

Exégesis crítica en la aplicación blockchain en la seguridad de la información en diversos sectores

Critical exegesis on the application of blockchain in information security across various sectors

Recibido: octubre 13 de 2024 | Revisado: noviembre 07 de 2024 | Aceptado: diciembre 03 de 2024

DOMINICK REVILLA¹
DIEGO RODRÍGUEZ¹
ALBERTO MENDOZA DE LOS SANTOS¹

RESUMEN

En la actualidad, la protección de la información se ha convertido en una necesidad indispensable y omnipresente. En este contexto, la tecnología blockchain ha surgido como una solución disruptiva, generando un impacto significativo gracias a su estructura descentralizada y su capacidad para proporcionar un registro inmutable y transparente de las transacciones. Este artículo tiene como objetivo analizar cómo el blockchain ha sido implementado exitosamente para proteger datos sensibles, abarcando desde aplicaciones financieras hasta la gestión de registros médicos, mediante una revisión sistemática de la información recopilada entre los años 2018 y 2024. El estudio ofrece una visión integral y actualizada sobre cómo esta tecnología está transformando la seguridad de la información, destacando su creciente relevancia en un entorno digital cada vez más vulnerable a las amenazas cibernéticas.

Palabras clave: Cadena de bloques, integridad de datos, seguridad de información, privacidad

ABSTRACT

Nowadays, the protection of information has become an indispensable and omnipresent need. In this context, blockchain technology has emerged as a disruptive solution, generating a significant impact thanks to its decentralized structure and its ability to provide an immutable and transparent record of transactions. This article aims to analyze how blockchain has been successfully implemented to protect sensitive data, ranging from financial applications to medical records management, through a systematic review of information collected between the years 2018 and 2024. The study offers a comprehensive and updated vision of how this technology is transforming information security, highlighting its growing relevance in a digital environment that is increasingly vulnerable to cyber threats.

Keywords: Blockchain, data integrity, security information, privacy

¹ Universidad Nacional de Trujillo,
Trujillo, Perú

Autor de correspondencia:
t1523300121@unitru.edu.pe

© Los autores. Este artículo es publicado por la Revista Campus de la Facultad de Ingeniería y Arquitectura de la Universidad de San Martín de Porres. Este artículo se distribuye en los términos de la Licencia Creative Commons Atribución No-Comercial – Compartir-Igual 4.0 Internacional (<https://creativecommons.org/licenses/by/4.0/>), que permite el uso no comercial, distribución y reproducción en cualquier medio siempre que la obra original sea debidamente citada. Para uso comercial contactar a: revistacampus@usmp.pe.

<https://>

Introducción

Hoy en día vivimos en una era digital en la cual el flujo de información es demasiado constante y masivo, lo que da paso a que la seguridad de los datos se convierta en un recurso de alto valor para entidades o empresas de cada sector. Esta tendencia a almacenar y salvaguardar información nos obliga a tener dependencia de los sistemas tecnológicos y a la conectividad global; por lo que mantener la seguridad de datos sensibles ya no es opcional, es decir, se ha convertido en una obligación esencial para asegurar la continuidad operativa, la imagen corporativa y el acatamiento de las normativas legales.

En la última década, la seguridad de la información ha pasado por una evolución significativa, ampliándose más allá de la seguridad informática básica para abarcar un enfoque más global conocido como seguridad de la información. Según Carvajal (2020), este concepto incluye la ciberseguridad y otros aspectos de la protección de datos, cubriendo cada etapa del manejo de información, como su uso, almacenamiento y transferencia. Las organizaciones han empezado a comprender que la ciberseguridad es solo una parte de un enfoque más amplio, que abarca la protección integral de la información.

Los avances han llevado a la creación de nuevos sistemas de control que permiten monitorear la información de manera más precisa y reaccionar frente a potenciales vulnerabilidades. Paralelamente, existen otras ventanas accesibles para todo el mundo que se han convertido en canales importantes para descifrar patrones de acceso y

comportamiento de los usuarios, lo que conlleva a surgir riesgos, totalmente nuevos, para la seguridad de la información. Tejada Berrio (2021) nos dice que los datos tanto personales como empresariales están cada vez más expuestos a amenazas, y esto ha llevado a la implementación de legislaciones y estándares que obligan a las organizaciones a protegerse de intentos de robo de información que ellos manejan.

A nivel internacional, las normas ISO 27001, entre otras, han sido adoptadas ampliamente para asegurar que las organizaciones gestionen, adecuadamente, los riesgos generados comúnmente por la digitalización de información, protegiendo los activos más valiosos de la empresa, incluyendo los datos personales.

El block-chain es una tecnología que permite sincronizar transacciones o datos para proteger información de forma segura, descentralizada e inmutable. Surgió en 2008 como la base en el funcionamiento de la criptomoneda Bitcoin, propuesta por Satoshi Nakamoto. Desde entonces, ha evolucionado hasta convertirse en un instrumento tecnológico importante para salvaguardar la información en distintos sectores. Según Tapscott & Tapscott (2016), la principal característica del block-chain es su capacidad para registrar datos en bloques interconectados mediante criptografía, lo que asegura que la información no pueda ser alterada sin el consenso de todos los participantes en la red.

