Explorando los Principales Atributos de Blockchain para la protección de Datos médicos: Una Revisión Sistemática

Exploring the Key Attributes of Blockchain for Medical Data Protection: A Systematic Review

Anderson Jhanyx Reyes Riveros
Universidad Nacional de Trujillo.
Trujillo, Perú.
ajreyesr@unitru.edu.pe
https://orcid.org/0000-0002-7324-5055

Jean Marco Cárdenas Iglesias
Universidad Nacional de Trujillo.
Trujillo, Perú.
jcardenasi@unitru.edu.pe
https://orcid.org/0000-0003-0315-3953

Alberto Mendoza de los Santos
Universidad Nacional de Trujillo.
Trujillo, Perú.
amendozad@unitru.edu.pe
https://orcid.org/0000-0002-0469-915X

ARK: ark:/42411/s15/a130
DOI: 10.48168/innosoft.s15.a130
PURL: 42411/s15/a130

RECIBIDO 04/01/2023 • ACEPTADO 05/03/2024 • PUBLICADO 30/03/2024

RESUMEN

Este artículo aborda la protección de datos médicos en sistemas de información médica, centrándose en la creciente adopción de registros médicos electrónicos (EHR). Reconoce los desafíos de seguridad inherentes a los sistemas centralizados y aboga por un intercambio seguro de datos médicos. La metodología sigue los principios de la declaración PRISMA, utilizando motores de búsqueda como SCOPUS, PUBMED e IEEE XPLORE para identificar 20 documentos relevantes. Estos documentos se centran en atributos clave de la tecnología Blockchain: control de acceso, privacidad de datos, seguridad de datos y encriptación. Los resultados indican que el control de acceso es el atributo más recurrente, seguido por la privacidad de datos, seguridad de datos y encriptación. La discusión resalta la aplicabilidad práctica de estos atributos, mejorando la confianza del paciente y la eficiencia del flujo de trabajo médico. Las conclusiones afirman la relevancia de la Blockchain en la protección de datos médicos, señalando oportunidades para investigaciones futuras, especialmente en entornos de salud menos desarrollados. El estudio proporciona un marco integral para profesionales de la salud y desarrolladores, subrayando la necesidad de una mayor aplicación y exploración de estrategias de implementación mediante

casos de estudio específicos. En resumen, la revisión sistemática aporta de manera significativa al conocimiento y aplicación de blockchain en la gestión segura de la información médica a nivel global. Destaca la importancia de atributos clave de blockchain en la mejora de la seguridad, privacidad e integridad de los datos médicos, ofreciendo una perspectiva completa para profesionales y desarrolladores interesados en este ámbito.

Palabras claves: blockchain, control de acceso, datos médicos, Seguridad de información

ABSTRACT

This article addresses the protection of medical data in health information systems, focusing on the growing adoption of electronic health records (EHRs). It recognises the security challenges inherent in centralised systems and advocates for the secure exchange of medical data. The methodology follows the principles of the PRISMA statement, using search engines such as SCOPUS, PUBMED and IEEE XPLORE to identify 20 relevant documents. These papers focus on key attributes of blockchain technology: access control, data privacy, data security and encryption. The results indicate that access control is the most recurring attribute, followed by data privacy, data security and encryption. The discussion highlights the practical applicability of these attributes, improving patient confidence and medical workflow efficiency. The conclusions affirm the relevance of the blockchain in medical data protection, pointing to opportunities for future research, especially in less developed healthcare settings. The study provides a comprehensive framework for healthcare professionals and developers, highlighting the need for further application and exploration of implementation strategies through specific case studies. In summary, the systematic review makes a significant contribution to the understanding and application of blockchain in the secure management of medical information globally. It highlights the importance of key attributes of blockchain in improving the security, privacy and integrity of medical data, providing a comprehensive perspective for practitioners and developers interested in this area.

Keywords: *blockchain, access control, medical data, information security*

INTRODUCCIÓN

Los datos médicos son cruciales para el cuidado de los pacientes y es debido al grado de importancia que es requerido para su uso en toda institución médica. El almacenamiento no solo consta de datos médicos, sino también de datos de diagnósticos y hospitalizaciones. Según el estudio [1] indica que debido a la amplitud de estos datos, los sistemas de información médica se vuelven cada vez más complejos y estructuralmente extensos, consecuentemente esto conlleva a que se opte por sistemas de información electrónicos.

En el presente, debido al adelanto tecnológico se manejan los registros médicos electrónicos (EHR, por sus siglas en inglés), Abeywardena [2] la define como un sistema interorganizacional, que almacena datos médicos del paciente (datos poblacionales, registro de avance, fármacos, señales corporales, historial médico, inmunizaciones, datos de laboratorio e informes de radiografía, etc.), este sistema mejora la óptima atención médica debido a que permiten el intercambio y acceso de datos en tiempo real a todo el entorno médico (laboratorios, especialistas, farmacias, escuelas médicas, etc.), a su vez brindan automatización de actividades y soporte en la toma de decisiones. Sin duda los sistemas EHR gestionan eficientemente los datos médicos, pero esto también trae consigo los principales problemas de toda información expuesta electrónicamente.

La información médica que afecta directamente a la salud de un paciente debe ser íntegra y fiable. Además, la privacidad del paciente debe protegerse de la exposición a usuarios no autorizados. Por lo tanto, es necesario desarrollar un sistema seguro de intercambio de datos médicos que pueda proporcionar la integridad y fiabilidad de los datos médicos y proteger la privacidad del paciente abordando los problemas de los actuales sistemas centralizados de intercambio de datos médicos. Se ha propuesto la descentralización del sistema para complementar los problemas del actual sistema de intercambio de datos médicos [3].

Una de las tecnologías más innovadoras que se ha desarrollado en los últimos años ha sido el blockchain, no solo por la versatilidad que presenta sino también por la seguridad que garantiza. Dentro del presente artículo tenemos como objetivo el detallar los beneficios, retos y oportunidades que ofrecen los sistemas de seguridad y control de acceso a los datos médicos mediante el uso de esquemas basados en la tecnología blockchain [4].

