Entre Ciencia e Ingeniería, vol. 17, no. 34, julio-diciembre de 2023, páginas 36-42. DOI: https://doi.org/ 10.31908/19098367.2667
ISSN 1909-8367 (Impreso), ISSN 2539-4169 (En línea)

# Elementos de Seguridad para Gestión Documental con Blockchain[1]

# Security Elements for Document Management with Blockchain

J. Gutiérrez, P.A. Villa y A.M. López

Recibido: julio 21 de 2021 – Aceptado: noviembre 10 de 2023

***Resumen*—La tecnología Blockchain es reconocida por la transparencia e inmutabilidad de los datos que allí se registran. Estas características son esenciales en un sistema de gestión documental donde se requieren mecanismos de seguridad que eviten la falsificación de la información. Por esta razón, varios autores han optado por aprovechar los beneficios de la tecnología Blockchain en sus sistemas de gestión de documentos de tipo académico, médico, laboral, entre otros. No obstante, en su implementación se deben incluir elementos que refuercen la seguridad de la información pues los documentos suelen contener información sensible que requiere un tratamiento especial. En este artículo se realiza una revisión de los artículos más recientes sobre gestión documental con Blockchain con el objetivo de extraer los elementos de seguridad implementados en sus soluciones y realizar una síntesis que pueda servir como base a todo aquel interesado en desarrollar un sistema similar.**

***Palabras clave*— Blockchain, confidencialidad, documentos, gestión documental, seguridad de la información.**

***Abstract*— Blockchain technology is well known for the transparency and immutability of the data stored in it. These characteristics are essential in a document management system where security mechanisms are required to prevent information forgery. Therefore, several authors have chosen to take advantage of the benefits of Blockchain technology in their document management systems for academic, medical, and work-related documents, among others. However, its implementation must include elements that reinforce information security, since documents often contain sensitive information that requires special treatment. This article reviews the most recent articles on document management with Blockchain in order to extract the security elements implemented in their solutions and make a synthesis that can be used as a basis for anyone interested in developing a similar system.**

***Keywords*— Blockchain, confidentiality, documents, document management, information security.**

## I. Introducción

BLOCKCHAIN, o cadena de bloques, es una de las tecnologías más prometedoras en la actualidad, gracias a sus características principales: transparencia e inmutabilidad de la información registrada. Se define como "un libro mayor distribuido que actúa como un registro abierto y fiable de transacciones de una parte a otra y que, además, no está almacenado por una autoridad central, sino que todos los participantes tienen una copia y las actualizaciones se propagan por toda la red" [1].

Surgió en 2008 cuando Satoshi Nakamoto dio a conocer Bitcoin. Desde ese momento se han realizado numerosos estudios para aprovechar sus beneficios en diversos campos, entre los que se encuentra la gestión documental. El interés en este tema surge debido a la transformación digital que está ocurriendo en las empresas, donde la emisión de documentos se realiza en formato digital y requiere mecanismos que permitan asegurar la integridad y la validez de estos.

Generalmente, cuando los documentos se emiten en papel es más difícil falsificarlos porque se incluyen algunas características de seguridad [2]. Sin embargo, una de las desventajas de este formato es la ralentización en la verificación de los documentos, ya que se debe hacer principalmente de manera manual [2]. Esta es una tarea común en la contratación de personal, debido a que hay estudios que sugieren que el 30% de los solicitantes de empleo falsifican información relacionada con títulos recibidos, instituciones a las que asistieron o membresías profesionales [3], [4].

El compartir documentos también ha sido un proceso complicado, pues algunas organizaciones (por ejemplo, universidades u hospitales) suelen ser reacias a permitir que sus usuarios compartan sus datos fuera de su dominio

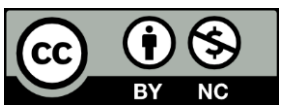
[1]Producto derivado del proyecto de investigación "Transformación de la cadena de suministros de documentos sin riesgo a través de Blockchain", apoyado por la Universidad Tecnológica de Pereira - Holding Digital.com S.A.S. a través del grupo de investigación Nyquist.

J. Gutiérrez, Holding Digital.com S.A.S., Pereira, Colombia, email: jotangutierrez@gmail.com.

P.A. Villa, Holding Digital.com S.A.S., Pereira, Colombia, email: paula2713@gmail.com.

A.M. López, Universidad Tecnológica de Pereira, Pereira, Colombia, email: anamayi@utp.edu.co.

**Como citar este artículo:** Gutiérrez, J., Villa, P.A. y López, A.M. Elementos de Seguridad para Gestión Documental con Blockchain, Entre Ciencia e Ingeniería, vol. 17, no. 34, pp. 36-42, julio-diciembre 2023. DOI: https://doi.org/ 10.31908/19098367.2667.



administrativo [5]. Existen casos, como los mencionados en [5] donde las universidades de Australia y Nueva Zelanda subcontrataron el intercambio de registros académicos a una organización de terceros llamada My eQuals (*https://www.myequals.edu.au/*), que emite los certificados de forma digital facilitando la experiencia para el usuario. Sin embargo, generalmente el propietario del documento debe ir a la organización a solicitarlo, e incluso escanearlo, para poder compartirlo con algún interesado.

