UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

TIA
Tecnología, Investigación y Academia

Certificación digital de documentos académicos basada en la tecnología de blockchain

ACADEMIC DOCUMENTS DIGITAL CERTIFICATION BASED ON BLOCKCHAIN TECHNOLOGY

Steve Eduardo Moscoso Urdaneta[1], David Felipe Suárez Chacón[2],
Daniela Martin Vega[3]

Artículo de investigación

Para citar: Moscoso, S., Suárez S., Martin, D. (2019), Certificación digital de documentos académicos basada en la tecnología de blockchain. TIA,7(2), pp. 20-27.

Fecha de recepción:
2019-11-053
Fecha de recepción:
2019-12-13

Resumen:
La tecnología Blockchain es una manera efectiva de asegurar la confiabilidad de un sistema de transacciones. Esta característica la hace bastante apetecible para ser aplicada en sistemas de generación de documentos que requieran ser autenticados y/o verificados. En este artículo describiremos las principales características de Blockchain y cómo podrían ser utilizadas en diversos procesos de expedición de documentos oficiales.

Palabras Clave: Auditoría de Documentos, Blockchain, Certificación de Documentos, Seguridad en Documentos, Transparencia.

ISSN: 2344-8288
Vol. 7 No. 2
Julio- diciembre 2019
Bogotá-Colombia

Abstract:
In this research, you can find information about Augmented Reality, the advances it has The Blockchain technology is an effective way of ensuring the reliability of a transaction system. This feature makes of it a very useful tool to be applied on document-generation systems in which a given document might be required to be verified on its authenticity. In this paper, we will describe the main features that Blockchain provides, and how these can be utilized on several processes regarding official document issuing.

Key Word: Blockchain, Document Audit, Document Certification, Document Security, Transparency

[1] Ingeniero de Sistemas, Universidad Nacional de Colombia. Banco Colpatria Red Multibanca Colpatria S. A, steve.moscoso@gmail.com. Colombia.
[2]Ingeniero de Sistemas, Universidad Nacional de Colombia. Banco Colpatria Red Multibanca Colpatria S. A, schdavidf@gmail.com. Colombia
[3] Ingeniera Catastral y Geodesta, Universidad Distrital Francisco José de Caldas. Instituto Geográfico Agustín Codazzi, Colombia. dmartinvega@gmail.com. Colombia

1.Introducción

En la actualidad los colombianos se enfrentan a un gran problema de falsificación de documentos públicos, este problema aplica para documentos de todo tipo, desde una licencia de conducción, las escrituras de un predio, y hasta los títulos profesionales.

Esta situación evidencia una clara falencia de los entes reguladores en esta materia ya que no cuentan con un mecanismo confiable y seguro con el cual certificar la veracidad tanto de los documentos como de los trámites asociados a estos.

Debido a los grandes avances tecnológicos existe una herramienta que permite certificar la autenticidad de cualquier tipo de transacción. Esta herramienta, conocida como *"Blockchain"*, es una tecnología que permitiría gestionar un registro de transacciones público, seguro e inmutable de cualquier documento.

2. Contenido

A. Tecnología Blockchain

De acuerdo con [1], se entiende *Blockchain* o cadena de bloques como "un libro de contabilidad público o una base de datos descentralizada; es decir, que, en lugar de tener un administrador central, es distribuido y verificado por consenso a los participantes de la red".

En términos generales, esta tecnología es una base red de procesamiento distribuida donde los datos y las tareas de procesamiento de las transacciones son repartidos a los participantes la red, sin embargo esta tecnología no consiste en una única técnica, sino que se vale de la criptografía, las matemáticas, distintos modelos económicos, combinados con redes "peer-to-peer" (punto a punto) y algoritmos de consenso distribuido para resolver el problema tradicional de sincronización de bases de datos distribuidas. Es una construcción de infraestructura que integra muchos campos.