Por tanto, el objetivo de la investigación es dar respuesta a la interrogante ¿Cuáles son los principales atributos de blockchain que se han identificado y estudiado en la literatura científica y técnica en relación con la protección de datos médicos?

Concepto del Blokchain

La definición de blockchain, es descrita como la base de datos que posee universalidad, no centralizada, posibilita el registro de un historial de operaciones cifradas (reemplaza la historia clínica del paciente convencional) haciéndola inalterable a futuros cambios, siendo así una plataforma de registro descentralizada que favorece a la no centralización, visibilidad y la integridad de los datos privados de cada paciente, en ese punto sus tres ventajas claves: monitorización, visibilidad e inmutabilidad [5].

La blockchain suministra de una base de datos distribuida inalterable apoyada en una serie de crecientes bloques. Estos, por ser públicos, integran a un sistema accesible fortaleciendo la

fiabilidad en base a la visibilidad y solidez del método de creación de la blockchain [6]. La plataforma, como es accesible, asimismo es seudoanonimo: los miembros registrados se verifican con claves públicas (alias), no con nombres [7].

Según esto, la blockchain puede brindar solidez, seguridad, visibilidad y capacidad de crecimiento a amplios sistemas de datos, facilitando así afrontar una diversidad de peligros, comprendiendo desde las filtraciones de datos. Mediante la blockchain, estos peligros pueden contrarrestar documentando uno a uno todos los movimientos hechas hacia los datos, generando conservar el reconocimiento y privilegios, logrando limitar al sujeto que tiene permiso de acceso de los datos mismos [8].

Sistemas de seguridad de datos médicos

En la actualidad, merece la pena prestar atención a como permitir que los pacientes sean propietarios de sus datos médicos y compartan sus datos médicos de forma segura y dinámica entre diferentes instituciones médicas, lo cual no es un tema nuevo para el intercambio de datos médicos. Muchas instituciones médicas pueden almacenar los datos de forma centralizada en servidores. A la hora de compartir datos médicos es necesario tener en cuenta cuestiones de seguridad y privacidad [9]. En [10], menciona que de igual modo posee la capacidad de incidir sobre las propias prácticas laborales así como obligaciones legitimas de los profesionales de salud. Los médicos pueden adoptar las excelentes decisiones en los cuidados del acceso a su historial clínico total, debido a la ausencia de acceso causa el retraso de decisiones relevantes e influir en el bienestar de salud [11].

Los registros de salud de información privada son la información más confidencial que hay, por lo tantos los profesionales médicos como las clínicas y servicios médicos están forzados por ley a velar por su secreto medico[12].

Aunque por otro lado los últimos dos poseen mayores recursos para resguardar la información confidencial, el personal médico con frecuencia dispone de medios limitados para garantizar la preservación del resguardo de los registros médicos[13].

Aunque con el tiempo es más habitual emplear la tecnología para digitalizar y modernizar los registros médicos o interactuar con el paciente, y de que también es más recurrente las consultas virtuales y la asistencia médica en línea para supervisar y gestionar a distancia el bienestar del paciente [14].

Teniendo en cuenta el panorama del sector salud y la necesidad de una mejora eficaz en la seguridad de datos médicos es que podemos aplicar técnicas como la blockchain que tiene por objetivo el gestionar y contar con un banco de datos integral de registros relacionado a la salud del paciente así como historias médicas, información de ADN, radiografías, registros biológicos,

datos de seguimiento médico, datos personales y demográficos e incluso redes sociales[15]. Cabe destacar que la Blockchain cumpla el rol de administrador de control de accesos y permisos para datos y registros médicos.

Control de acceso a datos médicos

El resguardo de información vinculados a la salud de pacientes ha sido una inquietud, para preservar la confidencialidad del paciente, cabe destacar la importancia de comprender como se almacenan, comparten, utilizan y gestionan sus datos [16].

Los sistemas de control de acceso en el campo de atención medica son especiales, esto debido a la capacidad de limitar el acceso a espacios importantes, impedir el esparcimiento de enfermedades, prevenir la sustracción de aparatos de cuidado médico y fármacos indispensables, así como velar por el bienestar de pacientes y colaboradores[17].

Aun cuando la urgencia de poseer mecanismos de protección seguras y el acatamiento de las legislaciones que aplican en el área, los centros médicos, e instituciones de salud todavía cuentan con algún margen para la manejabilidad en cuanto a la manera de la gestión del control de acceso. A fin de cuentas, diversas instalaciones de salud poseen múltiples espacios, secciones de personas bajo cuidado médico y estructuras físicas, así que necesitan invertir en un sistema de resguardo del centro médico concebido de modo particular.

Teniendo en cuenta lo anterior es importante tomar como referencia una de las principales ventajas en la Blockchain puesto que permite mejorar aspectos como el control de acceso al sistema de salud, dado que éstas no tienen únicamente un sitio de acceso a los registros, más que esto implica dentro de los registros distribuidos en variados nodos, dificultando así efectuar ataques como DDoS [18].

En contraste, en cuanto a la tecnología que no faculta suprimir o alterar obviando la autorización previa, la información una vez almacenada, conlleva a no poder modificar tal información en el sistema y asegura el no rechazo de algún individuo que haya efectuado el cambio a la información de la red [19].

Ventajas de la tecnología Blockchain

Las fundamentales ventajas de Blockchain son:

- Invariabilidad de datos: es casi improbable alterar la data de la red, y en instancias de ocurrir tendría la capacidad de anular la cadena de bloque.
- Red resiliente: Blockchain es resistente a problema en cierto modo, debido a que, si cierta parte genera un contratiempo, la totalidad de la red continuara operante con versión más reciente de información [20].
- Confiere garantía entre desconocidos: La tecnología Blockchain se desempeña conforme al contenido de registros, en consecuencia, no requiere de un tercero para otorgar fiabilidad sobre sí mismo.
- Diversidad de utilidad e implementaciones: Blockchain representa un sistema de información versátil al emplearla con una vasta gama de funciones y utilizaciones, como, por ejemplo, en procesos de votación, de certificación de propiedad en relación a bienes y derechos de autor, así como también al monitoreo de materia prima y productos terminados[21].

