**TÍTULO**

FIABILIDAD DE LA BLOCKCHAIN EN EL SECTOR SALUD

RELIABILITY OF THE BLOCKCHAIN IN THE IN THE HEALTH SECTOR

**Erika Milena Montaña Caro**1

**Julio Alejandro Pinzón Núñez**2

1Semillero Alfa, Facultad de Ingeniería/Ingeniería de Sistemas/Boyacá, Fundación Universitaria Juan de Castellanos, Tunja, Colombia. emontana@jdc.edu.co

2Facultad de Ingeniería y Ciencias Básicas, Fundación Universitaria Juan de Castellanos, Tunja, Colombia. jpinzon@jdc.edu.co

**Resumen:** Los registros electrónicos de salud (EHR) se presentan como una solución digitalizada para almacenar datos clínicos de pacientes y su historial médico. Sin embargo, se plantea la preocupación por la seguridad y privacidad de esta información. A través de la tecnología blockchain se puede abordar estas preocupaciones mediante la creación de sistemas seguros y descentralizados para el almacenamiento y el intercambio de datos médicos. Las características de distribución, descentralización, inmutabilidad y trazabilidad de los datos almacenados en la blockchain aseguran que los datos permanezcan confiables y seguros.

Se presenta una revisión de la literatura científica en el ámbito del almacenamiento de los registros médicos en la Blockchain para verificar las aplicaciones de esta tecnología en sistemas críticos como los que administran la información médica de las personas.

**Abstract:** Electronic health records (EHR) are presented as a digitized solution to store clinical data of patients and their medical history. However, concerns are raised about the security and privacy of this information. Through blockchain technology, these concerns can be addressed by creating secure, decentralized systems for storing and sharing medical data. The distribution, decentralization, immutability and traceability characteristics of data stored on the blockchain ensure that the data remains reliable and secure.

A review of the scientific literature in the field of storing medical records in the Blockchain is presented to verify the applications of this technology in critical systems such as those that manage people's medical information.

**Palabras Clave**: Blockchain, Registros electrónicos de salud (EHR), Seguridad, Aplicaciones, Algoritmos.

**Keywords**: Blockchain, Electronic Health Record (EHR), Security, Applications, Algorithms.

# INTRODUCCIÓN

Con la llegada de la tecnología varias personas suplen actividades manuales y hacen uso de aplicaciones en su vida diaria, esto facilita el desarrollo de varios oficios profesionales según el entorno que estén. Una de estas tecnologías es la blockchain, esta hace referencia a una base de datos encargada de almacenar y ejecutar transacciones hechas por los usuarios.

El uso de esta tecnología ha ganado amplia aceptación y uno de los sectores en donde se ha popularizado es el de la salud para realizar seguimiento de la cadena de suministro de medicamentos, guardar los registros médicos electrónicos y para compartirlos por la red que almacena toda esta información.

En este artículo se decidió hacer investigación sobre lo relacionado con seguridad de la blockchain en el sector de la salud, puesto que, la persistencia y transparencia son dos de sus características principales, lo que la hace valiosa para garantizar la confianza en situaciones donde la seguridad y la integridad de los datos son fundamentales.

# MATERIALES Y MÉTODOS

* Se realizo una búsqueda exhaustiva de la literatura científica en bibliotecas digitales como Science Direct, a través de parámetros de búsqueda en los campos: palabras claves y título que tenían los términos "Blockchain" y "Seguridad de los datos en el sector de la Salud". Cabe mencionar que se fueron refinando los parámetros de búsqueda como el filtrado por fechas, por categoría, etc.
* Lectura del abstract de las referencias recuperadas en la búsqueda y se evaluó si el artículo era relevante para la investigación, ayudando a determinar cuáles documentos seleccionar para este documento e identificando que recursos bibliográficos tratan o no el tema específico.
* De acuerdo a lo anterior se obtuvo los recursos identificados que tratan el tema, y se hizo lectura de estos.
* Además, se clasifico la temática de los resultados de investigación presentados en los recursos obtenidos y se inició con el documento.

# RESULTADOS

(Aldeco Perez & Rajsbaum, 2022) definen la cadena de bloques, o también conocida como blockchain, como una tecnología innovadora que ha sido ampliamente adoptada en diversas industrias. Se trata de una estructura de datos descentralizada y transparente que permite almacenar y compartir información de manera segura. Esta se compone de bloques que contienen datos y están enlazados entre sí mediante criptografía, formando así una cadena inmutable.

Cada bloque contiene información verificable y registra transacciones o eventos específicos. Una de las características principales de la cadena de bloques es su resistencia a la modificación y al fraude, una vez que los datos se registran en un bloque, se vuelven prácticamente inalterables.

Además, al ser una base de datos descentralizada, consensuada y distribuida entre múltiples nodos pertenecientes a una red permite almacenar información de forma inmutable, ordenada y transparente. Esta red hace transacciones seguras y directas entre participantes. En el sector de la salud, por ejemplo, la cadena de bloques se está utilizando para mejorar la interoperabilidad y seguridad de los datos médicos, al mantener un registro transparente y descentralizado de la información, los profesionales de la salud pueden acceder a los registros médicos de los pacientes de manera rápida y segura (Boček, Rodrigues, Strasser, & Stiller, 2017). La tecnología de blockchain ha comenzado a revolucionar el mundo de la salud al proporcionar una forma segura y eficiente de almacenar y compartir datos médicos.