En busca de mejorar estas situaciones, se han construido soluciones para gestionar el proceso de emisión y verificación de documentos utilizando la tecnología Blockchain. En este trabajo se realiza un estudio de los elementos implementados en dichas soluciones para conservar la seguridad de la información.

Este artículo está organizado de la siguiente forma: en la Sección II se presentan una introducción a la tecnología Blockchain. En la sección III se mencionan algunas soluciones desarrolladas para la gestión documental con Blockchain. Luego, en la sección IV se realiza una síntesis de la información encontrada. Finalmente, en la sección V se presentan las conclusiones.

## II. Tecnología Blockchain

El nombre de la cadena de bloques deriva de la manera en la que se guarda la información, pues las transacciones son registradas en bloques y cada uno de estos contiene un encabezado que lo enlaza al bloque anterior, formando una "cadena de bloques". Este enlace se crea usando funciones hash, que según el contenido del bloque generan de manera determinista una cadena de caracteres, de un tamaño determinado, llamada "valor hash". Con esto se logra la inmutabilidad de los datos, pues cualquier variación en el contenido de un bloque, genera un valor hash diferente al que se encuentra almacenado en el bloque siguiente.

La infraestructura de Blockchain se basa en una red entre pares (*peer-to-peer*) donde cada participante de la red se denomina nodo y funciona de manera autónoma conforme al mismo conjunto de reglas que abarcan el protocolo de pares, el protocolo de consenso, el procesamiento de transacciones, la gestión de libros mayores, entre otros [6].

Algunas de las características más relevantes de la cadena de bloques son: la descentralización, es decir, no depende de una autoridad central; inmutabilidad, ya que los datos una vez incluidos en la cadena no pueden ser modificados; y la transparencia, lograda al tener el libro mayor visible para todos los nodos.

Para lograr todo esto, Blockchain se basa en conceptos de criptografía para mantener la seguridad de las transacciones, teoría de juegos para alcanzar un consenso entre los participantes y ciencias de la computación para llevar todos los conceptos a una aplicación [7], [8].

Además, las cadenas de bloques pueden ser clasificadas, según el control de acceso, en públicas, privadas y de consorcio. Una cadena de bloques pública permite a cualquier persona unirse a la red, participar en el proceso de consenso y en la creación de transacciones. Una cadena privada es propiedad de una sola entidad que restringe el acceso y se encarga de asignar los permisos de lectura y escritura a los participantes. Mientras que en una cadena de tipo consorcio, el control se divide entre varias organizaciones.

Uno de los componentes principales de cualquier cadena de bloques es el algoritmo de consenso, que es el mecanismo a través del cual todos los participantes logran ponerse de acuerdo en el estado de la cadena. Existen varios algoritmos de consenso con características propias y que se enfocan en diferentes propósitos. El más conocido es Prueba de Trabajo (*Proof of Work, PoW*), pero también existe la Prueba de Participación (PoS), Prueba de Participación Delegada (DPoS), Tolerancia Práctica a Fallas Bizantinas (PBFT), Prueba de Autoridad, Prueba de Importancia, entre otros.

## III. Gestión Documental con Blockchain

Las soluciones que se han desarrollado para gestión documental con Blockchain han incluido información sobre certificados académicos, currículum vitae, registros médicos, entre otros. En cuanto a certificados académicos, en 2014 la Universidad de Nicosia se convirtió en la primera institución en emplear la cadena de bloques de Bitcoin para registrar los certificados de los estudiantes recibidos de las plataformas de cursos en línea [9], [10]. A partir de ahí, se han propuesto nuevos proyectos e integraciones con otras tecnologías que buscan mejorar la gestión de los documentos con Blockchain.

Es el caso de Blockcerts (*https://www.blockcerts.org/*), un proyecto que comenzó en 2015 como un estándar para crear, emitir, visualizar y verificar certificados basados en Blockchain y en el marco de Open Badges, a través del Verificador Universal de Blockcerts o creando uno propio a través del código abierto disponible en la página oficial [11], [12].

0xcert es otro proyecto que, a diferencia de Blockcerts, crea una Blockchain privada con diferentes tipos de moneda en la red que amplían el uso de la Blockchain [13]. Esta cadena de bloques privada separa el uso común de las transacciones y el proceso de certificación. Por lo tanto, la tasa de certificación se vuelve estable debido a los tokens no fungibles [13].

Otras soluciones para verificar la existencia de un artefacto digital se mencionan en [14], entre las que se encuentran: Veridoc Global (*https://veridocglobal.com/Passport*) que provee una solución para minimizar la creación de pasaportes falsos. POEX (*https://poex.io*/) es una solución basada en Bitcoin que brinda una prueba de existencia de cualquier documento digital. Los registros seguros de NEM (*https://nem.io/*) almacenan el hash del documento junto con los detalles de propiedad y la marca de tiempo en Mijin Blockchain. La solución Factoms Proof of Existence (*https://www.factom.com/solutions/connect/*) almacena el hash del documento en Factom Blockchain y confirma la existencia de datos y documentos con transacciones con marca de tiempo. La empresa SAP desarrolló TrueRec, una billetera digital segura y confiable para almacenar credenciales profesionales y académicas basadas en Ethereum [16].