Con el tiempo, esta tecnología ha superado su uso inicial en las

criptomonedas, expandiéndose hacia áreas que requieren altos niveles de protección de datos. Todo empezó en el sistema financiero. Su uso fue evolucionando llegando a ser una herramienta fundamental para incrementar la transparencia y la protección de las transacciones electrónicas. Nakamoto (2008), menciona que cada operación registrada en block-chain queda verificada y no puede ser alterada, lo que ayuda a disminuir el riesgo de estafas o fraudes y asegura la integridad de los movimientos financieros. De este modo, las instituciones financieras han adoptado esta tecnología para fortalecer la confianza en sus sistemas y realizar auditorías en tiempo real.

Para Patel (2021), en el sector de la salud, el block-chain se utiliza para proteger datos sensibles, como los historiales médicos. Al almacenar esta información en una cadena de bloques, se garantiza que solo los profesionales autorizados tengan acceso a ella, lo que ayuda a mantener la confianza de los pacientes. Esta tecnología no solo evita alteraciones en los registros médicos, sino que también facilita el intercambio seguro de información entre instituciones de salud. Así, la aplicación del block-chain en este ámbito ha mejorado el manejo de información personal y el tipo de atención médica.

En resumen, el block-chain tiene estructura descentralizada y su capacidad para asegurar la autenticidad manteniendo la integridad de los datos lo ha hecho ideal para proteger transacciones financieras, historiales médicos y procesos logísticos.

Método

En la presente revisión sistemática se optó por aplicar la metodología Prisma (Preferred Reporting Items for Systematic Review and Meta-Analyses).

Para el proceso de revisión se estableció el siguiente planteamiento: ¿Cómo ha impactado en los últimos seis años la implementación de la tecnología blockchain como seguridad de la información en diversos sectores?

Según (Moer et al, 2009) Prisma logra que el autor haga un análisis profundo ya que le ofrece pautas claras para desarrollar revisiones sistemáticas.

De manera que Moreno *et al.* (2018), una revisión sistemática consiste en un compendio organizado y detallado de la información existente con el propósito de resolver una pregunta particular, destacándose por exponer de manera clara y accesible los pasos seguidos en su elaboración.

De acuerdo a lo propuesto por Moreno *et al.* (2018), la elaboración de una revisión sistemática sigue una serie de etapas: formulación de una pregunta estructurada, búsqueda en bases de datos, selección de documentos relevantes, recopilación de información, evaluación crítica y análisis estadístico de los datos obtenidos, culminando con la presentación de los hallazgos.

En relación con la búsqueda de información, identificamos las palabras clave pertinentes para nuestro tema de investigación, que incluyen: “cadena de

bloques”, “Seguridad de la información” y “Integridad de datos”. Posteriormente, además de identificar estos términos, también se consideraron sus traducciones al inglés y sinónimos correspondientes.

La selección de términos en español utilizada en la búsqueda fue la siguiente: [(“Seguridad de la información”) AND ((“Cadena de bloques”) AND ((“Integridad de datos”))]. La selección de términos en inglés empleada fue: [(“Information Security”) AND ((Blockchain) OR (“Block-Chain”)) AND (“data integrity”)].

A continuación, se utilizaron las palabras clave mencionadas en bases de datos como Scopus, IEEE Xplore, SciELO y Google Académico. Para llevar a cabo esta investigación, se establecieron parámetros específicos, como el considerar solo publicaciones desde el 2018 al 2024, con el fin de analizar el

impacto actual del avance tecnología.

Resultados

Para obtener resultados exactos en la búsqueda de la literatura a revisar, utilizamos criterios de exclusión como: No contiene palabras claves, no guardan relación el blockchain y con la seguridad de información y por duplicidad. Por parte de los criterios de inclusión tomamos en cuenta que las publicaciones deben estar comprendidas entre los últimos seis años y que estén en inglés y español.

El número de publicaciones encontradas según los criterios antes mencionados fueron en total 158 artículos obtenidos de la siguiente forma: Google Académico, 43 artículos; SciELO, 15 artículos; Scopus, 69 artículos y IEEE: 31 artículos.