Los sistemas de registros electrónicos de salud (EHR) son una versión digital de los registros médicos en papel de un paciente que contiene su historial médico completo. Está diseñado para ser utilizado por profesionales de la salud como parte de un sistema integral para gestionar los registros de salud de los pacientes. Los EHR desempeñan un papel crucial en la gestión eficiente de la información del paciente, con el objetivo de mejorar la calidad de la atención médica y los resultados del paciente.

**BLOCKCHAIN**

La blockchain registrar transacciones las cuales son hechas por usuarios, estas se realizan en bitcoin y además se utiliza como criptomoneda o sistema de pago, lo innovador de esta moneda es que es descentralizada, (Academy, 2023). Lo anterior, se considera un avance tecnológico tanto para la criptografía como para la ciberseguridad, igualmente con casos de uso que inician desde sistemas de criptomonedas desplegados a nivel mundial como bitcoin, hasta contratos y redes inteligentes a través del internet de las cosas, (Martí, 2018). Por esta razón, la seguridad y la privacidad de la Blockchain continúan estando en discusión al implementar esta tecnología en diferentes aplicaciones (Rui Zhang, 2019).

Teniendo en cuenta lo anterior, es necesario revisar que soluciones de mejora existen en cuanto a la seguridad para blockchain, y si estas pueden usarse en el desarrollo de las aplicaciones que utilizan esta tecnología, (Xiaoqi Li, 2017).

Cabe mencionar que una red blockchain puede rastrear datos, cuentas, producción y mucho más. (IBM, s.f.). y la cantidad de datos de salud que se pueden recopilar se ha incrementado debido a la digitalización de registros físicos, sensores y otros dispositivos tecnológicos.

(Lee H.-H. , 2013) reconoce el desarrollo de tecnología de la información (TI) y la red, como aspectos clave en el desarrollo empresarial para la implementación de procesos tridimensionales; como la gestión de datos, la colaboración en red y la toma de decisiones. Se puede decir que, Internet es una plataforma eficiente y pública que puede ser utilizada para el intercambio de información y la comunicación el cual permite que múltiples usuarios se conecten y compartan información entre sí, es por lo que se considera equivalente a un sistema de proceso tridimensional.

Debido al correcto funcionamiento de este tipo de tecnología, la cual permite que se almacene la información de los pacientes de una forma segura (Azzi , Chamoun , & Sokhn , 2019) y que esta será prácticamente inalterable y almacenada en múltiples nodos simultáneamente, permitiendo diferentes respaldos en caso de presentar algún tipo de dificultad técnica y asegurándose que la custodia de la información no dependa de un único sitio de almacenamiento.

La implementación, desarrollo y constante mejora de Blockchain en el sector salud es importante, puesto que, es una herramienta tecnológica lo suficientemente potente para el almacenamiento de grandes cantidades de información. Además, brinda garantías en seguridad, como lo mencionan (Pirtle & Ehrenfeld , 2018) buscando tener así un registro único e irrepetible de los datos, lo cual ayuda a la generar certificaciones.

**REGISTROS EHR (Electronic Health Record**)

Según (Chen, 2019), en el sector salud se ha implementado sistemas de registros electrónicos de salud (EHR), consisten en una versión digitalizada de los registros de datos clínicos del paciente e incluso el historial médico. Por contextualizar en Colombia estos registros se conocen como la historia clínica.

En 2020 (Huyun) expuso que los EHR son una recopilación de información relacionada con la salud de las personas, que incluye enfermedades, medicamentos, imágenes médicas e información personal como nombre, edad, sexo, peso e información de facturación. Por lo general, estos datos son confidenciales y deben protegerse contra el acceso no autorizado; por lo tanto, uno de los mayores desafíos en los sistemas de atención médica es compartir datos médicos de forma segura dicho de otra manera sin que se produzcan fugas de datos del paciente (Chen, 2019).

(Lee, Chang, & Raymond, 2020) Consideran que estos datos son confidenciales y deben protegerse contra el acceso no autorizado, por lo tanto, uno de los mayores desafíos en los sistemas de atención médica es compartir datos de forma segura dicho de otra manera sin que se produzcan fugas del dato del paciente.

Estos registros EHR pueden compartir información con proveedores y organizaciones de atención médica mejor dicho para esto fueron diseñados, sin embargo, estos han enfrentado problemas relacionados con la seguridad, privacidad y confidencialidad de los datos (Kumar, 2021).

**EHR EN LA BLOCKCHAIN**

Además, el uso de la tecnología blockchain garantiza la integridad, la protección contra la manipulación y la trazabilidad del índice de EHR (Chen, 2019), y solo los profesionales de la salud que participan en el cuidado de un paciente pueden acceder y utilizar una historia clínica electrónica (Roman, 2019).