B. Arquitectura Blockchain

Los bloques de una Blockchain están conformados por una cabecera y un cuerpo. La cabecera se compone de las siguientes partes, las cuales describen las características del bloque [2]:

Versión del Bloque. Indica cuál conjunto de reglas de validación de bloque se aplicarán.

Hash de raíz del árbol Merkle. *Hash* de todas las transacciones de este bloque.

Etiqueta de Tiempo. Tiempo actual en formato de tiempo universal, en segundos transcurridos desde enero 01 de 1970.

Hash del Bloque Padre. *Hash* de 256 *bits* que apunta hacia el bloque anterior.

A su vez, el cuerpo de bloque se compone de un contador de transacciones y de las transacciones propiamente [2]. La estructura de cada bloque de la cadena se muestra en la Figura 1.

C. Beneficios de la Tecnología Blockchain

Descentralización. La característica principal de *Blockchain* es que no se confía en un único nodo centralizado. Por el contrario, cada transacción es controlada, compartida y autorizada por todos los nodos que participan de la red [3].

Trasparencia. Los datos almacenados por los sistemas de *Blockchain* son transparentes para cada nodo. Como si

fueran libros contables, cada transacción queda registrada y cualquier nodo puede consultarla [4].

Código abierto. La mayoría de los sistemas de *Blockchain* son abiertos para cualquier individuo que desee participar en la red. Es decir, cualquiera puede acceder a la información de la red. Los registros pueden ser verificados públicamente además de que las personas pueden usar esta tecnología para crear cualquier aplicación que quieran [1].

Autonomía. Gracias a la base del consenso, cada nodo en el sistema de *Blockchain* puede transferir o actualizar datos de manera segura. La idea es poder confiar tanto en una sola persona, como en todo el sistema, ya que nadie puede alterarlo [5].

Inmutabilidad. Cualquier registro se preservará para siempre ya que las operaciones que se realizan no se pueden alterar y son únicas. Las transacciones efectuadas son realizadas con base a un sistema criptográfico, lo que significa que permite que las operaciones sean casi imposibles de hackear [4].

Anonimidad. La tecnología de Blockchain solucionó el problema de confianza entre nodos, es decir, la transferencia de datos. Inclusive, cada transacción puede ser anónima. Solo es necesario conocer la dirección de *Blockchain* de la persona.

D. Tipos de Blockchain

La tecnología de *Blockchain* puede ser dividida brevemente en tres tipos:

Blockchain pública: Cualquier persona puede ver las transacciones y verificarlas. De igual manera puede participar en el proceso para obtener un consenso. Por ejemplo, *Bitcoin* y *Ethereum* son *Blockchain* públicas [3].

Blockchain híbrida: Esto significa que existe un nodo que tiene una autoridad superior a los demás y es quien decide qué nodo puede ser seleccionado para resolver una tarea en la red, usualmente tiene asociaciones de negocio. Los datos en la *Blockchain* pueden ser públicos o privados, lo que la convierte en un modelo parcialmente descentralizado. Por ejemplo *HyperLedger* y *R3CEV* son ejemplos de *Blockchain* híbridas [1].

Blockchain privada: En este caso los nodos están restringidos, lo que implica que no cualquier persona puede establecerse como nodo en la *Blockchain*. Un ente central tiene la autoridad de gestión de acceso tanto de nuevos nodos como de los nuevos datos de manera estricta [3].

Arquitectura Blockchain

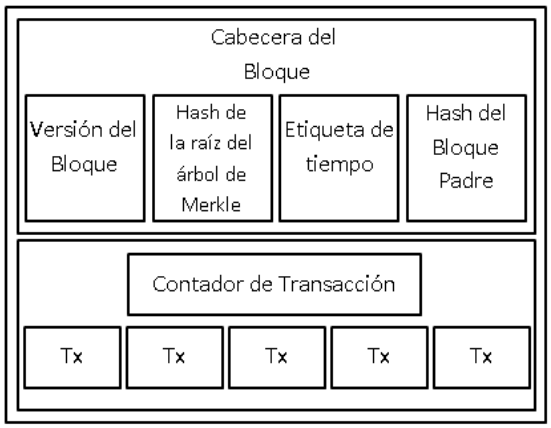

Fig. 1. Fuente: Elaboración propia.