Figura 1
Resultados por tipo de base de datos

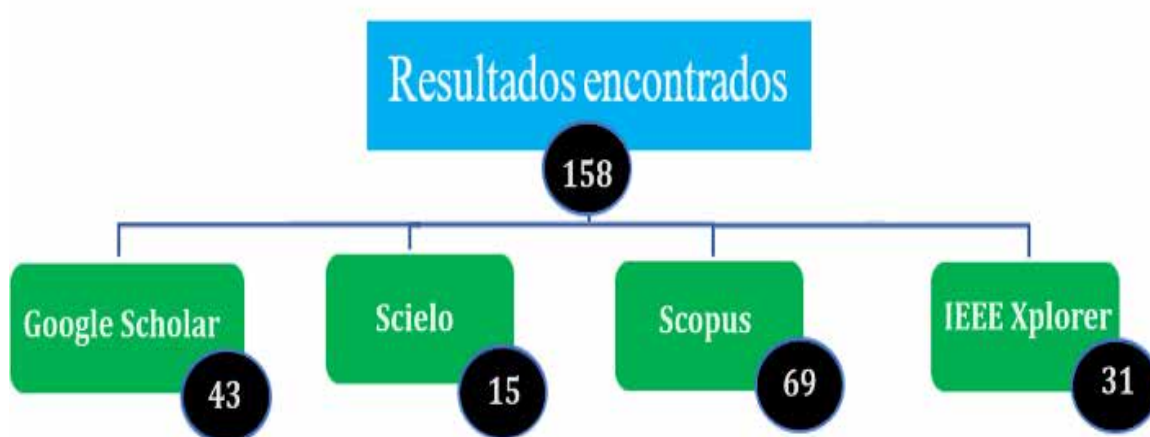


Figura 2

Flujograma del proceso de selección de artículos

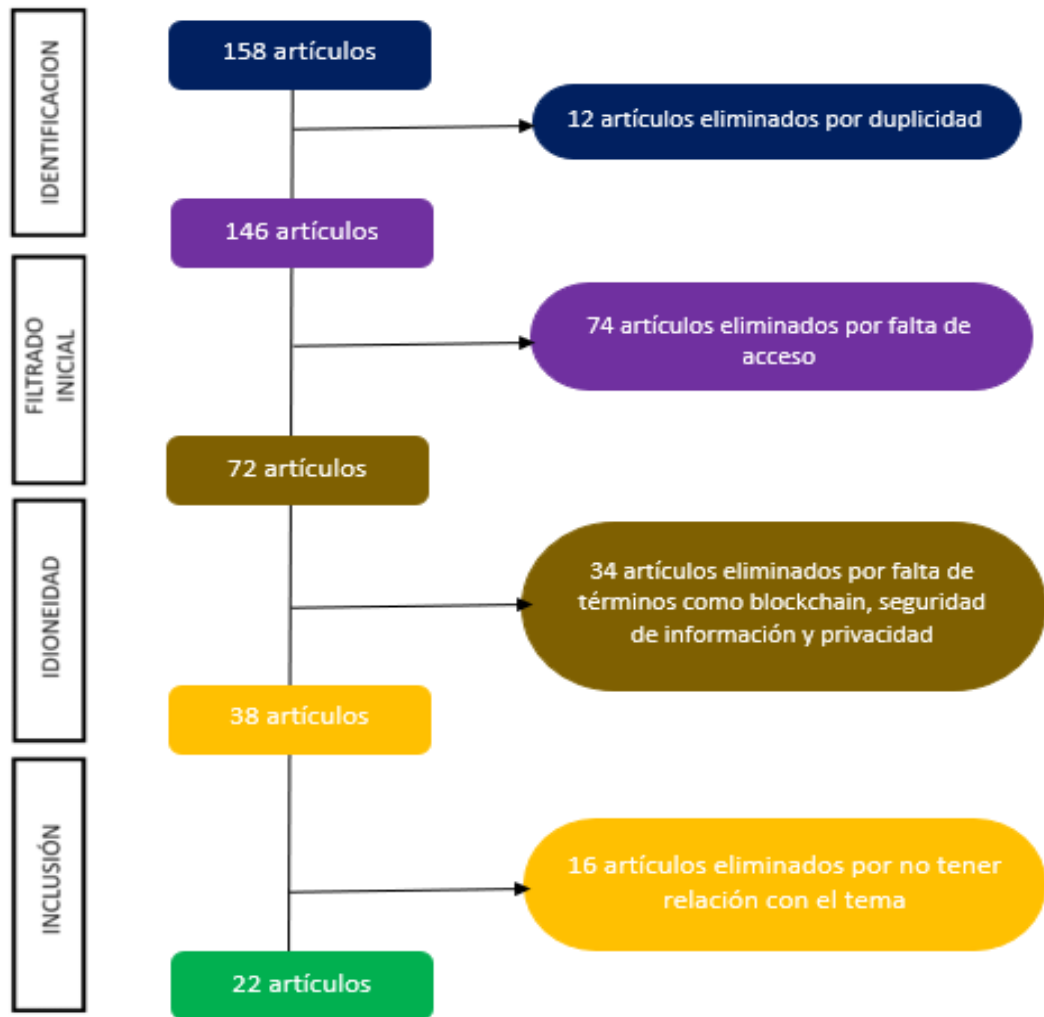


Figura 3

Gráfico de concurrencia

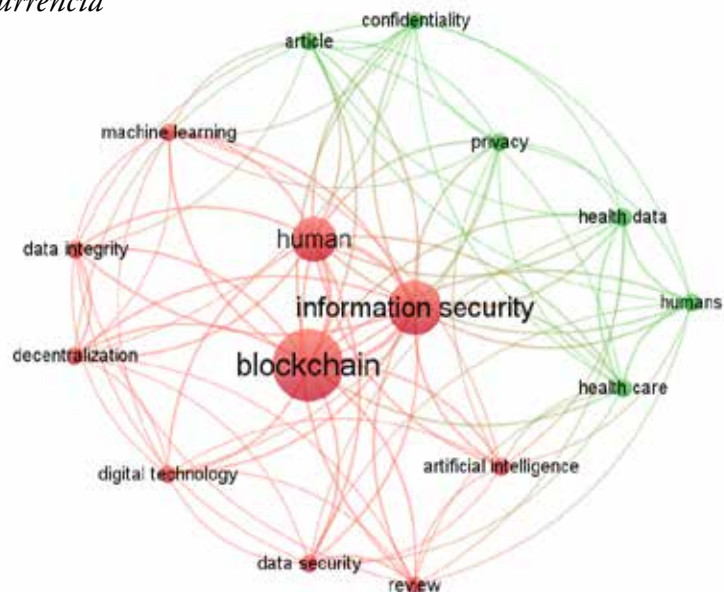


Tabla 1
Exégesis crítica en la aplicación Blockchain en la Seguridad de la Información de diversos sectores