A diferencia de los métodos más tradicionales que se usan en este sector la tecnología blockchain proporciona una plataforma que admite una amplia gama de transferencias directas de activos digitales entre pares (Nakamoto, 2009). De igual manera en el sector salud existe una plataforma amigable con la privacidad para datos de atención médica en la nube basada en un entorno blockchain donde el almacenamiento y la ejecución de la computación en datos confidenciales de atención médica en la nube se basa en una red llamada peer to peer (P2P).

Esta red descentralizada se utiliza en todos los equipos informáticos del lugar, por poner como ejemplo los computadores de un hospital (Mohamad, y otros, 2021). Por medio de esta red, se pueden calcular estimaciones para terapias, medicina, remedios de diversas enfermedades e incluso tratar trastornos, utilizando los recursos guardados por estos dispositivos (Shen, Guo, & Yang, 2019). Con estos equipos se puede monitorear y hacer seguimiento médico para corroborar el diagnóstico hecho por el profesional, mejorando así la calidad de la salud.

Según (Chelladurai & Pandian , 2021), la arquitectura distribuida de la Blockchain garantiza que los datos no se procesen en ningún lugar centralizado, por lo que son accesibles para todos los usuarios de la red. Este sistema descentralizado evita los ataques, reforzando y asegurando el sistema. Además, facilita un mejor control de los historiales médicos y de la atención al paciente, al minimizar al doble las prácticas médicas y el seguimiento, ahorrando tiempo y recursos tanto a los profesionales como a los pacientes. El paciente vigilará a dónde va su información y lo conseguirá manteniendo los historiales médicos en una blockchain (Zhang, Schmidt, Blanco, & Lenz, 2018, págs. 1-41).

(Haleem & Javaid, 2021), señalan que los hospitales pueden trazar sus servicios utilizando un marco Blockchain, incluso a lo largo de todo el ciclo de vida mediante el seguimiento de dispositivos tales como marcapasos, monitoreo en tiempo real, etc. Esta tecnología puede utilizarse para mejorar la gestión del historial del paciente, acelerando así las acciones clínicas con un mantenimiento optimizado de los datos.

Este proceso inicia con el paciente, quien es el encargado de compartir sus datos personales con médicos y organizaciones sanitarias, hay que destacar, que esto se realiza con la ayuda de los sistemas EHR (Electronic Health Record). Supongamos que un paciente mantiene sus datos en un sistema en la nube que usa blockchain como plataforma de almacenamiento de datos. El sistema almacenará los datos en la cadena de bloques y cuando el paciente comparta sus datos con el sistema, este será el encargado de proporcionar un servicio de almacenamiento de estos, incluso cuando los datos se compartan con los médicos o las organizaciones de atención médica (Abdalá Al , Bhuiyan, & Kiyomoto, 2019).

Además, estos son registros de datos clínicos de un paciente e incluso el mismo historial médico, esto se lleva a cabo por medio del sistema, allí se almacenan los datos en la cadena de bloques y cuando el paciente comparta sus datos con el sistema este será el encargado de proporcionar un servicio de almacenamiento de datos e incluso cuando estos se compartan con los médicos o las organizaciones de atención, de esta manera se busca llegar a identificar que la aplicación tenga la capacidad de compartir datos clínicos de forma segura.

**CARACTERISTICAS DE SEGURIDAD E INMUTABILIDAD DE ESOS REGISTROS**

La red es compartida y la información se almacena en toda esta, aumentando así la fiabilidad de esta tecnología (Sharples & Domingue, págs. 490–496). Esta información es tratada y distribuida por la blockchain, aunque permanece igual porque sus nodos garantizan la integridad (Springer, 2019), es decir que esta tecnología puede proteger los datos de salud de posibles pérdidas, fraudes o ataques de seguridad, como los ransomware.

En consecuencia, el sistema es el principal responsable de la pérdida de datos. Por lo anterior, la tecnología blockchain garantiza la integridad de los datos, creando propuestas diferentes para solucionar y controlar el efecto de los ataques utilizando un enfoque descentralizado, pero estas soluciones de alguna manera no logran garantizar la privacidad general de los sistemas centrados en el paciente.

Teniendo en cuenta lo anterior, estos registros son una de las aplicaciones más destacadas de blockchain en el sector de la salud, ya que, consiste en un almacenamiento descentralizado y seguro de los datos médicos en la cadena de bloques permitiendo tener un registro detallado y verificable de la información de los pacientes (Medinaceli Diaz, 2020). Por esto se facilita el intercambio eficiente de datos entre profesionales de la salud, garantizando la privacidad y confidencialidad de la información.

Otro punto en el sector salud, es el Cifrado de búsqueda basado en blockchain para compartir registros médicos electrónicos, se destaca un método para compartir este tipo de datos, lo anterior, se basa en la construcción de un índice para EHR (Electronic Health Record) y estos encriptarlos antes de subirlos a la nube pública. El índice EHR se crea a través de expresiones lógicas complejas y se almacena en la cadena de bloques, de modo que un usuario de datos puede usar las expresiones para encontrarlo (mundial, s.f.)

