Robotic emotional expression generation based on mood transition and personality model, https://doi.org/10.1109/TSMCB.2012.2228851, IEEE Transactions on Cybernetics, 43(4), 1290–1303 (2013)

Jirgensons, M., y Kapenieks, J., Blockchain and the future of digital learning credential assessment and management, https://doi.org/10.2478/jtes-2018-0009, Journal of Teacher Education for Sustainability, 20(1), 145–156 (2018)

Kuzlu, M., Pipattanasomporn, M., y otros dos autores, Performance analysis of a hyperledger fabric blockchain framework: throughput, latency and scalability, https://doi.org/10.1109/Blockchain.2019.00003, Proceedings 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019, 536–540 (2019)

Misra, S., Mukherjee, A., y otros cuatro autores, Blockchain at the edge: performance of resource-constrained IoT networks, https://doi.org/10.1109/tpds.2020.3013892, IEEE Transactions on Parallel and Distributed Systems, 32(1), 1–1 (2020)

Nakamoto, S., Bitcoin: a peer-to-peer electronic cash system, t.ly/UrC5, acceso Diciembre (2020)

Ordoñez, L.A.T., Niviayo, E.J.R., y Molano, J.I.R., Approach to blockchain and smart contract in Latin America: application in Colombia, https://doi.org/10.1007/978-3-030-31019-6_15, Applied Computer Sciences in Engineering, 1052, 500–510 (2019)

Preukschat, A., Kuchkovsky, C., y otros tres autores, Blockchain: la revolución industrial de internet, https://doi.org/10.22235/rd.v0i19.1721, Revista de Derecho, 19, 197–201 (2016)

Resolución número 000042 (05 de Mayo de 2020): Dirección de Impuestos y Aduanas Nacionales-DIAN, 601-620, Santafé de Bogotá, Colombia (2020)

Romo, M.J.B., Guerrero, J.A.B., y Amado, R.J.C., Sintesis y caracterización del nanomaterial TIo2-mwcnts (oxido de titanio-nanotubos de carbono de pared múltiple), https://doi.org/10.4067/S0718-07642016000600016, Informacion Tecnologica, 27(6), 153–162 (2016)

Sahu, A., y Ghosh, S.M., Review paper on secure hash algorithm with its variants, https://doi.org/10.13140/RG.2.2.13855.05289, International Journal of Technical Innovation in Modern Engineering & Science, 3(5), 1–7 (2017)

Santos, D., Dallos, L., y Gaona-García, P.A., Algoritmos de rastreo de movimiento utilizando técnicas de inteligencia artificial y machine learning, https://doi.org/10.4067/s0718-07642020000300023, Información Tecnológica, 31(3), 23–38 (2020)

Shahzad, B., y Crowcroft, J., Trustworthy electronic voting using adjusted blockchain technology, https://doi.org/10.1109/ACCESS.2019.2895670, IEEE Access, 7, 24477–24488 (2019)

Solarte-Rivera, J., Vidal-Zemanate, A., y otros tres autores, Document management system based on a private blockchain for the support of the judicial embargoes process in Colombia, https://doi.org/10.1007/978-3-319-92898-2_10, Lecture Notes in Business Information Processing, 316(28), 126–137 (2018)

Swamy, S.N., y Kota, S.R., An empirical study on system level aspects of Internet of Things (IoT), https://doi.org/10.1109/access.2020.3029847, IEEE Access, 8, 188082–188134 (2020)

Syed, T.A., Alzahrani, A., y otros cuatro autores, A comparative analysis of blockchain architecture and its applications: problems and recommendations, https://doi.org/10.1109/ACCESS.2019.2957660, IEEE Access, 7, 176838–176869 (2019)

Tanwar, S., Kaneriya, S., y otros dos autores, ElectroBlocks:a blockchain-based energy trading scheme for smart grid systems, https://doi.org/10.1002/dac.4547, International Journal of Communication Systems, 33(15), 1–15 (2020)

Tapscott, A., y Tapscott, D., How blockchain is changing finance, Harvard Business Review, 1(9), 2–5 (2017)

Vásquez, A., Bernal, J.F., y Tarazona, G.M., Cryptocurrency and its digital panorama in the Colombian government, https://doi.org/10.1007/978-3-030-21451-7_19, Communications in Computer and Information Science, 1027, 225–234 (2019)

Visconti, A., y Gorla, F., Exploiting an HMAC-SHA-1 optimization to speed up PBKDF2, https://doi.org/10.1109/TDSC.2018.2878697, IEEE Transactions on Dependable and Secure Computing, 17(4), 775–781 (2018)

Wan, J., Tang, S., y otros cinco autores, Software-defined industrial internet of things in the context of industry 4.0, https://doi.org/10.1109/JSEN.2016.2565621, IEEE Sensors Journal, 16(20), 7373–7380 (2016)

Wang, Z., Jin, H., y otros 3 autores, Ethereum smart contract security research: survey and future research opportunities, https://doi.org/10.1007/s11704-020-9284-9, Frontiers of Computer Science, 15(2), (2021)

Wu, H.T., y Tsai, C.W., An intelligent agriculture network security system based on private blockchains, https://doi.org/10.1109/JCN.2019.000043, Journal of Communications and Networks, 21(5), 503–508 (2019)

Xu, M., David, J.M., y Kim, S.H., The fourth industrial revolution: opportunities and challenges, https://doi.org/10.5430/ijfr.v9n2p90, International Journal of Financial Research, 9(2), 90–95 (2018)