También, se han desarrollado modelos con el objetivo de servir como guía para la construcción de aplicaciones. Das *et al*. [17] en su propuesta de un sistema de gestión de

documentos descentralizado que utiliza Blockchain, diseñaron un modelo de datos para el libro mayor que incluye un identificador de la transacción, direcciones de origen y destino de la solicitud, tipo de transacción, fase del proyecto, identificador y estado del documento, marca de tiempo y firma del emisor. Además, crearon un marco de contrato inteligente dividido en dos tipos de lógicas: un ejecutor de subprocesos y un orquestador de procesos, encargado de llamar las funciones de los ejecutores de subprocesos según el flujo de trabajo. Aunque todo fue planteado para proyectos de construcción, su diseño permite adaptarlo a cualquier proyecto.

Investigaciones recientes siguen avanzando en análisis específicos sobre la pertinencia de implementación de esta tecnología, es así como los autores en [53] realizaron análisis de tres escenarios de implementación diferentes y concluyeron que sería ventajoso una adaptación rápida de innovaciones basadas en blockchain, y consideran como retos más allá de la tecnología los cambios a nivel de procedimientos de los diferentes actores y organizaciones involucradas en los procesos de despacho de aduanas. También se tienen investigaciones con propuestas específicas que llegan hasta la generación de sistemas orientados a la prestación de servicios, los autores en [54].

Adicionalmente, sigue siendo vigente el análisis de la tecnología para identificar las áreas de mayor aplicación e identificar posibles nuevas áreas en las que se requiera la aplicación de esta tecnología. Un ejemplo de esto es el análisis realizado por los autores en [55], estos realizaron una revisión bibliográfica que permitió conocer sobre la tecnología y concluir que la mayoría de las aplicaciones blockchain se centraron los procesos de construcción, incluyendo como temáticas principales la gestión de pagos por uso y la gestión de la cadena de suministro.

A nivel de instituciones de educación superior, en especial el proceso de generación y validación de diplomas, los autores en [56] encontraron a partir del análisis realizado que se tienen muchas dificultades en la práctica durante la implementación de sistemas de blockchain, entre las que se encuentran, el mantenimiento del sistema y el consumo de energía, el aumento en la dificultad de actualizar los datos debido al proceso de hash, revocación de títulos y regeneración, falta de conocimiento y dificultad de uso.

Se presenta a continuación un análisis de elementos asociados a la seguridad de la información y cómo diferentes estudios han abordado esta temática.

## IV. Seguridad de la Información en Gestión Documental con Blockchain

Un sistema de gestión de documentos debe contar con características como la transparencia y la seguridad del documento [14], es decir, de la información que va a tratar. La seguridad de la información es definida por el estándar internacional ISO/IEC 27000:2018 como "*la preservación de la confidencialidad, la integridad y la disponibilidad de la información. También incluye la preservación de la autenticidad, la responsabilidad, el no repudio y la confiabilidad, cuando sea necesario. Su propósito es la protección de la información y de los sistemas de información del acceso no autorizado, el uso, la revelación, la interrupción, la modificación o la destrucción*" [18].

Las tres primeras propiedades son conocidas como los pilares de la seguridad de la información, siendo la confidencialidad la que asegura que la información solo esté disponible o sea divulgada a personas, entidades o procesos autorizados; la integridad garantiza la exactitud y completitud de la información; y la disponibilidad pone la información accesible y utilizable a petición de una entidad autorizada [18].

Para lograr todas estas características empleando una cadena de bloques, hay que utilizar una configuración adecuada y elementos que refuercen la seguridad de la información.

### A. *Configuración básica de la red Blockchain*

Generalmente, para aplicaciones de gestión documental se elige una cadena de bloques de tipo consorcio [5], [19], [20] debido a que los documentos suelen contener información sensible y los usuarios quieren estar seguros de con quién la están compartiendo [5]. Sin embargo, en [10] y [21] utilizaron cadenas de bloques públicas para que nadie tuviera el derecho de excluir datos o participantes. Respecto a las plataformas, las más usadas son Ethereum [10], [20]–[22] y Hyperledger Fabric [14], [19], [23], a esta última le resaltan como beneficio la modularidad ofrecida.

El almacenamiento fuera de la cadena es la opción preferida para guardar los documentos [10], [14], [19], [22], [23], tanto por privacidad como por las limitaciones de almacenamiento que presenta la cadena de bloques. Dentro de esta se guarda únicamente el hash del documento, que es un identificador único basado en su contenido [17] y conserva la privacidad al ser prácticamente imposible averiguar el contenido original de un hash.

Como sistema de archivos las aplicaciones han optado por IPFS (*InterPlanetary File System*) [10], [14], [17], [22], ya que permite mantener la plataforma completamente descentralizada [10] evitando el problema de tener un único punto de fallo y garantizando la disponibilidad de la información [24]. También, existen alternativas como un servidor de almacenamiento [20] o un almacén de datos personales (*Personal Data Store*) que permite a los usuarios recopilar, almacenar y dar acceso exclusivo a sus datos mientras protege su privacidad [5], [25], como es el caso de OpenPDS [25].

Por otra parte, si se utilizan Contratos inteligentes, es crucial garantizar que su implementación esté libre de errores y vulnerabilidades y sea segura contra ataques [26]. Para esto, en [26] utilizaron herramientas como ChainSecurity, Securify [27] y Oyente [28].