**APLICACIONES DE ESTA TECNOLOGÍA QUE TUVIERON ÉXITO**

La organización que utiliza blockchain es la Mayo Clinic, allí se lleva un registro detallado de los historiales clínicos de sus pacientes y es gracias a esta tecnología que los médicos pueden acceder a la información de manera segura y actualizada, mejorando la calidad de la atención médica y reduciendo los problemas de integración y estandarización de los sistemas de salud (Blockchain, 2021).

En 2019 (Abdalá Al , Bhuiyan, & Kiyomoto; Medinaceli) indicaron que el intercambio de datos en el sistema podía ser controlado por los pacientes. Este almacena los datos personales cifrados para garantizar la privacidad general de los mismos, de modo que incluso si el sistema es atacado, los datos robados no tendrán sentido para ellos. El potencial de la blockchain en la atención médica es superar los desafíos relacionados con la seguridad de los datos, la privacidad, el intercambio y el almacenamiento (Engelhardt, 2017).

En 2019 (Mackey, Kuo, Gummadi, & et al) afirmaron que en el sector de la salud, la tecnología blockchain logro posicionarse de manera positiva frente a los resultados que obtuvo en atención médica de las empresas y las partes interesadas para optimizar los procesos comerciales, mejorar los resultados de los pacientes, la gestión de datos de los mismos, mejorar el cumplimiento, reducir los costos y permitir un mejor uso de los datos relacionados con la atención médica.

Los autores (Lee, Chang, & Raymond, 2020) plantearon una solución basada en blockchain, teniendo en cuenta que es un enfoque viable, el cual permite desarrollar algoritmos criptográficos para garantizar la integridad de los datos, auditorías estandarizadas y algunos contratos formalizados para el acceso a los datos. El sistema propuesto, está diseñado para que solo el índice de búsqueda se agregue a la cadena de bloques para facilitar la distribución de EHR, mientras que los EHR reales se almacenan en un servidor de nube pública en forma encriptada. Cuando los usuarios desean acceder a estos EHR, deben autenticarse ante el propietario de los datos para obtener la autorización junto con la clave de descifrado. Con esta disposición, el propietario de los datos tiene control total sobre quién puede ver sus datos, y además se puede garantizar la privacidad de datos de los pacientes.

Por otra parte, Fast Healthcare Interoperability Resources (FHIR); es una aplicación de Blockchain para compartir datos clínicos de forma segura y escalar, además es esencial para la toma de decisiones clínicas colaborativas y efectivas de tratamiento y atención para los pacientes.

Se puede indicar como ejemplo el momento en el que los pacientes visitan los consultorios de los diferentes proveedores de atención médica, quienes deben poder intercambiar información de salud sobre sus pacientes de manera oportuna y sensible a la privacidad para garantizar que tengan el conocimiento más actualizado sobre las condiciones de salud del paciente. Asimismo, el intercambio de datos también es esencial en la atención de enfermedades como el cáncer, en donde, grupos de médicos con diferentes especialidades, se reúnen en las llamadas juntas de tumores, donde se planea como tratar al paciente; la inteligencia agregada y conocimientos ayudan a los médicos a comprender las necesidades del paciente y, a su vez, a aplicar tratamientos más efectivos en persona y a distancia (Zhang Et al, 2018).

Por otro lado, en EE. UU, el Instituto de Tecnología de Massachusetts (Azaria , Ekblaw , Vieira , & Lippman, 2016), desarrolló MedRed un sistema descentralizado de gestión de registros para manejar las historias clínicas, utilizando la tecnología Blockchain. Este sistema ofrece a los pacientes un registro completo e inmutable, un fácil acceso a su información médica en todos los proveedores y sitios de tratamiento. MedRec junto con la Blockchain gestionan la autenticación, confidencialidad, responsabilidad y el intercambio de datos, consideraciones esenciales para manejar información confidencial.

**PROBLEMAS DE SEGURIDAD**

Teniendo en cuenta a los autores (Zhang Et al, 2018), se puede identificar que existen algunos inconvenientes en cuanto a la infraestructura técnica de los sistemas de TI en la salud, los cuales impiden el intercambio seguro y escalable de datos entre instituciones, dicho de otra manera, esto genera problemas de seguridad y privacidad con respecto a la protección de la identidad y la confidencialidad del paciente, se destaca que los problemas de escalabilidad que se pueden presentar en los conjuntos de datos a gran escala pueden ser difíciles de transmitir electrónicamente debido a la configuración restrictiva del firewall o las limitaciones en el ancho de banda, esto puede afectar el tiempo de respuesta general del sistema y la velocidad de transacción de datos (A.B., 2018).

Cabe resaltar que estos problemas de seguridad y privacidad siguen persistiendo porque existe una necesidad, por mencionar la de compartir los datos, sin embargo, existe la posibilidad y riesgo de alterar esta información, esto se da en la telemedicina, sin embargo, existen algoritmos creados para prevenir este tipo de ataques.