Id	Titulo	Autores	Año	Sector
1	El impacto del Blockchain en la cadena de suministros de la industria agropecuaria	Burgos Rojas, M. A., Haro Polo, C. I., & Mendoza de los Santos, A. C.	2022	Cadena de Suministro
2	Explorando los principales Atributos de Blockchain para la protección de Datos médicos	Reyes Riveros, A. J., Cárdenas Iglesias, J. M., & Mendoza de los Santos, A. C.	2024	Salud
3	The Health Care Sector's Experience of Blockchain:	Yeung, K.	2021	Salud
4	A blockchain framework for patient-centered health records and exchange	Hylock, R. H., & Zeng, X.	2019	Salud
5	A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain.	Qin, Q., Jin, B., & Liu, Y.	2021	Salud
6	Ensuring data integrity of healthcare information in the era of digital health.	Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., Kumar, R., & Khan, R. A.	2021	Salud
7	Improving Diagnosis through Digital Pathology	Subramanian, H., & Subramanian, S.	2022	Salud
8	A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage	Y. Zhang, H. Geng, L. Su and L. Lu,	2022	Almacenamiento en la nube
9	Blockchain Technology in Education.	Machado, A., Sousa, M., & Rocha, Á.	2020	Educación
10	Research on the Application of Blockchain Technology in Education and Teaching in Higher Vocational Colleges	Yin, X., Yu, Y., Hu, B., Luo, Q., & Tang, Z.	2022	Educación
11	Blockchain-Based Caching Architecture for DApp Data Security and Delivery	Kim, D., & Park, S.	2024	Aplicaciones Descentralizadas
12	Blockchain Driven Access Control Mechanisms, Models and Frameworks	Bashir Dar, A., Hamid Lone, A., Naaz, R., Iqbal Baba, A., & Wu, F.	2022	Internet de las cosas
13	Blockchain and IPFS Integrated Framework in Bilevel Fog-Cloud Network for Security and Privacy of IoMT Devices	Mehbodniya, A., Neware, R., Vyas, S., Kumar, M. R., Ngu-lube, P., & Ray, S.	2021	Internet de las cosas
14	Revamped Dual-key Stealth Address Protocol for IoT Using Encryption and Decentralized Storage.	Odoom, J., Xiaofang, H., Danso, S. A., Soglo, R. S., & Nyarko, B. N. E.	2023	Internet de las cosas

15	Blockchain Based Public Cloud Security for E-Voting System on IoT Environment	Vijaya Kumar, A., Sarvani, G. V., & Satya, D.	2020	Internet de las cosas
16	BBTCD: blockchain based traceability of counterfeited drugs.	Rai, B. K.	2022	Industria farmacéutica
17	Blockchain for Data Originality in Pharma Manufacturing	Durá, M., Leal, F., Sánchez-García, Á., Sáez, C., García-Gómez, J. M., Chis, A. E., & González-Vélez, H.	2023	Industria farmacéutica
18	A Blockchain Secured Pharmaceutical Distribution System to Fight Counterfeiting	Zoughalian, K., Marchang, J., & Ghita, B.	2022	Industria farmacéutica
19	Project data categorization, adoption factors, and non-functional requirements for blockchain based digital twins in the construction industry 4.0.	Teisserenc, B., & Sepasgozar, S.	2021	Construcción / Industria 4.0
20	New Blockchain Based Special Keys Security Model with Path Compression Algorithm for Big Data	Bakir, C.	2022	Big data
21	Blockchain technology based information classification management service	Hong, G. W., Kim, J. W., & Chang, H.	2021	Big data
22	Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain	Zhao, Y., Li, Q., Yi, W., & Xiong, H.	2023	Agricultura

Cadena de suministro

Según Burgos *et al.* (2022) en una industria de fresas en Zhejiang, tras cuatro años operando sin un sistema de gestión y control de datos, se optó por implementar Blockchain para asegurar la veracidad de la información utilizada y monitorear en todo momento el recorrido de los datos a lo largo de la cadena de suministro, identificando quién los generó, así como el lugar y momento de su creación.

Salud

Reyes *et al.* (2024) concluyen que existen cuatro pilares fundamentales

en la preservación y seguridad de la información médica: el control de accesos, la privacidad de datos, la seguridad de datos y la encriptación.

Según Yeung (2021), las tecnologías blockchain en el sector sanitario han demostrado potencial en la gestión de datos y la privacidad de los pacientes, permitiendo un intercambio seguro y automatización de la trazabilidad. Sin embargo, los autores subrayan que la adopción a gran escala enfrenta desafíos técnicos y organizacionales, como la interoperabilidad y la confianza social. Aunque las aplicaciones en áreas no clínicas como la gestión administrativa han mostrado cierto éxito, los avances

en el uso clínico aún son incipientes. El futuro de blockchain en la salud dependerá de superar estos desafíos y lograr una implementación que ofrezca valor agregado frente a alternativas más tradicionales.

Hylock & Zeng (2019), describen cómo blockchain puede transformar la manera en que se acceden y comparten los datos de los pacientes, permitiendo a los individuos tener mayor control sobre su información médica. Al emplear estándares de interoperabilidad y contratos inteligentes, se propone que los pacientes puedan gestionar quién tiene acceso a sus registros médicos, mejorando tanto la seguridad como la privacidad en la atención médica. Este enfoque refleja un avance significativo hacia atender las necesidades, preferencias y valores individuales de cada paciente, aunque su éxito dependerá de la adopción y colaboración entre instituciones que, actualmente, tienen prácticas muy fragmentadas.