E. Algoritmos de Consenso de Blockchain

Un algoritmo de consenso en el entorno de *Blockchain* es un conjunto de reglas para determinar si una adición de un bloque nuevo a la cadena es válida o no. Este algoritmo es acordado por todos los nodos de la red. Existen varias estrategias para este algoritmo, de las cuales se presentan los dos más comunes a continuación:

PoW (Proof-of-Work): es un algoritmo en el que se genera una pieza de datos, la cual necesita alta capacidad de procesamiento para ser construida, pero que a su vez sea fácil de verificar [6]. En una cadena de bloques, los mineros compiten entre sí para confirmar un bloque, es decir, para registrar sus transacciones. Quien gane la competencia recibe una recompensa y de esta manera se incentiva a que los nodos de la *Blockchain* tengan cada vez más capacidad de cómputo [3].

PoS (Proof-of-Stake): de manera similar al algoritmo PoW, es un algoritmo de consenso el cual busca conformar un bloque. Sin embargo, en este la probabilidad de recibir la recompensa es directamente proporcional a la cantidad de bloques que se poseen [6]. De esta manera quienes están más interesados en la seguridad de la cadena son quienes aseguran las transacciones de la misma [7].

Emisión de certificados end-to-end (*Blockcerts*)

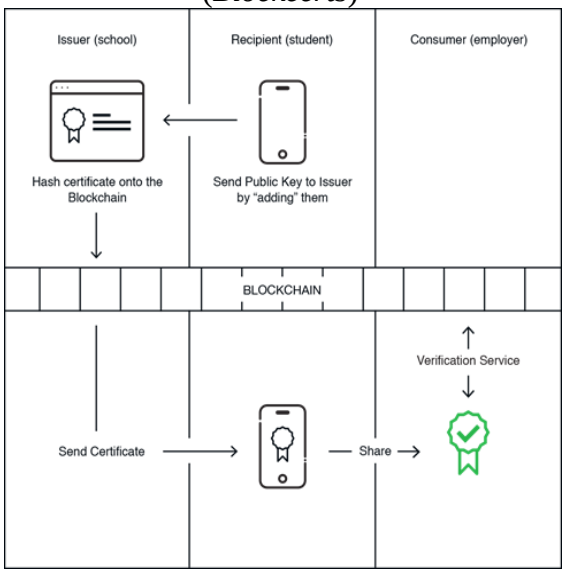

Fig. 2. Fuente: The Open Standard for Blockchain Certificates [8]

F. Estándar Blockcerts (Blockchain Certificates)

Blockcerts es un estándar abierto para crear aplicaciones que emiten y verifican registros oficiales basados en *Blockchain*. Estos pueden incluir certificados para credenciales académicas, licencias profesionales y más [8].

Contiene componentes para crear, emitir, ver y verificar certificados en *Blockchain* y provee un sistema descentralizado de credenciales. La red de la cadena de bloques funciona como un proveedor de confianza, verificando credenciales de forma segura. *Blockcerts* puede ser usado en contextos académicos y profesionales para verificar la legalidad de un título o certificado [9]. Por ejemplo, las universidades pueden emitir títulos a través de dicha plataforma, que podrían ser verificados al instante cuando los estudiantes los utilicen para solicitar trabajo o continuar sus estudios en otras instituciones. El código de *Blockcerts* es libre, por lo cual cualquier persona puede desarrollar aplicaciones basadas en su código fuente [8]. La Figura 2 muestra el proceso de emisión de certificados usando la tecnología *Blockcerts.*

3.Estado del arte

A. Aplicación de Blockchain en Criptomonedas

La aplicación más fuerte y reconocida de *Blockchain* a nivel mundial son las criptomonedas, entre ellas la más popular en el mercado es el *Bitcoin*, la cual está revolucionando la industria de servicios financieros. El ejemplo de *Bitcoin* muestra claramente cómo con la tecnología *Blockchain* se puede garantizar la propiedad de los bienes digitales, gracias a la existencia de varias bases de datos que comparten la misma información y que hacen parte de la cadena para garantizar su

integridad y transparencia al realizar transacciones [10].