(Casas, 2020) Expone que los registros electrónicos de salud, suelen ser objeto de múltiples ataques de seguridad, donde la pérdida de información puede afectar a un gran número de pacientes cada año. Además, estos sistemas permiten que los usuarios con acceso al sistema realicen modificaciones de manera directa, sin dejar rastro del cambio. Por otro lado, estas soluciones permiten que los registros sean almacenados usando múltiples formatos diferentes, dependiendo del proveedor determinado, y esto puede terminar generando inconsistencias en los análisis, y provocando diagnósticos y tratamientos erróneos que pueden provocar daños, tanto físicos como psicológicos en los pacientes.

**ALGORITMOS**

En el año 2011 (M. Li, págs. 383-392), plantearon un esquema de autorización detallado para que los usuarios tuvieran acceso de búsqueda en fuentes de confianza localizadas según sus atributos. Presentaron dos esquemas autorizados de búsqueda privada de palabras clave (APKS), los cuales estaban basados en cifrado de predicado jerárquico (HPE), para buscar en EHR cifrados en la nube pública. Sus esquemas proporcionan funcionalidades, por mencionarlas, búsquedas multidimensionales de múltiples palabras clave con consulta de rango simple.

Xhafa Et al (2014, págs. 1795–1802), propuso un esquema de búsqueda de palabras clave difusas con ABE anónimo, diseñado para un entorno de nube híbrida. Lo anterior se realizó utilizando una nube privada como proxy para implementar de forma segura sus datos de EHR a la nube pública. También adoptaron el cifrado basado en atributos para lograr un acceso detallado y de control.

De acuerdo a lo anterior Liu et al (2016), mostró un sistema de intercambio de EHR basado en la nube, que admite palabras clave difusas para buscar. Este esquema de búsqueda facilita que un médico (u otro usuario) recupere rápidamente los EHR. Cabe resaltar que este algoritmo también se adopta para autenticar a los usuarios en base a sus atributos.

Guo et al (2016, págs. 1-8), plantearon un esquema de autorización detallado basado en una base de datos relacional. Luego gestionaron un esquema SSE dinámico que soporta reenviar la privacidad y la verificabilidad delegada para los datos de EHR. Los autores utilizaron almacenamiento en la nube e Internet de las cosas (IOT) para facilitar la monitorización remota de pacientes, Yang et al (2017, págs. 1-9).

Teniendo en cuenta lo anterior los sistemas de búsqueda de EHR no admiten el intercambio de datos y tampoco están diseñados para una construcción o aplicación específica. Además, la mayoría de estos esquemas utilizan el mecanismo ABE para realizar un control de acceso detallado. Como son distintos esquemas estos tienen diferentes formas para crear índices, y no existen métodos generales para compartir EHR a pesar de que todos ellos se basan en ABE (Lee W. K., 2019).

Actualmente los sistemas de salud carecen de métodos y criterios para la verificación y autenticación de la identidad a través de las organizaciones. Por ejemplo, los proveedores de servicios de red tienen diferentes políticas estos no reconocen los métodos aplicados por otro servicio de red, es así como se concluye que para el intercambio de datos la opción más factible es a través de mensajería segura y directa (Desalvo K, 2015). Por ello, se lanzó el proyecto directo (HealthIT.gov, 2018) para crear una forma estándar en donde los participantes (usuarios) envían documentos autenticados, los cuales poseen información de salud encriptada directamente a destinatarios conocidos y confiables a través de Internet. En el caso de proveedores o centros de atención que utilizan sistemas EHR sin la integración directa no pueden obtener estos datos por medio del intercambio directo.

Aunque existe la posibilidad que los datos pueden estar encriptados, debido a fallas en los algoritmos de encriptación o el software este tipo de implementaciones pueden exponer el contenido de los datos en el futuro. Para ofrecer seguridad de los datos a largo plazo, es indispensable contar con un diseño de almacenamiento de datos, este puede ser simple, lo que garantiza minimizar los errores de software (Shea R, 2018), sin importar que los datos estén o no encriptados en la cadena, permiten el flujo de datos desde un usuario a otro.

La Blockchain puede proporcionar soluciones para la autenticidad y la trazabilidad de los activos transferidos junto con registros de transacciones auditables y seguros entre las partes interesadas (Chang & Chen, 2020).

Cabe mencionar que la plataforma que relaciona la privacidad de los datos de atención médica en la nube está basada en un entorno de cadena de bloques (E Hendrick, B Schooley, and C Gao). Se han propuesto algunos marcos a nivel nacional basados en la nube para sistemas médicos electrónicos. Patra, et al (págs. 402–405), propusieron un modelo que está basado en la nube y se ocupa de los datos privados de los pacientes. Este modelo asegura la rentabilidad, y dicho sistema fue diseñado para áreas rurales donde el costo juega un papel muy importante. Los profesionales médicos podrían atender a los pacientes de forma remota a través de un modelo basado en la nube que almacena todos estos datos en la misma.

Yin et al. (2017), expusieron un sistema centrado en el paciente basado en la nube. Este modelo incluye tres capas: capa de recopilación de datos, capa de gestión de datos y capa de servicio de datos (Koo, 2016), En este se concedieron los permisos de un administrador para el control de acceso basado en la Blockchain registrando los datos de salud mejorando así la capacidad de interoperabilidad de este sistema.