Desventajas de la tecnología Blockchain

Las fundamentales desventajas de Blockchain son:

- Invariabilidad de datos: así como es su ventaja, a su vez puede ser lo contrario, esto debido al momento en que las personas erran en registrar información, generando así problemas en la realidad, dado que los datos no podrán ser editada[22].
- Cambio de celeridad del manejo de información. La red puede mermar la celeridad de los intercambios al momento que se suscite un contratiempo con la red o mientras las tarifas de ese proceso suelen ser de menor costo, reduciendo así el estímulo a los mineros, es decir aquellos relacionados a dicha actividad[23].
- Desmesurada cantidad de recursos. Blockchain representa una red de unanimidad, en consecuencia, sirve de múltiples elementos en el momento de autenticar diferentes versiones de similar registro.
- Potencial crecimiento de falta de empleo. Blockchain posee la capacidad descartar intermediarios que protejan la información y suministren garantía de su contenido. Entonces, ciertas áreas y ocupaciones se verían afectadas. Pasando algo similar con la innovación que produce la tecnología [24].

Metodología

Las revisiones sistemáticas son beneficiosas en numerosas facetas esenciales, del cual son capaces de brindar una consolidación de la situación actual de la información dentro de un campo particular, con base en la cual puede llegar a encontrar venideras preferencias en relación al estudio, enfocar dudas que desde otro enfoque no tienen la posibilidad de ser resueltas por estudios únicos, reconocer desafíos en el estudio inicial que necesitan ser solucionados en próximas investigaciones y crear o valorar teorías acerca de qué forma acontecen eventos de interés [25].

Con el propósito de esta misma revisión sistemática se empleó la metodología PRISMA, la cual fue diseñado sobre todo para revisiones sistemáticas que analizan los impactos de las acciones médicas, sin importar la estructura de los estudios añadidos. A pesar de ello, los elementos del registro de control son utilizables para las publicaciones de revisiones sistemáticas la cual valoran diferentes enfoques no ligados a la salud (por ejemplo, programas sociales o educativos), así mismo múltiples puntos son válidos a revisiones sistemáticas con fines diversos al estudio de enfoques (un caso, análisis de origen, predominio o proyección).

La declaración PRISMA 2020 se sitúa orientada con el propósito de ser aplicada en revisiones sistemáticas el cual contienen resumen (por ejemplo, metaanálisis de contrastaciones por parejas u otros procedimientos de síntesis estadística) o que no involucren resumen (por ejemplo, puesto que hay solo un estudio valido).

Los ítems de la declaración PRISMA 2020 son significativos para las revisiones sistemáticas de enfoques híbridos (abarcan estudios cuantificables y descriptivos), aunque de igual manera ellos mismos necesitan analizar las normativas en relación con la demostración y resumen de información descriptiva [26],[27]. Igualmente, se brinda un formato PRISMA para el esquema de secuencia, que es capaz de adaptarse en propósito de si la revisión sistemática es original o actualizada (Figura 1).