B. *Aplicación de Blockchain en Ámbitos Médicos*

En lo que respecta a los datos de salud de los pacientes, un correcto almacenamiento de esta información, que puede ser recolectada gracias a la infinidad de aplicaciones y accesorios portátiles que existen actualmente, puede llegar a garantizar una correcta gestión de la investigación médica. Un ejemplo de estas aplicaciones es la empresa suiza *healthbank*, la cual ofrece a sus usuarios una plataforma en la que se pueden guardar y gestionar sus datos de salud de manera segura. Esta empresa aún no aplica *Blockchain*, pero el paso siguiente a dar por la corporación es incorporar esta tecnología. Ya en la actualidad, *healthbank* utiliza la información de los pacientes para la investigación, pero con *Blockchain* se ofrecería a los investigadores la posibilidad de rastrear los datos de salud con fecha y hora para examinar el avance [10].

Otra de las aplicaciones revolucionarias y más importantes de *Blockchain* en la industria de la salud es la posibilidad de disminuir de manera significativa la falsificación de medicamentos. El monitoreo a los procesos de producción de medicamentos ha sido una tarea bastante complicada para la industria, y se estima que alrededor del 10% de los medicamentos en el mundo son falsos, afectando tanto a los productos para mejorar el estilo de vida como a los medicamentos para el tratamiento de enfermedades graves como el cáncer.

Una red de investigación de la industria, llamada *Hyperledger*, recientemente mostró como *Blockchain* puede contribuir en la reducción de la falsificación de medicamentos e involucró varias compañías importantes a nivel global en este propósito. Los medicamentos se deben registrar en la base de datos, y por medio de *Blockchain* se puede determinar cuándo y dónde fue producido el medicamento, así como detectar el origen de un producto y sus componentes; y finalmente se hace clara y disponible la información de cualquier transferencia de propiedad de los medicamentos para fácilmente rastrearlos e identificarlos [10].

C. *Aplicación de Blockchain en Ámbitos Académicos*

Escuela de Holberton: La Escuela de Holberton, ubicada en San Francisco, desde octubre de 2015 utiliza el sistema *Blockchain* para almacenar y entregar los certificados que emite para sus estudiantes y egresados. Hacer uso de una cadena de bloques les ha permitido detener la emisión falsa, y la alteración de los registros guardados previamente.

"*La tecnología de Blockchain es el futuro de las certificaciones, y creemos que en los siguientes años más escuelas van a usar esta tecnología para validar sus certificados y diplomas*" indicó Sylvain Kalache, cofundador de la escuela Holberton en la entrevista realizada para la página http://www.marketwired.com [11].

Massachusetts Institute of Technology (MIT): En el MIT se ha estado trabajando una iniciativa que ha tenido muy buena recepción por parte de la comunidad académica. El programa piloto conocido como *Blockcerts Wallet*, surgió como un programa piloto a partir de un trabajo conjunto entre la oficina *"Registrar"* y la compañía *"Learning Machine"* [12].

Phillip Schmidt, director de innovación en el Media Lab del MIT comenzaba a experimentar con Blockchain generando

certificados digitales para su equipo de trabajo. *Learning Machine* y el *Media Lab* estarían colaborando después para construir el *OpenSource Toolkit* denominado *Blockcerts* [7]. A partir de este producto hicieron una implementación que aprovechaba los beneficios de seguridad evidenciados en la *Blockchain* utilizada por *Bitcoin*. Esta aplicación provee la seguridad de los datos transmitidos valiéndose de algoritmos de cifrado asimétrico, en los cuales se utilizan propiedades específicas de la aritmética modular para poder cifrar un conjunto de datos mediante cálculos matemáticos que involucran una *llave privada*, y descifrarlos mediante procedimientos similares usando una *llave pública*[2].