Por otra parte, la Blockchain garantiza la seguridad de los datos recopilados y ayuda a mantener su privacidad. La información obtenida mediante esta tecnología se analiza utilizando diversas soluciones basadas en inteligencia artificial.

(Sharma, Bahl, Bagha, & Javaid, 2020), Afirmaron que en la pandemia COVID-19, la tecnología Blockchain, desempeño un papel importante en el seguimiento de la propagación del coronavirus. Gracias a esta técnica, se pudo identificar a los pacientes de alto riesgo, y de esta manera se pudo controlar la información de esta infección en tiempo real. Inicialmente fue definida como una base de datos digital que abarcaba información que luego fue utilizada y compartida simultáneamente dentro de una extensa red descentralizada, y fue así, como se demostró el uso de la telemedicina para pacientes diabéticos en la lucha contra la pandemia de COVID-19 (Bahl, Singh, Javaid, & Khan, 2020).

Blockchain ofreció varias soluciones viables en la pandemia, como el seguimiento de brotes, donaciones y la gestión de la cadena de suministro médico. También se usó para establecer un intercambio de datos rápido, y confiable con las partes interesadas. Se evidencio que, en todo el mundo, los hospitales se enfrentaron a la escasez de equipos médicos para luchar contra esta pandemia (Lyengar , Bahl , & Vaishya , 2020, págs. 499-501).

Durante este tiempo se lanzaron muchas plataformas, las cuales utilizaron blockchain para facilitar el intercambio de información y datos valiosos relacionados con COVID-19.

En marzo de 2020 La Organización Mundial de la Salud (OMS) lanzó “MiPasa”. Se trata de una plataforma basada en la blockchain. Esta facilita el intercambio de información totalmente privada entre particulares, autoridades estatales e instituciones sanitarias. La plataforma también les permite a funcionarios de salud pública y a los individuos cargar datos sobre diferentes momentos de la infección y la ubicación exacta (Govindan, Mina, & Alavi , 2020).

En España por ejemplo se desarrolló un proyecto denominado Pasaporte de empleados (PricewaterhouseCoopers, 2020), que tuvo como objetivo en el contexto de la crisis sanitaria y social, desarrollar una solución basada en tecnología Blockchain que habilitaba la introducción y consulta de datos médicos relativos a la información de COVID-19 identificando así el estado de los empleados.

En otro estudio (Griggs, y otros, 2018) adoptaron una blockchain privada, basada en el protocolo Ethereum, para facilitar no sólo el uso seguro de sensores médicos, sino también para erradicar los riesgos de seguridad asociados a un sistema de monitorización remota de pacientes. Su estrategia basada en esta tecnología puede facilitar la monitorización remota segura en tiempo real, permitiendo así a los médicos hacer un seguimiento del estado de salud de sus pacientes desde lugares distantes, al tiempo que mantienen un historial seguro y actualizado de los pacientes.

Por otra parte (Peña , Gutierrez, & Gutierrez, 2020) Sugirieron un modelo de seguridad para proteger los datos de pacientes en sistemas mHealth (salud móvil) utilizando Blockchain. Este modelo se implementa bajo una plataforma de Blockchain que permite recopilar, compartir e integrar los datos de manera segura a través de una aplicación móvil mediante dispositivos mHealth para la atención médica en las clínicas de Perú.

En 2017 (Zheng, Xie, Dai, & Wang), afirmaron que el mecanismo de Blockchain permite a toda la comunidad, indicar que persona es de su confianza, para que ante cualquier eventualidad pueda verificar los registros en una arquitectura blockchain, aunque de esta manera los datos se vuelven propensos a posibles riesgos de privacidad y seguridad.

Finalmente, uno de los desafíos de la Blockchain y quizás el más crucial, es la seguridad y la privacidad de los datos (Kuo , Hsu, & Ohno-Machado, 2016), ya que, con la implementación de aplicaciones basadas en esta tecnología, se busca eliminar la necesidad de un tercero para llevar a cabo una transacción (Alhadhrami, Alghfeli, Alghfeli, Abedlla, & Shuaib, 2017, págs. 1-4).

**CONCLUSIONES**

Los registros electrónicos de salud junto con la tecnología blockchain ha superado desafíos críticos en el sector de la salud, mejorando la seguridad y transparencia de la información médica. Esta integración ha demostrado ser una solución efectiva para garantizar la confidencialidad de los datos y proporcionar una plataforma más segura y transparente para el manejo de registros médicos.

La tecnología blockchain garantiza la responsabilidad e integridad, creando diferentes propuestas para solucionar y controlar el efecto de los ataques utilizando un enfoque descentralizado pero estas soluciones de alguna manera no logran garantizar la privacidad general de los sistemas centrados en el paciente.

Existen inconvenientes en la infraestructura técnica de los sistemas de tecnología de la información en la salud, que impiden el intercambio seguro y escalable de datos entre instituciones, ocasionando problemas de seguridad y privacidad con respecto a la protección de la identidad y la confidencialidad de las personas.