Según la propuesta de Qin *et al.* (2021), el consorcio blockchain para gestionar los registros médicos de accidentes cerebrovasculares, abordando la necesidad de intercambiar datos médicos de manera segura y eficiente entre hospitales. El uso de mecanismos como el encriptado proxy y el cifrado buscable asegura dos aspectos claves para el manejo de información: privacidad e integridad, en este caso de datos médicos, haciendo que el intercambio entre instituciones sea más seguro y confiable. Este caso demuestra, claramente, cómo blockchain puede mejorar la gestión de enfermedades críticas, permitiendo que los tratamientos se optimicen con acceso rápido y seguro a los datos. Sin embargo,

el alto costo de estas soluciones podría ser una barrera para su adopción.

En el sector salud, Zarour *et al.* (2021), refieren al uso de blockchain con el enfoque en garantizar la integridad de los datos médicos. La tecnología proporciona una forma segura y eficiente de gestionar y proteger los datos de los pacientes, reduciendo el riesgo de manipulación y brechas de seguridad. Blockchain ofrece un enfoque descentralizado que fortalece la confianza en la información médica. Nuestra perspectiva es que este uso es esencial en un mundo donde la protección de datos personales se vuelve cada vez más importante; sin embargo, la integración de blockchain en sistemas de salud puede encontrar resistencia debido a su complejidad.

De acuerdo con Subramanian & Subramanian (2022), el blockchain se aplica al sector salud, específicamente, en la gestión de la patología digital. Utilizando contratos inteligentes y almacenamiento descentralizado (IPFS), se busca mejorar la eficiencia y seguridad en el almacenamiento y transmisión de imágenes médicas de alta resolución, reduciendo costos y mejorando la accesibilidad al diagnóstico remoto. Consideramos que el uso de blockchain en este ámbito tiene un gran potencial para hacer que la atención médica sea más eficiente y accesible; sin embargo, la adopción generalizada sigue siendo un desafío debido a las barreras técnicas y de infraestructura.

Almacenamiento Cloud

El servicio de almacenamiento en la nube nace como una alternativa a los métodos de almacenamiento tradicionales.

El almacenamiento en la nube ofrece la capacidad de almacenar y acceder a grandes volúmenes de datos, lo que disminuye los costos de gestión para los usuarios que manejan grandes cantidades de información.

En su artículo, Y. Zhang *et al* (2022), proponen implementar un esquema de verificación de integridad de datos, que en comparación con ciertos métodos basados en TPA (auditores), será implementado usando tecnología Blockchain consiguiendo servicios de verificación de integridad más difíciles de manipular

Educación

Según Manchado *et al.* (2020), el uso de tecnologías blockchain se utiliza en la evaluación formativa, específicamente, en la obtención de diplomas. Sin embargo, también se emplean en el diseño e implementación de actividades de aprendizaje y en el seguimiento de todos los procesos de manera distribuida.

Asimismo, Yin *et al.* (2022) mencionan que las aplicaciones que emplean blockchain en la educación proponen implementar un sistema de big data de información y aprendizaje con el fin de que los estudiantes y profesores quienes son los principales usuarios se conviertan en beneficiarios de los recursos e información didáctica.

Aplicaciones descentralizadas

Según Kim & Park (2024), las aplicaciones descentralizadas tradicionales enfrentan problemas de rendimiento, especialmente, en términos

de latencia debido a las restricciones en la entrada/salida de datos fuera de la cadena. Para solucionar esto, los autores proponen una arquitectura de caché basada en nodos de blockchain, lo que reduce la latencia en más del 89% y mejora el rendimiento al tiempo que asegura la integridad de los datos mediante valores hash y un cifrado basado en atributos que protege el acceso no autorizado. Actualmente, estas aplicaciones se utilizan en sectores como los servicios financieros para proteger transacciones, el Internet de las Cosas para gestionar datos distribuidos, la atención médica para garantizar la seguridad de los registros médicos, y la gestión de derechos digitales para asegurar la autenticidad de la información, mejorando la privacidad y seguridad en entornos sensibles.

Internet de las cosas

Según Bashir Dar *et al.* (2022), las tecnologías blockchain han demostrado ser superiores a los sistemas de control de acceso tradicionales en sectores como el IoT y el cuidado de la salud, donde se requiere una mayor seguridad y privacidad para el acceso a los datos. Al integrar contratos inteligentes y control de acceso en base a atributos, blockchain ofrece una trazabilidad y la descentralización, eliminando intermediarios y reduciendo el riesgo de manipulaciones o accesos no autorizados. Estos avances son esenciales en áreas donde la confianza en la autenticidad de los datos es crucial, como en la gestión de registros médicos electrónicos y la seguridad de dispositivos IoT.

Según Mehbodniya *et al.* (2021), el uso de un marco integrado de blockchain e IPFS en una red de nube

de dos niveles para dispositivos IoT tiene como objetivo mejorar mantener la privacidad de los datos, especialmente, dentro del ámbito del Internet de las Cosas Médicas (IoMT). Este enfoque asegura que los datos médicos sensibles sean almacenados y transmitidos de manera eficiente, utilizando una estructura descentralizada para evitar la vulnerabilidad a ataques y asegurando la autenticación de dispositivos y la protección de la privacidad del paciente. Este marco se implementa en niveles de borde, niebla y nube, mejorando la escalabilidad y optimización de recursos, lo cual es crucial en escenarios de atención médica en tiempo real, como el seguimiento remoto de pacientes. Las transacciones entre dispositivos IoMT se aseguran mediante contratos inteligentes, que garantizan la autenticidad y verificación de no repudio.