Finalmente, para asegurar el acceso a la cadena de bloques, en [29] se propone un sistema de autenticación multifactor que utiliza huellas digitales y preguntas secretas para asegurar las llaves privadas de los usuarios en una red Blockchain. Este es un punto importante a tener en cuenta, puesto que, si una persona obtiene de alguna manera la llave privada de otro usuario, tendría la capacidad de hacerse pasar por ese usuario si no existen medidas de autenticación adicionales para garantizar que la llave realmente le pertenece [30].

### *B. Métodos de Protección de la Confidencialidad*

Para conservar la confidencialidad de la información, en [31] la red se segrega en canales, donde cada canal contiene únicamente a los participantes autorizados a acceder a los datos que se despliegan en él, manteniéndolos privados para otras entidades. Además, todos los datos que transitan entre los nodos son cifrados a través de TLS (*Transport Layer Security*). Un aspecto clave, que se incluye en [31] es el registro automático en la Blockchain de todo aquel que solicite un documento, en su caso un certificado electrónico. De esta manera, se puede realizar una auditoría y un seguimiento confiable.

Los autores de [32] incluyeron en su sistema un módulo de protección de privacidad descentralizado que le permite a los propietarios de los datos seleccionar la configuración de privacidad deseada para estos antes de compartirlos.

Como se menciona en [33], el cifrado de datos se recomienda tanto cuando los datos se envían a través de redes (datos en movimiento) como cuando se almacenan (datos en reposo). Para esto se utilizan principalmente las funciones hash y la criptografía asimétrica [34], [35] que utiliza claves de cifrado (también llamadas llaves), cuya administración y distribución deben ser "seguras y estrictamente controladas" [33]. Además, se debe tener en cuenta la existencia de herramientas como las Tablas Arcoíris, que contienen una gran cantidad de hashes con su respectivo dato en bruto y permiten a los atacantes descifrar información en un periodo de tiempo corto en comparación con la técnica de fuerza bruta [36]. Por esta razón, es importante utilizar un algoritmo de encriptación fuerte.

El sistema CP-ABE (*Ciphertext-Policy Attribute-Based Encryption*) [37] ha sido utilizado en [38]–[40] para controlar el acceso a los documentos al trabajar con Blockchain. Una ventaja de CP-ABE es que permite realizar una autorización implícita, es decir, la autorización se incluye en los datos cifrados y solo las personas que cumplen con la política asociada pueden descifrar los datos [38], logrando un control de acceso detallado sobre estos [24]. Por lo tanto, no es necesario conocer con anticipación el conjunto de usuarios que podrán descifrar los datos.

Para incrementar la seguridad también se utilizan los hashes salados, que añaden unos bits aleatorios a la cadena antes de pasarla a la función hash, de esta manera se hace más complicado un ataque de fuerza bruta. Sin embargo, en [10] identificaron que al usar la misma "sal" para todos los cálculos de hash, se genera un problema de trazabilidad, por lo cual sugieren generar diferentes valores de sal para cada documento.

De manera similar, Brunner *et al.* [10] notaron que utilizar el mismo par de llaves para todas las transacciones también ocasiona trazabilidad, es decir, si un atacante conoce la identidad del propietario de una llave también podría conocer todas las transacciones que este ha realizado. La solución implementada por los autores consiste en utilizar un nuevo par de llaves en cada transacción, por lo cual se emplea un Monedero Determinista Jerárquico (*HD wallet*) que genera diferentes llaves a partir de un solo par.

### *C. Validación de los Documentos*

En las aplicaciones que utilizan Blockchain, la forma más común para verificar si un documento es auténtico es calcular el hash del documento que se ha recibido y compararlo con el hash que se encuentra almacenado en la cadena de bloques, si coinciden entonces se puede confirmar su autenticidad, sino el documento es falso [19]. Además, es necesario contar con un mecanismo que permita autenticar a todo aquel que emita un documento, con el fin de evitar la suplantación.

Baldi *et al.* [11] proponen el uso de certificados X.509 que enlazan la identificación del emisor a su llave pública, aunque esto requiere de una Autoridad de Certificación que centralizaría la red. Por lo que sugieren usar Identificadores Descentralizados (DID) para contrarrestar los ataques de falsificación a la vez que se mantiene la descentralización.

En [41] se tiene una estructura de datos donde se almacena la información personal del propietario, en su caso, del título académico. Esta información se encripta con la llave pública del propietario, de manera que este pueda acceder de manera segura a su información y editarla, reduciendo la interacción con terceros. También, se encripta la información del perfil con la llave pública de cada tercero que tenga autorización para verla.

Como medida de seguridad, también se pueden tener en cuenta las marcas de tiempo. Por ejemplo, en [42] se plantea añadir un criterio adicional en el que se defina un tiempo específico durante el cual se debe emitir el título para que se considere válido. Si el diploma, se emite en un tiempo diferente, el diploma no se validará a pesar de contar con una firma potencialmente válida. Esto se hace con el fin de evitar vulnerabilidades, por ejemplo, si se filtra la llave privada de un emisor.