Para la generación de llaves pública y privada (un concepto no muy familiar para la comunidad en general) crearon una aplicación móvil con la cual un grupo de 111 estudiantes participaron para generar copias verificables de sus diplomas. Los directores involucrados aseguran que hay muchas posibilidades interesantes de aplicación para estas nuevas plataformas [12].

Universidad CESYT: CESYT es una universidad argentina con más de 40 años de historia ofreciendo programas curriculares profesionales. Durante el foro de *Bitcoin* en julio de 2015 expresaron su necesidad de usar un sistema para verificar digitalmente sus diplomas y certificaciones usando *Blockchain* [13].

A partir de octubre 27 del 2015 empezaron a operar con un sistema basado en la tecnología de *Blockchain* para el propósito mencionado anteriormente [13]. El aplicativo usa las funciones de cifrado *hash* para firmar digitalmente los documentos y almacenarlos en la *Blockchain*, lo que constituye la validación digital de los documentos. La verificación de los documentos se puede hacer a través de un sitio web con tan solo introducir el identificador del documento.

Su sistema se basa en dos conceptos clave: la firma digital y la marca de tiempo (o *timestamp*), los cuales solucionan gran parte de los posibles conflictos con falsificación y fraudes de títulos de estudios.

Universidad de los Andes (Venezuela): En la universidad nacional de los Andes en Mérida, Venezuela, el estudiante Andrés Isaac Aguilar Arocha presentó como trabajo de grado un documento que se titula: "*Certificación digital de documentos basada en contratos inteligentes en la tecnología Blockchain*" donde detalla el proceso de certificación digital de documentos usando la cadena de bloques. En este documento se explica a nivel general el diseño e implementación para un sistema no centralizado de certificación de documentos electrónicos, específicamente basándose en la tecnología utilizada por la criptomoneda *Ether*. El sistema se diseñó para apoyar la verificación de dos tipos de documentos: certificado de calificaciones y constancia de estudio. El sistema no se ha implementado aún [14].

D. Aplicación de Blockchain en Ámbitos de Verificación de Identidad

Modelo de Gestión de Información de Recursos Humanos: En el Simposio de la IEEE (2017) un equipo de trabajo colaborativo entre el Laboratorio de Sociedad Digital y Blockchain de la Universidad Beihang, la Universidad de Ciencia y Tecnología de Macao y la Universidad Marítima de Dalián, presentaron un modelo de aplicación de Blockchain para el manejo de información de selección de personal.

En este trabajo, los autores resaltaban la importancia de poder verificar la veracidad de la información académica que un postulante consignaba en su *Currículum Vitae et Studiorum*, ya que usualmente se presentan inconsistencias por títulos inexistentes o mención de habilidades profesionales con que no se cuentan en realidad [15].

En la propuesta se establecen las propias empresas como los nodos de la Blockchain, afianzando así la transparencia en los procesos de selección y en la información de perfiles profesionales del mercado laboral. También se propone un marco de trabajo y lenguaje de modelado basado en Blockchain para la especificación, diseño, implementación y pruebas de un sistema de información de este tipo (BML Framework) [15].

Biometría para la Seguridad de Documentos de Identificación**:** En la 41º Conferencia de Computer Software and Applications del IEEE (2017) el Grupo de Investigación en Biometría y Seguridad de Internet de la Universidad de Darmstadt (Alemania) ha propuesto un modelo de Blockchain basado en Bitcoin donde aplican una capa de seguridad adicional para asegurar la autenticidad de diversos documentos de identificación civil.