El hecho de implementar la tecnología blockchain en el sector de la salud surge como una solución competente para superar desafíos en la integridad y seguridad de los datos médicos. Además, su capacidad para proporcionar un registro inmutable y descentralizado aumenta la transparencia y credibilidad del sistema de salud, otorgando a los pacientes control sobre sus datos.

# REFERENCIAS

# [1] Abdalá al , 0, Bhuiyan, A, & Kiyomoto, M. (2019). *plataforma amigable con la privacidad para datos de atención médica en la nube basada en un entorno de cadena de bloques.* obtenido de https://doi.org/10.1016/j.future.2018.12

[2] Academy, B. (13 de Abril de 2023). *¿Qué es la minería de criptomonedas o criptominería y cómo funciona?* Obtenido de https://academy.binance.com/es/articles/what-is-crypto-mining-and-how-does-it-work

[3] Aldeco Perez, R., & Rajsbaum, S. (20 de Diciembre de 2022). Obtenido de ¿Qué es Blockchain?: https://www.researchgate.net/publication/366570202

[4] Alhadhrami, Z., Alghfeli, S., Alghfeli, M., Abedlla, A., & Shuaib, K. (23 de Noviembre de 2017). *Introducing blockchains for healthcare.* Obtenido de doi: 10.1109/ICECTA.2017.8252043.

[5] Azaria , A., Ekblaw , A., Vieira , T., & Lippman, A. (2016). *MedRec: Using blockchain for medical data access and permission management.* doi:https://doi.org/ 10.1109/OBD.2016.11

[6] Azzi, R., Chamoun, R., & Sokhn, M. (01 de Septiembre de 2019). *The power of a blockchain-based supply chain.* Obtenido de https://doi.org/10.1016/j.cie.2019.06.042

[7] Bahl, S., Singh, R., Javaid, M., & Khan, H. (Octubre de 2020). *Telemedicine technologies for confronting COVID-19 pandemic.* Obtenido de DOI: 10.1142/S2424862220300057

[8] Blockchain, O. (2021). *Innovaciones Blockchain en el sector Salud*. Obtenido de https://observatorioblockchain.com/hypernifty/blockchain-salud-innovaciones/

[9] Boček, T., Rodrigues, B., Strasser, T., & Stiller, B. (24 de Julio de 2017). *Blockchains everywhere – a use-case of blockchains in the pharma supply-chain.* Obtenido de 10.23919/INM.2017.7987376

[10] C. Guo, R. Z. (2016). *o, Fine-grained database field search using attribute-based encryption .*

[11] Casas, C. O. (2020). *Sistema Seguro de Manejo de Historias Clínicas con base en Blockchain.* Obtenido de http://hdl.handle.net/1992/50750

[12] Chelladurai, U., & Pandian , S. (23 de Marzo de 2021). *Un novedoso sistema de automatización de registros electrónicos de salud basado en blockchain para la atención médica.* Obtenido de https://doi.org/10.1007/s12652-021-03163-3

[13] Chen, L. (Junio de 2019). *Blockchain based searchable encryption for electronic health record sharing .* Obtenido de https://www.researchgate.net/publication/330498481

[14] Desalvo K, G. E. (02 de Abril de 2015). *Connecting Health and Care for the Nation; A Shared Nationwide Interoperability Roadmap.* Obtenido de https://www.healthit.gov/sites/default/files/comments/acp\_comment\_letter\_to\_onc\_on\_draft\_roadmap-final-2015-04-02.pdf

[15] E Hendrick, B Schooley, and C Gao. (2013). Obtenido de IEEE 10th Consumer Communications and Networking Conference (CCNC)

[16] Engelhardt, M. (2017). Enganchar la atención médica a la cadena: una introducción a la tecnología blockchain en el sector de la salud. Revista Tecnología Innov. Manag.

[17] Govindan, K., Mina, H., & Alavi , B. (2020). *A decision support system for demand management in healthcare supply chains considering the epidemic outbreaks: A Case Study of Coronavirus Disease 2019 (COVID-19).* Obtenido de https://doi.org/10.1016/j.tre.2020.101967

[18] Griggs, K., Ossipova, O., Kohlios, C., Baccari, A., Howson, E., & Hayajneh, T. (2018). *Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring.* Obtenido de https://dx.doi.org/10.1007/s10916-018-0982-x

[19] Haleem, A., & Javaid, M. (2021). *Blockchain technology applications in healthcare: An overview.* Obtenido de https://doi.org/10.1016/j.ijin.2021.09.005.

[20] HealthIT.gov. (16 de Julio de 2018). Obtenido de https://www.healthit.gov/test-method/direct-project

[21] Huyun, S. (2020). *Aplicaciones de blockchain para garantizar la seguridad y privacidad de los sistemas.* Elsevier.