### *D. Revocación de Documentos*

Según el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) los propietarios de los datos tienen derecho a pedir que estos sean eliminados [43]. También, las organizaciones emisoras de los documentos pueden considerar necesario revocar un documento, por ejemplo, si contiene información errónea o ha cambiado alguna condición desde que fue expedido.

Sin embargo, en la cadena de bloques no se pueden realizar modificaciones y por lo tanto tampoco se puede borrar la información que se encuentre allí registrada. Por esta razón, los investigadores han desarrollado estrategias que permitan obtener los beneficios de la cadena de bloques a la vez que se puede cumplir con este requisito.

En SPROOF [10] y Cerberus [44] cada emisor contiene dentro de la información de su perfil, una lista de revocación donde se registran las URL de los certificados que han sido revocados. Para este proceso se utilizan contratos inteligentes [44] que contienen las reglas que se deben seguir antes de añadir un certificado a la lista de revocación.

Además de esto, los autores de [45] proponen enlazar, de manera opcional, el hash del certificado con un documento en formato JSON (*JavaScript Object Notation*) que contenga información complementaria como el motivo y la fecha de revocación. Este debe almacenarse también en un recurso distribuido como IPFS para conservar la descentralización.

### *E. Ataques a la cadena de bloques*

Para garantizar la seguridad de los datos también se deben considerar los ataques informáticos que podría sufrir la cadena de bloques, de manera que se puedan establecer estrategias para evitarlos o mitigar su impacto.

En primer lugar, un atacante puede atentar contra el protocolo de consenso con el fin de alterar los datos de los bloques [20], por lo que su objetivo es conseguir la mayoría del poder de consenso, como es el caso de los ataques del 51% en los algoritmos de PoW o PoS [46] o los ataques bizantinos en el protocolo BFT donde 1/3 de los nodos de consenso adversarios pueden causar que el protocolo se interrumpa o se detenga [46]. Por esta razón, en [46] se recomienda el uso de incentivos que recompensen la participación honesta y desalienten o castiguen las violaciones del protocolo.

También han surgido propuestas para evitar los ataques del 51%, por ejemplo, Bae y Lim [47] sugieren dividir a los mineros en grupos y elegir aleatoriamente un único grupo de manera que solo los que pertenezcan a él puedan minar el siguiente bloque, con el fin de reducir las posibilidades de un ataque exitoso. Mientras que, Gupta *et al.* [48] en su investigación describieron paso a paso el proceso para implementar un protocolo de consenso híbrido basado en PoW-PoS como solución a este problema.

Un ataque similar es la minería egoísta, también llamado de retención de bloque, en el que un atacante intenta construir en forma privada una cadena secreta y revelar esta al público solo cuando la cadena honesta esté alcanzando la secreta [46]. Por la regla de la cadena más larga, la cadena secreta sería aceptada y el minero egoísta obtendría todas las recompensas. Es más factible que se presente cuando el poder de consenso del minero egoísta alcanza un umbral, por ejemplo del 30% [46]. La mayoría de los estudios realizados en torno a la minería egoísta se han enfocado en desarrollar estrategias de detección o diseños conceptuales [49], tal como el Estado de Verdad propuesto por Saad *et al.* [50] que busca identificar comportamientos de minería egoísta usando la altura de confirmación de transacción esperada y la altura de publicación del bloque.

Con un ataque Sybil también se pretende obtener el control de la red, para lo cual un nodo malicioso forja múltiples identidades a través de la virtualización [20]. Este ataque puede conducir a otros ataques como el de denegación de servicio y denegación de servicio distribuido [51], que atentan contra la disponibilidad de la información [52]. Para prevenirlo, en EduRSS [20] usaron una Blockchain de consorcio donde los miembros votan a favor o en contra de la unión de un nuevo nodo a la red. Este a su vez debe proveer información oficial que permita su identificación. Otra opción, es que cada nodo monitoree el comportamiento de los demás y verifique si algún nodo está reenviando bloques de un solo usuario en particular durante un periodo de tiempo [51].

Algo similar ocurre en un ataque de repetición, en el que un atacante logra camuflar las identidades interceptando y reproduciendo mensajes de un nodo específico [20].

También, uno de los ataques más perjudiciales para un sistema de gestión de documentos es la manipulación por colusión, en la que una transacción realizada con éxito se distribuye y se almacena en cada nodo. Sin embargo, en este caso, más de la mitad de los nodos se confabulan para manipular los datos de transacciones almacenadas en la etapa inicial de la red de Blockchain [20]. Es más factible que este se dé cuando hay pocos miembros.

## V. Conclusiones

La implementación de Blockchain en la gestión documental es un tema en el que varios autores han realizado sus aportes para reforzar los beneficios ofrecidos por esta tecnología, especialmente la seguridad de la información.

A partir de la revisión de la literatura, se puede notar que las principales preocupaciones son la protección de la confidencialidad y la construcción de sistemas robustos que puedan soportar los ataques más comunes a la cadena de bloques, como el ataque del 51% o la manipulación por colusión.

La mayor parte de los artículos analizados emplearon una Blockchain de tipo consorcio para los sistemas de gestión documental, debido a que consideran importante conocer la identidad tanto de los que emisores como de los receptores de los documentos para evitar suplantaciones.