El mecanismo que utilizan para mejorar la seguridad se basa en la captura de datos biométricos en el momento de registro del documento, lo cual permitirá asegurar la pertenencia del documento al portador. En este trabajo se detalla que estos datos serán guardados como meta-datos de la cabecera de una transacción de Bitcoin, sirviéndose de los algoritmos de cifrado vigentes para garantizar la confiabilidad de la transacción a lo largo del tiempo [16].

Para el almacenamiento de estos metadatos, que pueden incluir imágenes de retina y representaciones digitales de huella dactilar, se proponen varias alternativas recomendadas de compresión de datos establecidas por la ISO/IEC JTC1 y por la Organización Internacional de Aviación Civil [16].

3. Conclusiones

Blockchain incorpora una serie de conceptos innovadores en términos de la autonomía y transparencia del sistema. Hemos visto en los ejemplos revisados cómo varias necesidades son susceptibles de ser suplidas mediante implementaciones especializadas con criterios específicos.

El panorama para utilizar esta tecnología es prometedor, ya que se pueden encontrar muchos entornos en los que tanto entidades públicas como privadas se beneficien del esquema de transacciones aseguradas que se obtiene al usar *Blockchain*.

A partir de los pilotos que se vienen trabajando por parte de las diferentes comunidades académicas, seguramente habrá trabajos colaborativos que resulten en plataformas bastante sólidas y estandarizadas que fortalezcan los lazos y trabajos conjuntos entre las instituciones educativas en el ámbito internacional.

4. Referencias

[1] M. Crosby, N. Nachiappan, P. Pattanayak, S. Verma and V. Kalyanaraman, (2015).“Blockchain Technology Beyond Bitcoin”, pp. 3,

[2] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, (2017)."An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” IEEE *International Congress on Big Data (BigData Congress)*, Honolulu, HI, 2017, pp. 557-564.

[3] Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017. Survey of consensus protocols on blockchain applications. In *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on* (pp. 1-5). IEEE.

[4] H. Halpin and M. Piekarska, (2017)."Introduction to Security and Privacy on the Blockchain," 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, 2017, pp. 1-3.

[5] Z. Chen and Y. Zhu, (2017)."Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging," 2017 IEEE International Conference on AI & Mobile Services (AIMS), Honolulu, HI, USA, 2017, pp. 93-99.

[6] English, S. M., & Nezhadian, E. (2017). Conditions of Full Disclosure: The Blockchain Remuneration Model. arXiv preprint arXiv: 1703.04196.

[7] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. J. Kishigami, (2015)."Blockchain contract: A complete consensus using blockchain," 2015 IEEE 4th. Global Conference on Consumer Electronics (GCCE), Osaka, , pp. 577-578.

[8] Blockcerts. (2017). "The Open Standard for Blockchain, Certificates". As of 14 March 2017: http://www.blockcerts.org

[9] Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards.

[10] M. Mettler, (2017)."Blockchain Technology in Healthcare: The Revolution Starts Here," in IEEE 18th International Conference on e-Health Networking, Applications and Services.

[11] Holberton School to Authenticate Its Academic Certificates With the Bitcoin Blockchain, (2015). http://www.marketwired.com/press-release/holberton-school-authenticate-its-academic-certificates-with-bitcoin-blockchain-2065768.htm

[12] Digital Diploma Debuts at MIT, (2017)- http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017

[13] Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2017). EduCTX: A blockchain-based higher education credit platform. arXiv preprint arXiv: 1710.09918.

[14] Arocha, B. A. I. A. (2017). Certificación digital de documentos basada en contratos inteligentes en la tecnología Blockchain.

[15] X. Wang, L. Feng, H. Zhang, C. Lyu, L. Wang and Y. You, (2017). "Human Resource Information Management Model based on Blockchain Technology," IEEE Symposium on Service-Oriented System Engineering (SOSE), pp. 168-173.

[16] N. Buchmann, C. Rathgeb, H. Baier, C. Busch and M. Margraf. (2017)."Enhancing Breeder Document Long-Term Security Using Blockchain Technology,"IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, 2017, pp. 744-748.