Odoom *et al.* (2023), se enfocan en la tecnología IoT y las aplicaciones descentralizadas, proponiendo un protocolo que utiliza blockchain para mejorar la privacidad y seguridad en el manejo de transacciones. El sistema emplea direcciones sigilosas y almacenamiento descentralizado, lo que asegura que las transacciones realizadas a través de IoT sean más seguras y confidenciales. Por ello, este protocolo aborda con éxito problemas críticos de privacidad en el IoT, aunque su complejidad técnica podría limitar su adopción a corto plazo.

Vijaya Kumar *et al.* (2020), tratan sobre la aplicación de blockchain en sistemas de votación electrónica dentro del ámbito de la tecnología IoT. Blockchain garantiza que los votos sean almacenados de manera segura y que

no se puedan manipular, utilizando un enfoque de doble autenticación y encriptación. Por lo tanto, creemos que el uso de blockchain en votaciones electrónicas es fundamental para asegurar la integridad de los sistemas democráticos, especialmente, en contextos donde la seguridad del voto es un tema sensible; sin embargo, la infraestructura necesaria puede ser una barrera en países en desarrollo y el nuestro no está preparado para ello.

Industria farmacéutica

Según Rai *et al.* (2023), la trazabilidad de medicamentos falsificados es un problema crítico en la cadena de suministro farmacéutica debido a la falta de transparencia y la posibilidad de manipulación de los datos. Para abordar esto, los autores proponen una solución utilizando blockchain con contratos inteligentes y almacenamiento en IPFS para prevenir la integridad de los datos y permitir un seguimiento descentralizado de los medicamentos en toda la cadena de suministro. Esta aplicación de blockchain mejora la seguridad, privacidad y trazabilidad de los medicamentos, lo que es especialmente útil en sectores como la atención médica, donde es crucial garantizar la autenticidad de los productos. Además, tecnologías como Ethereum y contratos inteligentes permiten intercambios eficientes y seguros entre las partes involucradas, eliminando la necesidad de intermediarios y reduciendo el riesgo de falsificaciones.

Durá *et al.* (2023), refieren al blockchain en un ámbito farmacéutico que es utilizado para garantizar la integridad y originalidad de los datos

en la fabricación de medicamentos. Esto se logra mediante el uso de una red privada de blockchain y contratos inteligentes, que permiten rastrear y verificar la autenticidad de los datos a lo largo del proceso de fabricación. Con ello podemos decir que mejora la transparencia y la trazabilidad, esenciales para combatir la falsificación de medicamentos. Consideramos que esta tecnología puede revolucionar la cadena de suministro farmacéutica al garantizar la seguridad de los productos, aunque su implementación dependerá de la disposición de las empresas para adoptar nuevas tecnologías.

Para Zoughalian *et al.* (2022), el blockchain se utiliza para combatir la falsificación de medicamentos a través de un sistema de distribución seguro. El uso de pruebas de conocimiento cero y modelos de reputación asegura que los medicamentos distribuidos sean auténticos y que todas las transacciones dentro de la cadena de suministro sean rastreables y verificables. Interpretamos que el sistema ofrece una solución sólida al problema global de la falsificación de medicamentos, aunque su implementación en mercados menos regulados podría presentar desafíos.

Construcción / Industria 4.0

Según Teisserenc *et al.* (2021), las tecnologías de blockchain y los gemelos digitales son clave para la Industria de la Construcción 4.0, permitiendo una mayor eficiencia, colaboración y sostenibilidad a través de la digitalización de los procesos. Los gemelos digitales, replicas virtuales de activos físicos, mejoran la trazabilidad y seguridad de todos los datos en cada una de las etapas

en el proyecto, y el uso de blockchain asegura la integridad y confianza en la cadena de valor. Esta tecnología, aplicada a la construcción da acceso a una mejor administración de los recursos, así como la automatización de procesos mediante contratos inteligentes. Los sectores donde estas tecnologías tienen un impacto más evidente incluyen la gestión de residuos, la gestión de energía en edificios inteligentes, y la infraestructura urbana contribuyendo a la economía circular y la sostenibilidad ambiental.

Big Data

El análisis de Bakir (2022), propone un nuevo modelo de seguridad para big data usando blockchain y un algoritmo de compresión de rutas. Este enfoque permite gestionar grandes cantidades de información y mantenerla segura, asegurando la multidimensionalidad de la seguridad de información. Este modelo es útil en campos que generan grandes volúmenes de datos, como las redes sociales y la medicina. Consideramos que su contribución a la eficiencia del manejo de datos es significativa, pero la implementación de este modelo en big data podría verse limitada por su complejidad.

Hong *et al.* (2021), proponen el uso de blockchain para clasificar y proteger grandes volúmenes de datos. El sistema asegura la integridad de los datos a través de un libro mayor distribuido, lo que permite una gestión de la seguridad más económica y eficiente. Blockchain, en este caso, reduce los costos al ofrecer un enfoque unificado de seguridad. Considero que esta aplicación es, particularmente, útil en

la gestión de datos a gran escala, aunque su implementación puede estar limitada por la infraestructura tecnológica de las organizaciones.