Es importante notar que algunas soluciones de seguridad implican centralizar parcial o completamente la red, dejando de lado una de las principales características de Blockchain; es de aclarar que si bien la tecnología funciona de manera descentralizada, para aplicaciones relacionadas con la seguridad documental es necesario considerar el conjunto de involucrados con los documentos y quien debe garantizar la custodia de los mismos no sólo en términos de confidencialidad sino también legales, siendo esta la razón por la que las organizaciones deberán optar por soluciones donde se tenga la certeza de confiabilidad de quienes intervienen en el proceso, y esto se puede evidenciar al hacer énfasis en que la mayoría de Blockchain implementadas son de tipo consorcio. En cada proyecto se deben analizar las diferentes alternativas y optar por aquella que mejor se adapte a sus requisitos.

## Referencias


[1] J. Berryhill, T. Bourgery, y A. Hanson, «Blockchains Unchained: Blockchain Technology and its Use in the Public Sector», *OECD Working Papers on Public Governance*, n.º 28, 2018, doi: 10.1787/3c32c429-en.

[2] A. Grech y F. Camilleri Anthony, «Blockchain in Education», Publications Office of the European Union, EUR - Scientific and Technical Research Reports JRC108255, 2017. [En línea]. Disponible en: http://publications.jrc.ec.europa.eu/repository/handle/JRC108255

[3] T. A. Buckhoff, «Preventing Fraud by Conducting Background Checks», *The CPA Journal*, 2003. Accedido: oct. 06, 2020. [En línea]. Disponible en: http://archives.cpajournal.com/2003/1103/dept/d115203.htm

[4] J. Wang y B. H. Kleiner, «Effective employment screening practices», *Management Research News*, vol. 23, n.º 5/6, pp. 73-81, 2000, doi: 10.1108/01409170010782055.

[5] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, y P. Sarda, «Blockchain as a Notarization Service for Data Sharing with Personal Data Store», en *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 2018, pp. 1330-1335. doi: 10.1109/TrustCom/BigDataSE.2018.00183.

[6] Y. Xiao, N. Zhang, W. Lou, y Y. T. Hou, «A Survey of Distributed Consensus Protocols for Blockchain Networks», *IEEE Commun. Surv.*

*Tutorials*, vol. 22, n.º 2, pp. 1432-1465, 2020, doi: 10.1109/COMST.2020.2969706.

[7] B. Singhal, G. Dhameja, y P. S. Panda, *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Apress, 2018. [En línea]. Disponible en: https://doi.org/10.1007/978-1-4842-3444-0

[8] K. Sultan, U. Ruhi, y R. Lakhani, «Conceptualizing Blockchains: Characteristics & Applications», en *IADIS International Conference Information Systems 2018*, Lisbon, Portugal, 2018, pp. 49-57. Disponible en: https://arxiv.org/ftp/arxiv/papers/1806/1806.03693.pdf

[9] M. Sharples *et al.*, *Innovating Pedagogy 2016: Exploring new forms of teaching, learning and assessment, to guide educators and policy makers*. 2016.

[10] C. Brunner, F. Knirsch, y D. Engel, «SPROOF: A Platform for Issuing and Verifying Documents in a Public Blockchain», en *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, Prague, Czech Republic, 2019, vol. 1, pp. 15-25. doi: 10.5220/0007245600150025.

[11] M. Baldi, F. Chiaraluce, M. Kodra, y L. Spalazzi, «Security analysis of a blockchain-based protocol for the certification of academic credentials», *arXiv*, 2019.Disponible en: http://arxiv.org/abs/1910.04622

[12] «Badges and Blockcerts», *Hyland Credentials*, 2019. https://www.hylandcredentials.com/badges-and-blockcerts/

[13] T. T. Huynh, T. Tru Huynh, D. K. Pham, y A. Khoa Ngo, «Issuing and Verifying Digital Certificates with Blockchain», en *2018 International Conference on Advanced Technologies for Communications (ATC)*, Ho Chi Minh City, Vietnam, 2018, pp. 332-336. doi: 10.1109/ATC.2018.8587428.

[14] S. Chiliveri, J. Grandhi, M. Uttam Patil, L. E. P.R., y M. Ethirajan, «ProveDoc: A Blockchain Based Proof of Existence with Proof of Storage», en *2019 International Conference on Information Technology (ICIT)*, Bhubaneswar, India, 2019, pp. 239-244. doi: 10.1109/ICIT48102.2019.00049.

[15] «Connect Solutions», *Factom*. https://www.factom.com/solutions/connect

[16] B. Boeser, «Meet TrueRec by SAP: Trusted Digital Credentials Powered by Blockchain», *SAP News Center*, 2017. https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/

[17] M. Das, X. Tao, y J. C. P. Cheng, «A Secure and Distributed Construction Document Management System Using Blockchain», en *Proceedings of the 18th International Conference on Computing in Civil and Building Engineering*, São Paulo, Brazil, 2021, pp. 850-862. doi: 10.1007/978-3-030-51295-8_59.

[18] ISO/IEC, «ISO/IEC 27000:2018». 2018. [En línea]. Disponible en: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[19] V. Marella y A. Vijayan, «Document Verification using Blockchain for Trusted CV Information», presentado en Americas' Conference on Information Systems (AMCIS), Virtual conference, 2020. Disponible en:https://aisel.aisnet.org/amcis2020/adv_info_systems_research/adv_info_systems_research/12

[20] H. Li y D. Han, «EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme», *IEEE Access*, vol. 7, pp. 179273-179289, 2019, doi: 10.1109/ACCESS.2019.2956157.