[22] IBM. (s.f.). *Blockchain* . Obtenido de https://www.ibm.com/es-es/topics/blockchain

[23] Koo, L. A. (2016). *Blockchain for health data and its potential use in health it and health care related research*. Obtenido de In ONC/NIST Use of Blockchain for Healthcare and Research Workshop

[24] Kumar, R. (23 de Septiembre de 2021). *Tecnología Blockchain para la gestión de la privacidad de los datos.* Obtenido de https://www.taylorfrancis.com/chapters/edit/10.1201/9781003133391-13/blockchain-ehr-

[25] Kuo , T., Hsu, C., & Ohno-Machado, L. (2016). *ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks.*

[26] L. Yang, Q. Z. (2017). *a reliable, searchable and privacy-preserving e-Healthcare system for cloud-assisted body .*

[27] Lee, H.-H. (2013). *How a "3-D" supply chain process system could revolutionize .* Obtenido de Council of Supply Chain Management Professionals (CSCMP)

[28] Lee, W. K., Chang, C.-H., & Raymond, K. (15 de Octubre de 2020). *Blockchain based searchable encryption for electronic health record sharing.* Obtenido de https://www.researchgate.net/publication/330498481

[29] Lyengar , K., Bahl , S., & Vaishya , R. (2020). *Challenges and solutions in meeting up the urgent requirement of ventilators for COVID-19 patients.* Obtenido de https://doi.org/10.1016/j.dsx.2020.04.048

[30] M. Li, S. Y. (2011). *Authorized Private Keyword Search over Encrypted Data in Cloud Computing, in: Proceedings .*

[31] Mackey, T., Kuo, T., Gummadi, B., & et al. (27 de Marzo de 2019). *Desafíos y oportunidades para las aplicaciones de la tecnología blockchain en el futuro de la atención médica.* Obtenido de https://doi.org/10.1186/s12916-019-1296-7

[32] Manas Ranjan Patra, R. K. (2012). Crhis:. *In Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*, 402–405.

[33] Martí, M. S. (04 de Junio de 2018). *Seguridad en la Internet de las cosas. Estudio de IOTA para el Internet of Things.* (U. O. Catalunya, Ed.) Obtenido de http://hdl.handle.net/10609/82145

[34] Medinaceli Diaz, I. (2020). *Blockchain en el ámbito de la Salud.* Obtenido de https://www.redipd.org/sites/default/files/2020-01/xvii-encuentro-p4-Karina-Medinaceli.pdf

[35] Mohamad, K., Defranco, J., Malas, T., Laplante, P., Giuseppe , D., Valdemar , V., & Neto, G. (2021). *Explorando la investigación en Blockchain para la atención médica y una hoja de ruta para el futuro.* Obtenido de 10.1109/TETC.2019.2936881

[36] mundial), C. (. (s.f.). *Desarrollo de Software EHR y Software EMR*. Obtenido de https://www.chetu.com/es/healthcare/ehr-emr-phr.php

[37] Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtenido de https://bitcoin.org/bitcoin.pdf

[38] Peña , N., Gutierrez, C., & Gutierrez, A. (06 de 01 de 2020). *Modelo de seguridad de los datos clínicos para los dispositivos mHealth basado en Blockchain.* Obtenido de http://hdl.handle.net/10757/650348

[39] PricewaterhouseCoopers. (2020). *COVID-19 Pasaporte de empleados.* Obtenido de https://www.pwc.es/es/covid/assets/pasaporte-empleados-covid-19-2.pdf

[40] Roman, L. (10 de Agosto de 2019). EMR, EHR y PHR combinados administran los datos para una mejor salud. págs. 40-78.

[41] Rui Zhang, R. X. (2019). Seguridad y Privacidad en Bolckchain. *ACM Computing Surveys*, 34. Obtenido de https://doi.org/10.1145/3316481

[42] Sharma, A., Bahl, S., Bagha, A., & Javaid, M. (22 de Octubre de 2020). *La tecnología Blockchain y sus aplicaciones para combatir la pandemia COVID-19.* Obtenido de https://doi.org/10.1007/s42600-020-00106-3

[43] Sharples, M., & Domingue, J. (2016). La cadena de bloques y las felicitaciones: un sistema distribuido para el registro educativo, la reputación y la recompensa. Europa: Springer.

[44] Shen, B., Guo, J., & Yang, Y. (22 de Marzo de 2019). *MedChain: Intercambio eficiente de datos de atención médica a través de Blockchain.* Obtenido de https://doi.org/10.3390/app9061207

[45] Springer. (2019). Distributed immutabilization of records. *International Workshop on Security and Trust Management*, 122-137.

[46] Xiaoqi Li, &. P. (2017). *Una encuesta sobre la seguridad de los sistemas blockchain.*

[47] Yin Zhang, M. Q.-W. (2017). Health-cps: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal*, 88–95.

[48] Z. Liu, E. a. (2016). *Cloud-based electronic health record system supporting fuzzy keyword search, Soft Comput.*

[49] Zhang, P., Schmidt, D., Blanco, J., & Lenz, G. (2018). *Blockchain Technology Use Cases in Healthcare.* Obtenido de https://doi.org/10.1016/bs.adcom.2018.03.006

[50] Zheng, Z., Xie, S., Dai, H., & Wang, H. (30 de junio de 2017). Obtenido de Una visión general de la tecnología blockchain: Arquitectura, consenso y tendencias futuras.