Agricultura

Zhao *et al.* (2023), presentan el uso de blockchain para optimizar el almacenamiento de datos en el IoT agrícola. Mediante el uso de un árbol de Merkle ordenado y un método de escritura por lotes, se mejora la eficiencia y seguridad en el almacenamiento y manejo de grandes cantidades de datos. Blockchain asegura la trazabilidad y autenticidad de los datos agrícolas, mejorando la confianza en los sistemas de trazabilidad alimentaria. Este enfoque es innovador y necesario en el contexto agrícola actual, donde la seguridad y calidad de los productos son fundamentales; sin embargo, la adopción dependerá de la capacitación de los productores en el uso de estas tecnologías.

Discusión

Según lo visto, la implementación de la tecnología blockchain ha ganado relevancia en los últimos años en diversos sectores ya que tiene la capacidad para proporcionar trazabilidad, seguridad y transparencia en los datos y procesos.

Por lo visto en el caso de Burgos *et al* (2022), la industria de las fresas se vio beneficiada con esta tecnología ya que logró superar la falta de un sistema de gestión y control de datos.

El uso de blockchain permitió seguir el camino de la información a lo

largo de la cadena, identificando a los responsables de generar y manipular los datos, así como el momento y origen de creación.

La trazabilidad antes mencionada es fundamental en la cadena de suministro donde la autenticidad y calidad del producto son esenciales.

También hay que recalcar que blockchain permite asegurar la veracidad de los datos compartidos entre múltiples actores y automatizar transacciones mediante contratos inteligentes.

Otro campo impactado en el almacenamiento en la nube por el cual blockchain sustituye a los métodos tradicionales de auditoría (TPA), proporcionando a los usuarios servicios de almacenamiento más confiables y resistentes a las manipulaciones.

Conclusiones

El desarrollo y la implementación de las tecnologías blockchain demostraron ser una solución expresada en transparencia, seguridad y eficiencia en diferentes sectores: cadena de suministro, salud, almacenamiento cloud, aplicaciones descentralizadas entre otras.

La trazabilidad es un pilar importante en blockchain que permite monitorear el flujo de la información y encontrar el origen de estos logrando no solo corroborar la autenticidad de los datos, sino también reducir riesgos asociados a la manipulación y falsificación.

Por otro lado, la intersección entre blockchain y tecnologías novedosas como los gemelos digitales permiten logros significativos en áreas de la construcción y la gestión de recursos lo cual demuestra que la digitalización de procesos mediante blockchain no solo es una herramienta de innovación tecnológica, sino también una estrategia clave para lograr objetivos de sostenibilidad.

Por último, la implementación de blockchain donde la protección de datos es crítica como el almacenamiento en la nube, refuerza la importancia de contar con sistemas robustos que garanticen la confidencialidad e integridad de la información, reduciendo la necesidad

de intermediarios y la admisión solo a usuarios autorizados.

Por parte de las limitaciones al momento de la elaboración del artículo, solo se tomó en cuenta cuatro bases de datos: Scopus, IEEE Xplorer, SciELO y Google Académico, cantidad que puede aumentar si se pretende lograr una revisión más profunda, donde se aborde más campos en comparación con la presente literatura.

Finalmente, se espera continuar ampliando las revisiones futuras ya que la tecnología blockchain no tiene mucho tiempo en desarrollo y aún no ha llegado a su máxima expansión y es una tecnología en dinámica.

Referencias

- Alharbi, A. (2023). Applying Access Control Enabled Blockchain (ACE- BC) Framework to Manage Data Security in the CIS System. <https://doi.org/10.3390/23063020>
- Technology in Supply Chain Management. In Journal of Technology and Systems (Vol. 6, Issue 5). www.carijournals.org
- Bakir, C. (2022). New Blockchain Based Special Keys Security Model with Path Compression Algorithm for Big Data. IEEE Access. <https://doi.org/10.1109/ACCESS.2022.3204289>
- Bashir Dar, A., Hamid Lone, A., Naaz, R., Iqbal Baba, A., & Wu, F. (2022). Blockchain Driven Access Control Mechanisms, Models and Frameworks: A Systematic Literature Review. Journal of Information Security and Cybercrimes Research, 5(1), 01–30. <https://doi.org/10.26735/tyif2196>
- Burgos Rojas, M. A., Haro Polo, C. I., & Mendoza De los Santos, A. C. (2022). El impacto del Blockchain en la cadena de suministros de la industria agropecuaria: Una Revisión Bibliográfica. INGENIERÍA INVESTIGA, 4. <https://doi.org/10.47796/ing.v4i0.708>
- Cárdenas-Solano, L. J., Martínez-Ardila, H., & Becerra-Ardila, L.