[21] R. Poorni, M. Lakshmanan, y S. Bhuvaneswari, «DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts», en *2019 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2019, pp. 215-219. doi: 10.1109/ICCES45898.2019.9002576.

[22] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres, y F. Wendland, «Blockchain for Education: Lifelong Learning Passport», presentado en ERCIM-Blockchain 2018, Amsterdam, Netherlands, 2018. doi: 10.18420/blockchain2018_07.

[23] P. Pandey y R. Litoriya, «Securing and authenticating healthcare records through blockchain technology», *Cryptologia*, vol. 44, n.º 4, pp. 341-356, 2020, doi: 10.1080/01611194.2019.1706060.

[24] S. Wang, Y. Zhang, y Y. Zhang, «A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems», *IEEE Access*, vol. 6, pp. 38437-38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[25] Y.-A. de Montjoye, S. S. Wang, y A. (Sandy) Pentland, «On the Trusted Use of Large-Scale Personal Data», *IEEE Data Engineering Bulletin*, vol. 35, n.º 4, pp. 5-8, 2012.

[26] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, y M. H. Rehman, «Decentralized document version control using ethereum blockchain and IPFS», *Computers & Electrical Engineering*, vol. 76, pp. 183-197, 2019, doi: 10.1016/j.compeleceng.2019.03.014.

[27] P. Tsankov, A. Dan, D. D. Cohen, A. Gervais, F. Buenzli, y M. Vechev, «Securify: Practical Security Analysis of Smart Contracts», *arXiv:1806.01143 [cs]*, 2018, Accedido: ene. 14, 2021. [En línea]. Disponible en: http://arxiv.org/abs/1806.01143

[28] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, y A. Hobor, «Making Smart Contracts Smarter», en *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 2016, pp. 254-269. doi: 10.1145/2976749.2978309.

[29] S. Şahan, A. F. Ekici, y Ş. Bahtiyar, «A Multi-Factor Authentication Framework for Secure Access to Blockchain», en *Proceedings of the 2019 5th International Conference on Computer and Technology Applications*, Istanbul, Turkey, 2019, pp. 160-164. doi: 10.1145/3323933.3324083.

[30] D. Berdik, S. Otoum, N. Schmidt, D. Porter, y Y. Jararweh, «A Survey on Blockchain for Information Systems Management and Security», *Information Processing & Management*, vol. 58, n.º 1, p. 102397, 2021, doi: 10.1016/j.ipm.2020.102397.

[31] C. Xu, H. Yang, Q. Yu, y Z. Li, «Trusted and Flexible Electronic Certificate Catalog Sharing System Based on Consortium Blockchain», en *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2019, pp. 1237-1242. doi: 10.1109/ICCC47050.2019.9064284.

[32] Z. Xiao *et al.*, «EMRShare: A Cross-Organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain», en *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, Singapore, 2018, pp. 998-1003. doi: 10.1109/PADSW.2018.8645049.

[33] P. Zhang, J. White, D. C. Schmidt, G. Lenz, y S. T. Rosenbloom, «FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data», *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267-278, 2018, doi: 10.1016/j.csbj.2018.07.004.

[34] S. Shamshad, Minahil, K. Mahmood, S. Kumari, y C.-M. Chen, «A secure blockchain-based e-health records storage and sharing scheme», *Journal of Information Security and Applications*, vol. 55, p. 102590, 2020, doi: 10.1016/j.jisa.2020.102590.

[35] H.-A. Lee *et al.*, «An Architecture and Management Platform for Blockchain-Based Personal Health Record Exchange: Development and Usability Study», *Journal of Medical Internet Research*, vol. 22, n.º 6, p. e16748, 2020, doi: 10.2196/16748.

[36] H. Kumar *et al.*, «Rainbow table to crack password using MD5 hashing algorithm», en *2013 IEEE Conference on Information Communication Technologies*, 2013, pp. 433-439. doi: 10.1109/CICT.2013.6558135.

[37] J. Bethencourt, A. Sahai, y B. Waters, «Ciphertext-Policy Attribute-Based Encryption», en *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA, USA, 2007, pp. 321-334. doi: 10.1109/SP.2007.11.

[38] T. Chen, Y. Yu, y Z. Duan, «Data Access Sharing Approach for Trade Documentations Based on Blockchain Technology», en *2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE)*, Xiamen, China, 2019, pp. 1732-1736. doi: 10.1109/EITCE47263.2019.9095045.

[39] C. Yuan, M. Xu, X. Si, y B. Li, «Blockchain with Accountable CP-ABE: How to Effectively Protect the Electronic Documents», en *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, Shenzhen, China, 2017, pp. 800-803. doi: 10.1109/ICPADS.2017.00111.

[40] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, y M. Guizani, «BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records», en *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, 2018, pp. 1-6. doi: 10.1109/GLOCOM.2018.8647713.

[41] C. BouSaba y E. Anderson, «Degree Validation Application Using Solidity and Ethereum Blockchain», en *2019 SoutheastCon*, Huntsville, AL, USA, 2019, pp. 1-5. doi: 10.1109/SoutheastCon42311.2019.9020503.