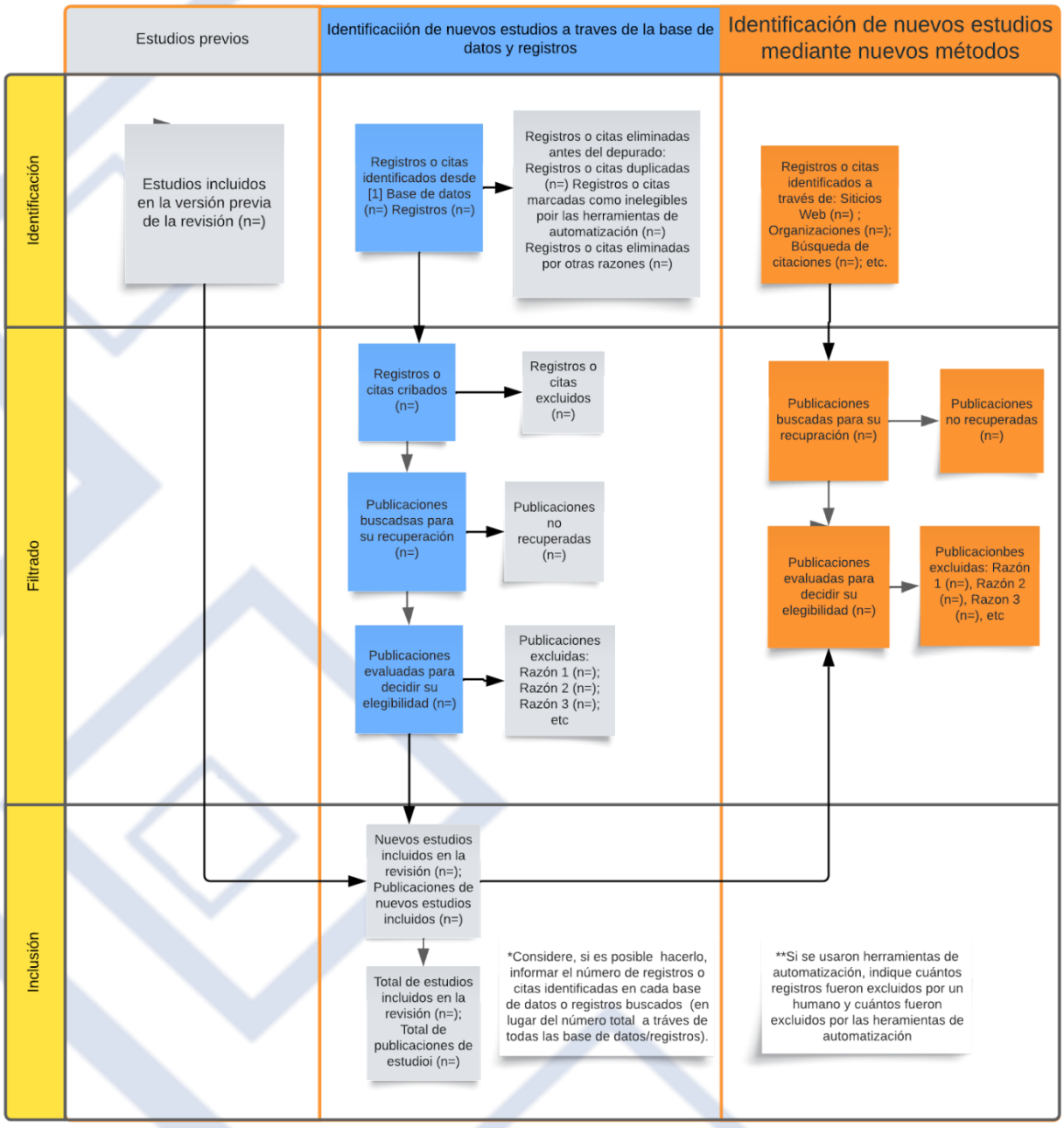

Figura 1. Diagrama de flujo PRISMA 2020

La versión más reciente ha sido ajustado por Yepes en [28]. Los cuadros en tono gris deben llenarse únicamente si son relevantes; en caso diferente, precisan ser eliminados del esquema de flujo. Es importante notar que un informe puede adoptar diversas formas, como un artículo en una publicación académica, borrador, resumen de ponencia, ficha de estudio, reporte de estudio médico, tesis o disertación, escrito no publicado, informe estatal u otro documento relevante.

Ecuaciones de búsqueda

Para poder comenzar el proceso de búsqueda, se implementó conectores booleanos de variables de estudio tomando en cuenta las diversas variables del tema. Con el fin de mejorar la precisión en la búsqueda de la literatura científica, se elaboró un protocolo que incluye la combinación de los términos predefinidos junto con los operadores booleanos detallados en la Tabla 1.

Tabla 1. Ecuación de búsqueda por fuente de búsqueda

Repositorio	Cadena de búsqueda
SCOPUS	TITLE-ABS-KEY (medical AND data AND security AND access AND contract AND blockchain)
PubMed	(medical data security and access control and blockchain)
IEEE xplore	("All Metadata": security) AND ("All Metadata": access control) AND ("All Metadata": medical data) AND ("All Metadata": blockchain)

Criterios de inclusión y exclusión

Los criterios de inclusión y exclusión son directrices particulares que se definen al llevar a cabo una revisión bibliográfica o un artículo de revisión. Su objetivo es determinar qué estudios o artículos serán considerados y cuáles serán descartados en la revisión. Estos criterios son esenciales con el fin de mantener la idoneidad y excelencia de los estudios incorporados en el análisis. Todos los criterios de inclusión planteados se visualizan en la Tabla 2 y todos los criterios de exclusión planteados se aprecia en la Table 3.

Tabla 2. Criterios de inclusión

N°	Criterios de inclusión
CI1	Los artículos deben abarcar la temática de los principales atributos de blockchain para la protección de datos médicos.
CI2	Seleccionar artículos redactados en inglés y español.
CI3	Los artículos hayan sido publicados entre los años 2018 y 2023.

Nota. CI= criterio de inclusión

Tabla 3. Criterios de exclusión

N°	Criterios de exclusión
CE1	Artículos duplicados.
CE2	Artículos que no hayan sido publicados entre los años 2018 y 2023.
CE3	Artículos que carecen de información relevante con nuestra temática.
CE4	Documentos que no sean artículos.

Nota. CE= criterio de exclusion

Proceso de recolección de información

Las primeras búsquedas se realizaron aplicando las directrices de inclusión mostrados en la Tabla 2, además de combinar los términos 'access control' y 'medical data security' en las bases de datos PubMed, SCOPUS usando combinaciones de términos booleanos AND y OR. Estas búsquedas arrojaron poca cantidad de resultados, algunos redundantes o poco valiosos para la revisión, pero nos brindaron una amplia comprensión del tema. Posteriormente se agregaron nuevos términos como 'blockchain', que ayudaron a que los resultados sean mucho mayores, sin embargo, no suficientes para nuestra revisión.

En la consulta de búsquedas en SCOPUS y PubMed se usaron las palabras anteriormente mencionadas haciendo diversas combinaciones: "access control"," medical security", "electronic health records" y "blockchain".

Al no tener mucha información acerca de la temática escogida se realizó una búsqueda manual mediante IEEE xplore con distintas combinaciones de los términos de búsqueda indicados como se logra visualizar en la Tabla 1.

Seguidamente, los documentos encontrados fueron depurados por los revisores aplicando los criterios de exclusión mostrados en la Tabla 3, con la finalidad de seleccionar aquellos que cumplieran con los estándares de relevancia y calidad para esta revisión sistemática. Se excluyeron los estudios que no estaban directamente relacionados con la temática, así como aquellos que no proporcionaban datos sustanciales para el análisis. Además, se descartaron aquellos documentos duplicados o de baja calidad metodológica. Este proceso de depuración aseguró la selección de fuentes confiables y pertinentes para el progreso de la actual revisión. Posteriormente, se procedió a la extracción de datos clave de los artículos seleccionados, lo cual constituye una fase crucial para la evaluación y resumen de la información.

En la Tabla 4, a continuación, se proporciona un desglose de los artículos correspondientes a cada base de datos y motores de búsqueda utilizados como punto de referencia.