- E. (2016). Information security management: A bibliographic review. *Profesional de La Informacion*, 25(6), 931–948. <https://doi.org/10.3145/epi.2016.nov.10>
- Carvajal R., A. E. (2020). Reflexiones sobre la seguridad de la información. *Revista SISTEMAS*, 155, 8–17. <https://doi.org/10.29236/sistemas.n155a2>
- Durá, M., Leal, F., Sánchez-García, Á., Sáez, C., García-Gómez, J. M., Chis, A. E., & González-Vélez, H. (2023). Blockchain for Data Originality in Pharma Manufacturing. *Journal of Pharmaceutical Innovation*, 18(4), 1745–1763. <https://doi.org/10.1007/s12247-023-09748-z>
- Hong, G. W., Kim, J. W., & Chang, H. (2021). Blockchain technology based information classification management service. *Computers, Materials and Continua*, 67(2), 1489–1501. <https://doi.org/10.32604/cmc.2021.013344>
- Hylock, R. H., & Zeng, X. (2019). A blockchain framework for patient-centered health records and exchange (healthChain): Evaluation and proof-of-concept study. *Journal of Medical Internet Research*, 21(8). <https://doi.org/10.2196/13592>
- Kim, D., & Park, S. (2024). Blockchain-Based Caching Architecture for DApp Data Security and Delivery. *Sensors*, 24(14). <https://doi.org/10.3390/s24144559>
- M Machado, A., Sousa, M., & Rocha, Á. (2020). Blockchain Technology in Education. *ICEEG '20*, 130–134. doi: <https://doi.org/10.1145/3409929.3416793>
- ehbodniya, A., Neware, R., Vyas, S., Kumar, M. R., Ngulube, P., & Ray, S. (2021). Blockchain and IPFS Integrated Framework in Bilevel Fog-Cloud Network for Security and Privacy of IoMT Devices. *Computational and Mathematical Methods in Medicine*, 2021. <https://doi.org/10.1155/2021/7727685>
- Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., Altman, D., Antes, G., Atkins, D., Barbour, V., Barrowman, N., Berlin, J. A., Clark, J., Clarke, M., Cook, D., D'Amico, R., Deeks, J. J., Devereaux, P. J., Dickersin, K., Egger, M., Ernst, E., ... Tugwell, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement (Chinese edition). *Journal of integrative medicine*, 7(9), 889–896. <https://doi.org/10.3736/jcim20090918>
- Moreno, B., Muñoz, M., Cuellar, J., Domancic, S., & Villanueva, J. (2018). Revisiones Sistemáticas: definición y nociones básicas. <http://dx.doi.org/10.4067/S0719-01072018000300184>
- Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

- Odoom, J., Xiaofang, H., Danso, S. A., Soglo, R. S., & Nyarko, B. N. E. (2023). Revamped Dual-key Stealth Address Protocol for IoT Using Encryption and Decentralized Storage. *International Journal of Computer Network and Information Security*, 15(1), 14–25. <https://doi.org/10.5815/ijcnis.2023.01.02>
- Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*, 25(4), 1398–1411. <https://doi.org/10.1177/1460458218769699>
- Qin, Q., Jin, B., & Liu, Y. (2021). A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain. *BioMed Research International*, 2021. <https://doi.org/10.1155/2021/6676171>
- Rai, B. K. (2023). BBTCD: blockchain based traceability of counterfeited drugs. *Health Services and Outcomes Research Methodology*, 23(3), 337–353. <https://doi.org/10.1007/s10742-022-00292-w>
- Reyes Riveros, A. J., Cárdenas Iglesias, J. M., & Mendoza de los Santos, A. C. (2024). Explorando los Principales Atributos de Blockchain para la protección de Datos médicos: Una Revisión Sistemática. *Innovación Y Software*, 5(1), 156-176. <https://doi.org/10.48168/innosoft.s15.a130>
- Subramanian, H., & Subramanian, S. (2022). Improving Diagnosis through Digital Pathology: Proof-of-Concept Implementation Using Smart Contracts and Decentralized File Storage. *Journal of Medical Internet Research*, 24(3). <https://doi.org/10.2196/34207>
- Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin. <https://icdt.osu.edu/blockchain-revolution-how-technology-behind-bitcoin-changing-money-business-and-world>
- Teisserenc, B., & Sepasgozar, S. (2021). Project data categorization, adoption factors, and non-functional requirements for blockchain based digital twins in the construction industry 4.0. *Buildings*, 11(12). <https://doi.org/10.3390/buildings11120626>
- Tejada, J., Universidad, *Bolivariana*, P., De Derecho, EN., Ciencias, Y., Facultad, P., & Derecho Medellín, D. E. (2021). DATOS PERSONALES Y PILARES DE LA SEGURIDAD DE LA INFORMACIÓN.
- Vijaya Kumar, A., Sarvani, G. V., & Satya, D. (2020). Blockchain Based Public Cloud Security for E-Voting System on IoT Environment. *IOP Conference Series: Materials Science and Engineering*, 981(4). <https://doi.org/10.1088/1757-899X/981/4/042013>

- Y. Zhang, H. Geng, L. Su and L. Lu, “A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage,” in *IEEE Access*, vol. 10, pp. 105920-105929, 2022. <https://doi.org/10.1109/2022.3211391>
- Yeung, K. (2021). The Health Care Sector’s Experience of Blockchain: A Cross-disciplinary Investigation of Its Real Transformative Potential. *Journal of Medical Internet Research*, 23(12). <https://doi.org/10.2196/24109>
- Yin, X., Yu, Y., Hu, B., Luo, Q., & Tang, Z. (2022). Research on the Application of Blockchain Technology in Education and Teaching in Higher Vocational Colleges. *ACM International Conference Proceeding Series*, 30–36.doi: <https://doi.org/10.1145/3523181.3523186>
- Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., Kumar, R., & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, 8(3), 66–77. <https://doi.org/10.1049/htl2.12008>
- Zhao, Y., Li, Q., Yi, W., & Xiong, H. (2023). Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain. *Agriculture (Switzerland)*, 13(2). <https://doi.org/10.3390/agriculture13020274>
- Zoughalian, K., Marchang, J., & Ghita, B. (2022). A Blockchain Secured Pharmaceutical Distribution System to Fight Counterfeiting. *International Journal of Environmental Research and Public Health*, 19(7). <https://doi.org/10.3390/ijerph19074091>