[42] F. Schär y F. Mösli, «Blockchain Diplomas: Using Smart Contracts to Secure Academic Credentials», *Beiträge zur Hochschulforschung*, vol. 41, pp. 48-58, 2019.

[43] Parlamento Europeo y Consejo de la Unión Europea, «REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - (Reglamento general de protección de datos)». 2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679

[44] A. Tariq, H. B. Haq, y S. T. Ali, «Cerberus: A Blockchain-Based Accreditation and Degree Verification System», *arXiv:1912.06812 [cs]*, 2019, Accedido: ene. 04, 2021. [En línea]. Disponible en: http://arxiv.org/abs/1912.06812

[45] F. R. Vidal, F. Gouveia, y C. Soares, «Revocation Mechanisms for Academic Certificates Stored on a Blockchain», en *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, Sevilla, Spain, 2020, pp. 1-6. doi: 10.23919/CISTI49556.2020.9141088.

[46] I. Homoliak, S. Venugopalan, Q. Hum, y P. Szalachowski, «A Security Reference Architecture for Blockchains», en *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 390-397. doi: 10.1109/Blockchain.2019.00060.

[47] J. Bae y H. Lim, «Random Mining Group Selection to Prevent 51% Attacks on Bitcoin», en *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Luxembourg City, Luxembourg, 2018, pp. 81-82. doi: 10.1109/DSN-W.2018.00040.

[48] M. Gupta, *Blockchain For Dummies®, 3rd IBM Limited Edition*, Third. Hoboken, NJ: John Wiley & Sons, Inc., 2020. [En línea]. Disponible en: https://www.ibm.com/downloads/cas/OK5M0E49

[49] K. Nicolas, Y. Wang, y G. C. Giakos, «Comprehensive Overview of Selfish Mining and Double Spending Attack Countermeasures», en *2019 IEEE 40th Sarnoff Symposium*, Newark, NJ, USA, 2019, pp. 1-6. doi: 10.1109/Sarnoff47838.2019.9067821.

[50] M. Saad, L. Njilla, C. Kamhoua, y A. Mohaisen, «Countering Selfish Mining in Blockchains», en *2019 International Conference on Computing, Networking and Communications (ICNC)*, Honolulu, HI, USA, 2019, pp. 360-364. doi: 10.1109/ICCNC.2019.8685577.

[51] P. Swathi, C. Modi, y D. Patel, «Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners», en *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, 2019, pp. 1-6. doi: 10.1109/ICCCNT45670.2019.8944507.

[52] L. Liu y B. Xu, «Research on information security technology based on blockchain», en *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, Chengdu, China, 2018, pp. 380-384. doi: 10.1109/ICCCBDA.2018.8386546.

[53] Güler, Kenan & Salihoğlu, Esengül & Öztürk, Emre & Pala, Osman. (2022). Blockchain in International Trade Documents Management Using NAHP Technique: Case of Kapikule and Istanbul Border Customs. 10.4018/978-1-6684-5876-1.ch019.

[54] P. Soares, R. Saraiva, I. Fernandes, A. Neto and J. Souza, "A Blockchain-based Customizable Document Registration Service for Third Parties," 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Shanghai, China, 2022, pp. 1-2, doi: 10.1109/ICBC54727.2022.9805500.

[55] Wu, Haitao (57205511865); Zhang, Pan (57730159800); Li, Heng (8692514900); Zhong, Botao (23975246400); Fung, Ivan W. H. (7006797603); Lee, Yiu Yin Raymond. Blockchain Technology in the Construction Industry: Current Status, Challenges, and Future Directions (2022) Journal of Construction Engineering and Management, 148 (10). DOI: 10.1061/(ASCE)CO.1943-7862.0002380. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85135183795&doi=10.1061%2f%28ASCE%29CO.1943-7862.0002380&partnerID=40&md5=6819321e3e875d7d6f8029166298f2ba

[56] A. Rustemi, V. Atanasovski, A. Risteski and P. Latkoski, "Challenges of Blockchain in Higher Education Institutions for Protection Against Diploma Forgery," 2023 International Balkan Conference on Communications and Networking (BalkanCom), İstanbul, Turkiye, 2023, pp. 1-6, doi: 10.1109/BalkanCom58402.2023.10167986.

**Jonatan Gutiérrez.** Ingeniero de sistemas y computación. Área de desempeño: Seguridad informática, perteneciente al grupo de investigación Nyquist de la Universidad Tecnológica de Pereira. Institución a la que pertenece: Holding Digital.com S.A.S. Pereira, Colombia.

**Paula Andrea Villa Sánchez.** Ingeniero de sistemas y computación. Especialista en redes de datos. Magíster en Ingeniería de sistemas y computación. Área de desempeño: División de proyectos. Institución a la que pertenece: Holding Digital.com S.A.S. Pereira, Colombia.

**Ana María López Echeverry.** Ingeniera electricista. Especialista en Telecomunicaciones. Magíster en Ingeniería. Área de desempeño: Redes y Comunicaciones y seguridad de la información. perteneciente al grupo de investigación Nyquist de la Universidad Tecnológica de Pereira. Pereira, Colombia.
ORCID: https://orcid.org/0000-0002-4589-9262.