Tabla 4. Artículos depurados empleando criterios de inclusión y exclusión

Base de datos	Artículos encontrados en total	Aplicando CE1	Aplicando CE2	Aplicando CE3	Aplicando CE4
SCOPUS	256	170	48	22	12
PubMed	57	43	21	8	5
IEEE xplore	16	14	8	4	3
TOTAL	329	227	77	34	20

Se aplicaron varios filtros a las publicaciones y revistas científicas seleccionadas (ver Figura 2), apegándonos a las directrices de inclusión y exclusión establecidos. Además, se evaluaron los principales atributos de blockchain que se han identificado y estudiado en la literatura científica y técnica en la relación con la protección de los datos médicos.

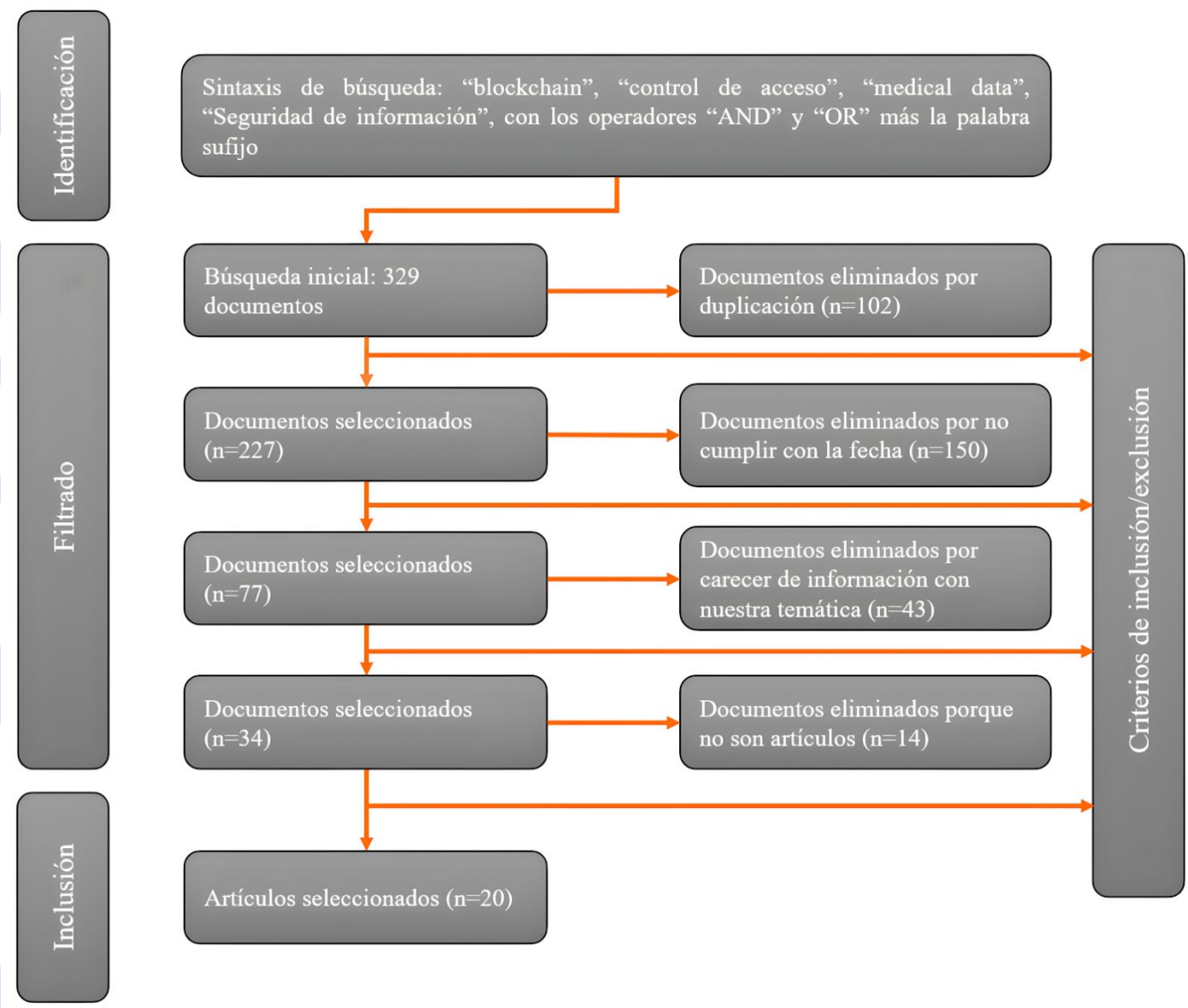

Figura 2. Diagrama de flujo PRISMA aplicado en este articulo

Resultados

Luego de ejecutar las directrices de inclusión y exclusión, se identificaron 20 artículos que cumplían con los requisitos establecidos. En la Tabla 5 se presenta un desglose detallado de estos

artículos, permitiendo así visualizar la evolución y enfoque de investigación orientada, tal como se refleja en las revistas donde fueron publicados.

Tabla 5. Resultados de búsqueda final y su respectivo enfoque de investigación orientada

N°	Autores	Atributos	Tipo	Tecnología
1	Liu, J., Li, X., Ye, L., Zhang, H., Du, X., Guizani, M	Privacidad de datos, control de acceso	Propuesta de sistema	Blockchain
2	Sharma, Balamurugan	Control de acceso, cifrado	Propuesta de sistema	Blockchain, Smart contract y cifrado proxy
3	Rupasinghe, T., Burstein, F., Rudolph, C.	Control de Acceso, privacidad de datos	Propuesta de arquitectura dinámica	Blockchain, smart contract,
4	Park, Y.-H., Kim, Y., Lee, S.-O., Ko, K.	Control de acceso	Propuesta de esquema	Blockchain, recifrado proxy, smart contract
5	Sun, Z., Han, D., Li, D., Wang, X., Chang, C.-C., Wu, Z.	Control de acceso	Propuesta de almacenamiento de seguridad de información	Blockchain, tejido Hyperledger, control de acceso basado en atributos, IPFS
6	Abeywardena, K.Y., Attanayaka, B., Periyasamy, K., Gunarathna, S., Prabhathi, U., Kudagoda, S	Control de acceso, privacidad de datos	Propuesta de sistema privado	Blockchain, criptografia, smart contract
7	Egala, B.S., Pradhan, A.K., Badarla, V., Mohanty, S. P	Control de acceso, privacidad de datos	Propuesta de esquema	Blockchain, smart contract
8	Younis, M., Lalouani, W., Lasla, N., Emokpae, L., Abdallah, M	Control de acceso, privacidad de datos	Propuesta de solución y nuevo protocolo	Blockchain, cloud, gestion de claves
9	Kumar, N.P.H., Prabhudeva, S.	Control de Acceso, privacidad de datos, encriptación	Propuesta de algoritmo	Blockchain Ethereum, sistema de archivos interplanetarios (IPFS), cifrado simétrico, smart contract

10	Majdoubi, D.E., Bakkali, H.E., Sadki, S	Control de acceso, privacidad de datos	Propuesta de sistema SmartMedChain	Blockchain en HyperLedger Fabric, sistema de archivos interplanetarios (IPFS), IoT
11	Hylock, R.H., Zeng, X	Privacidad de datos, control de acceso	Propuesta de sistema HealthChain	Blockchain, recifrado proxy, smart contract
12	Zhao, F., Yu, J., Yan, B.	Control de acceso	Propuesta de modelo de control	Blockchain, sistema de archivos interplanetarios (IPFS), smart contract
13	Devi Parameswari, C., Mandadi, V	Privacidad de datos, control de acceso	Propuesta de sistema	Blockchain, smart contract
14	Zhang, D., Wang, S., Zhang, Y., Zhang, Q., Zhang, Y	Control de acceso, privacidad de datos	Propuesta de esquema	Blockchain, smart contract
15	Chen, F., Huang, J., Wang, C., Tang, Y., Huang, C., Xie, D., Wang, T., Zhao, C	Control de acceso, seguridad de datos	Propuesta de diseño de control de acceso	Blockchain, smart contract, tejido Hyperledger
16	Hussien, H.M., Yasin, S.M., Udzir, N.I., Ninggal, M.I.H	Control de acceso, encriptación, privacidad de datos	Propuesta de esquema de control de acceso y autorización criptográfica	Smart contract, criptografía, cifrado, blockchain
17	Chen, Y., Meng, L., Zhou, H., Xue, G.	Control de acceso, encriptación, privacidad y seguridad de datos	Propuesta de esquema de preservación de la privacidad	Cifrado, Blockchain, tejido HyperLedger
18	Hafida Saidi; Nabila Labraoui; Ado Adamou Abba Ari; Leandros A. Maglaras; Joel Herve Mboussam Emati	Control de acceso, privacidad y seguridad de datos	Propuesta de sistema	Blockchain, smarts contracts
19	Eman-Yasser Daraghmi; Yousef-Awwad Daraghmi; Shyan-Ming Yuan	Control de acceso, encriptación, seguridad de datos	Propuesta de un diseño de sistema MedChain	Blockchain, smart contract, criptografía

20	Sabri Barbaria; Marco Casassa Mont; Essam Ghadafi; Halima Mahjoubi Machraoui; Hanene Boussi Rahmouni	Control de acceso, privacidad y seguridad de datos	Desarrollo de enfoque en intercambio de datos	Blockchain Hyperledger, smart contract

Tras un exhaustivo análisis de los 20 artículos seleccionados, se constató que diversos autores emplean una variedad de atributos en sus investigaciones sobre blockchain. Los atributos que fueron encontrados y seleccionado fueron (Control de acceso, privacidad de datos, seguridad de datos y encriptación). Con el fin de abordar la pregunta central de nuestra investigación, se hizo un escrutinio detallado y se procedió a la clasificación de estos atributos, cuyos resultados se presentan de manera detallada en la Tabla 6.

Tabla 6. Distribución de atributos de artículo seleccionados

N°	Control de acceso	Privacidad de datos	Seguridad de datos	Encriptación
1	1	1		
2	1			1
3	1	1		
4	1			
5	1			
6	1	1		
7	1	1		
8	1	1		
9	1	1		1
10	1	1		
11	1	1		
12	1			

13	1	1		
14	1	1		
15	1		1	
16	1	1		1
17	1	1	1	1
18	1	1	1	
19	1		1	1
20	1	1	1	
Total	**20**	**14**	**5**	**5**

A continuación, presentaremos el porcentaje de atributos aplicados en los artículos seleccionados (ver Figura 3). Se destaca que el Control de acceso es el atributo más prevalente, representando un 46% del total. Le sigue la Privacidad de datos con un 32%, mientras que tanto la Seguridad de datos como la Encriptación registran un 11% cada una.

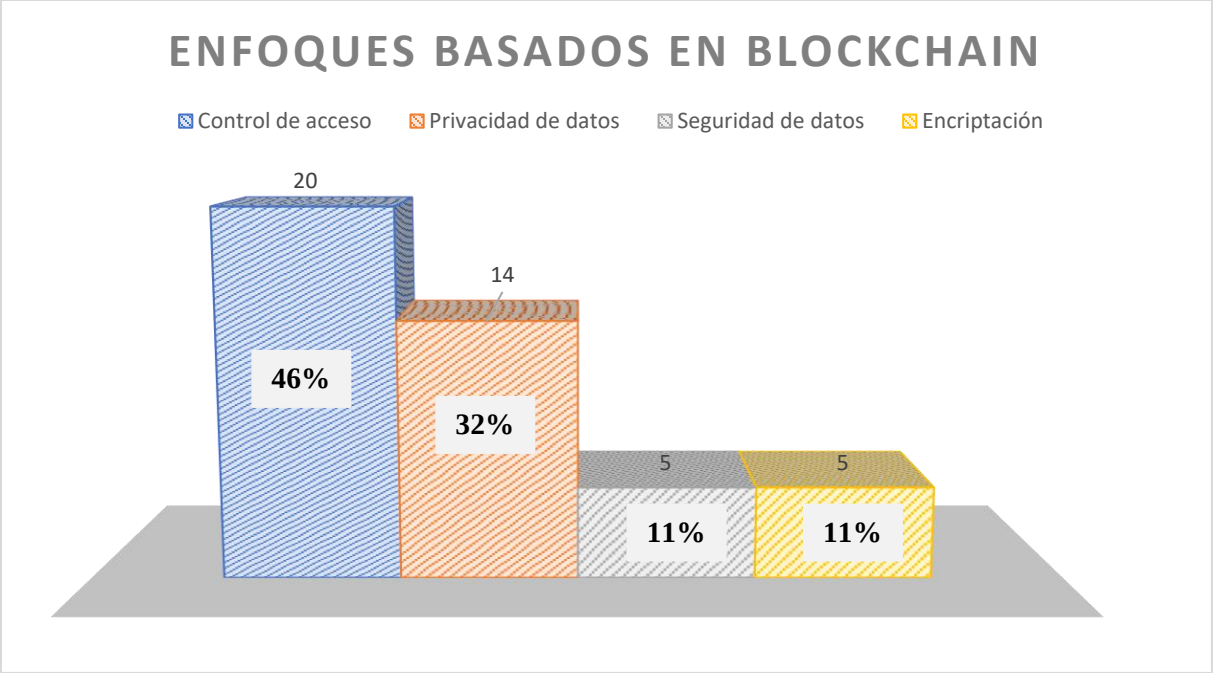

Figura 3. Distribución porcentual de los atributos de blockchain

Discusión

El empleo de Blockchain dentro de la atención médica y asistencia hacia el paciente, demanda el involucramiento de diversas entidades comprometidas, agregando proveedores, programas de bienestar y autoridades particulares. La integración de esta comunidad con el fin de conformar las directrices se volverá un desafío. Gracias a la índole de la información de la asistencia médica, poseer una garantía de datos siendo relevante. Como mencionamos en el presente artículo, hay diversas alternativas para tratar los desafíos de confidencialidad, tales como la Blockchain.

Los resultados encontrados con respecto a los principales atributos de blockchain para la protección de datos médicos, rige en cuatro atributos (control de acceso, privacidad de datos, seguridad de datos y encriptación) según los diferentes artículos, donde muestra de manera general que la implementación de dichos atributos aumenta la confianza, satisfacción del paciente y el flujo de trabajo eficiente. Estos resultados llegan a coincidir con Abubakar [29], lo cual señala que cuando se somete a análisis y evaluaciones de seguridad, el sistema de blockchain muestra mejoras de rendimiento en los niveles de privacidad de los datos, alta seguridad y diseño de control de acceso ligero en comparación con los modelos actuales de control de acceso centralizado, esto implica que los paciente tengan más confianza.

Una faceta fundamental de un sistema de asistencia médica equivale a la manera en la cual distribuyen la información mediante operaciones de secuencia de importancia. Esta tecnología posibilita la usabilidad compartida de la data sin prescindir de quitar las copias, equivocaciones y contradicciones de la cual puedan originarse mediante resguardo de información convencional, en otras palabras, suprime al mediador existente entre la solicitud de una prestación la cual generara un escenario más viable de intercambio de información médica.

Estos resultados coinciden con Tao [30], lo cual señala que a través de análisis de seguridad, rendimiento y comparación con otras soluciones, el esquema de este artículo puede satisfacer las necesidades de los escenarios de la vida real en términos de seguridad y viabilidad, y proporciona un nuevo modelo práctico para el intercambio de información médica.

Finalmente, es importante mencionar las limitaciones de este estudio. En su mayoría, los artículos analizados provienen de países desarrollados, lo que plantea retos con miras a la aplicación de Blockchain dentro del sector salud en países como Perú. Además, se observó una escasez de artículos sobre Blockchain publicados en países de Latinoamérica, y algunos de estos no están accesibles para su consulta.

Conclusiones

Esta revisión sistemática muestra un notable avance para el ámbito de la protección de datos médicos mediante tecnologías basadas en blockchain. La investigación ha proporcionado una visión detallada y exhaustiva de los atributos clave que destacan en esta área crucial. Específicamente, el control de acceso, la privacidad de datos, la seguridad de datos y la encriptación emergen como pilares fundamentales en la preservación y seguridad de la información médica en entornos blockchain.

Este estudio no solo consolida y sintetiza el estado actual del conocimiento sobre este tema, sino que también identifica áreas de oportunidad para futuras investigaciones. Uno de los hallazgos más relevantes es la necesidad de extender la aplicación de estas tecnologías a contextos menos desarrollados, como en el caso particular de Perú y países latinoamericanos, donde aún existe un amplio potencial por explorar.

En términos de contribución al campo, esta revisión sistemática proporciona un marco sólido y comprensivo para personal de salud, investigadores y desarrolladores de tecnología interesados en la protección de datos médicos. Ofrece una hoja de ruta valiosa al resaltar los atributos más prometedores y subraya la importancia de la aplicación de blockchain en la gestión segura de la información médica. Para futuras investigaciones, se sugiere un mayor énfasis en la adaptabilidad y viabilidad de estas soluciones en entornos de salud de países menos desarrollados. Además, sería beneficioso profundizar en la exploración de estrategias de implementación y casos de estudio específicos para analizar la influencia real de estos atributos en la práctica.

En resumen, esta revisión sistemática no solo enriquece el entendimiento sobre la protección de datos médicos con tecnologías blockchain, sino que también abre la puerta a una nueva era de investigación y desarrollo en este campo, con la aptitud de convertir el estilo en la cual se aborda la seguridad de la información médica a nivel global.

Contribución de Autoría

Anderson Jhanyx Reyes Riveros: Conceptualización, Análisis formal, Investigación, Visualización, Metodología, Software, Validación, Redacción - borrador original, Curación de datos, Escritura, revisión y edición. **Jean Marco Cárdenas Iglesias:** Conceptualización, Análisis formal, Investigación, Visualización, Metodología, Software, Validación, Redacción - borrador original, Curación de datos, Escritura, revisión y edición. **Alberto Carlos Mendoza de los Santos:** Visualización, Software, Validación, Redacción - borrador original, Curación de datos.

Referencias

[1] Z. Sun, D. Han, D. Li, X. Wang, C. C. Chang, and Z. Wu, "A blockchain-based secure storage scheme for medical information," Eurasip J. Wirel. Commun. Netw., vol. 2022, no. 1, 2022, doi: 10.1186/s13638-022-02122-6.

[2] K. Y. Abeywardena, B. Attanayaka, K. Periyasamy, S. Gunarathna, U. Prabhathi, and S. Kudagoda, "Blockchain based Patients' detail management System," ICAC 2020 - 2nd Int. Conf. Adv. Comput. Proc., pp. 458–463, 2020, doi: 10.1109/ICAC51239.2020.9357163.

[3] S. Lee, J. Kim, Y. Kwon, T. Kim, and S. Cho, "Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study," J. Med. Internet Res., vol. 24, no. 3, 2022, doi: 10.2196/29108.

[4] M. Abouali, K. Sharma, O. Ajayi, and T. Saadawi, "Performance Evaluation of Secured Blockchain-Based Patient Health Records Sharing Framework," 2022 IEEE Int. IOT, Electron. Mechatronics Conf. IEMTRONICS 2022, 2022, doi: 10.1109/IEMTRONICS55184.2022.9795759.

[5] S. Nandi, J. Sarkis, A. A. Hervani, and M. M. Helms, "Redesigning Supply Chains using Blockchain-Enabled Circular Economy and COVID-19 Experiences," Sustain. Prod. Consum., vol. 27, pp. 10–22, 2021, doi: 10.1016/j.spc.2020.10.019.

[6] F. Chen et al., "Data Access Control Based on Blockchain in Medical Cyber Physical Systems," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/3395537.

[7] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control," IEEE Internet Things J., vol. 8, no. 14, pp. 11717–11731, 2021, doi: 10.1109/JIOT.2021.3058946.

[8] S. Ghaffaripour and A. Miri, "Application of Blockchain to Patient-Centric Access Control in Medical Data Management Systems," 2019 IEEE 10th Annu. Inf. Technol.

Electron. Mob. Commun. Conf. IEMCON 2019, pp. 190–196, 2019, doi: 10.1109/IEMCON.2019.8936186.

[9] F. Zhao, J. Yu, and B. Yan, "Towards cross-chain access control model for medical data sharing," Procedia Comput. Sci., vol. 202, pp. 330–335, 2022, doi: 10.1016/j.procs.2022.04.045.

[10] C. D. Parameswari, "Healthcare data protection based on blockchain using solidity," pp. 577–580, 2020.

[11] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records," 2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc., pp. 1–6, 2018, doi: 10.1109/GLOCOM.2018.8647713.

[12] H. Saidi, N. Labraoui, A. A. A. Ari, L. A. Maglaras, and J. H. M. Emati, "DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data," IEEE Access, vol. 10, pp. 101011–101028, 2022, doi: 10.1109/ACCESS.2022.3207803.

[13] E. Y. Daraghmi, Y. A. Daraghmi, and S. M. Yuan, "MedChain: A design of blockchain-based system for medical records access and permissions management," IEEE Access, vol. 7, pp. 164595–164613, 2019, doi: 10.1109/ACCESS.2019.2952942.

[14] N. P. H. Kumar and S. Prabhudeva, "An Authorization Framework for Preserving Privacy of Big Medical Data via Blockchain in Cloud Server," Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 3, pp. 140–150, 2022, doi: 10.14569/IJACSA.2022.0130319.

[15] T. Rupasinghe, F. Burstein, and C. Rudolph, "Blockchain based dynamic patient consent: A privacy-preserving data acquisition architecture for clinical data analytics," 40th Int. Conf. Inf. Syst. ICIS 2019, no. Bacchus 2017, pp. 1–9, 2019.

[16] D. El Majdoubi, H. El Bakkali, and S. Sadki, "SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework," J. Healthc. Eng., vol. 2021, 2021, doi: 10.1155/2021/4145512.

[17] H. M. Hussien, S. M. Yasin, N. I. Udzir, and M. I. H. Ninggal, "Blockchain-based access control scheme for secure shared personal health records over decentralised storage," Sensors, vol. 21, no. 7, pp. 1–36, 2021, doi: 10.3390/s21072462.

[18] D. Zhang, S. Wang, Y. Zhang, Q. Zhang, and Y. Zhang, "A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/2759787.

[19] R. H. Hylock and X. Zeng, "A blockchain framework for patient-centered health records and exchange (healthChain): Evaluation and proof-of-concept study," J. Med. Internet Res., vol. 21, no. 8, pp. 1–30, 2019, doi: 10.2196/13592.

[20] Y. Sharma and B. Balamurugan, "Preserving the Privacy of Electronic Health Records using Blockchain," Procedia Comput. Sci., vol. 173, no. 2019, pp. 171–180, 2020, doi: 10.1016/j.procs.2020.06.021.

[21] A. Ali et al., "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography," Sensors, vol. 22, no. 2, 2022, doi: 10.3390/s22020528.

[22] Y. H. Park, Y. Kim, S. O. Lee, and K. Ko, "Secure outsourced blockchain-based medical data sharing system using proxy re-encryption," Appl. Sci., vol. 11, no. 20, 2021, doi: 10.3390/app11209422.

[23] S. Barbaria, M. C. Mont, E. Ghadafi, H. Mahjoubi Machraoui, and H. B. Rahmouni, "Leveraging Patient Information Sharing Using Blockchain-Based Distributed Networks," IEEE Access, vol. 10, pp. 106334–106351, 2022, doi: 10.1109/ACCESS.2022.3206046.