Integración de la tecnología Blockchain con procesos de gestión de registros médicos en la atención y prestación de servicios de salud

Andrés Favián Cáceres Ramírez, Zaira Sharick Flórez Guadrón, MBA. Néstor Fabián Santos Nova

***Abstract*—Este Proyecto busca integrar la tecnología blockchain con los procesos de gestión de registros médicos en entidades prestadoras de servicios de salud. La gestión eficiente y segura de los registros médicos constituye un desafío persistente en el sector salud, exacerbado por la creciente incidencia de violaciones de datos y una interoperabilidad insuficiente entre los sistemas de información sanitaria. Se abordan problemáticas actuales en la gestión de registros médicos electrónicos tanto en Colombia como a nivel mundial. Mediante un análisis detallado de literatura y la evaluación de casos de uso específicos, este trabajo identifica y propone vías de integración de Blockchain que prometen mejoras significativas en la seguridad de la información, la privacidad del paciente y la eficiencia operativa. Por medio de la adopción de blockchain y la computación en la nube, el proyecto crea un entorno seguro y eficiente para el almacenamiento, monitoreo y verificación de la información médica, tratando aspectos críticos como la privacidad de los pacientes y la tolerancia a fallas, señalando un cambio de paradigma hacia sistemas de salud más integrados y transparentes adaptado a las necesidades de la industria.**

***Index Terms*— Blockchain, cloud computing, interoperabilidad, registros medicos, salud.**

I. Introduction

EL presente trabajo de investigación tiene como objetivo principal analizar la integración de la tecnología Blockchain con los procesos de registros médicos electrónicos, centrándose en instituciones de atención y prestación de servicios en salud. La presente problemática en el sector salud colombiano y la violación de millones datos de salud a nivel mundial, caracterizados por la falta de eficiencia en la gestión de registros médicos y seguridad de estos, la ausencia de interoperabilidad entre sistemas de información motiva la necesidad de buscar soluciones innovadoras para superar estos desafíos.

La justificación de esta investigación se fundamenta en los problemas existentes en el sector salud, incluyendo la escasez de recursos y personal capacitado, lo que afecta la eficacia y eficiencia del sistema de atención médica. La tecnología Blockchain, reconocida por su transparencia y red distribuida segura, surge como una alternativa que podría mejorar la gestión de registros médicos electrónicos, ofreciendo una solución innovadora a los problemas actuales.

La relevancia de este proyecto radica en su contribución al avance y modernización de los registros médicos electrónicos, permitiendo a los usuarios ser dueños y acceder a su propia información para así mejorar la calidad de la atención médica. Con la combinación de Blockchain y tecnologías como Cloud Computing, se busca crear un entorno seguro y eficiente para el almacenamiento, monitoreo y verificación de información, abordando aspectos críticos como la privacidad y la tolerancia a fallas. Este trabajo de investigación busca generar conocimientos que impulsen la adopción de tecnologías innovadoras en la salud y la gestión de sistemas de información, mejorando la gestión de registros médicos y beneficiando a pacientes y profesionales de la salud.

II. Revisión de literatura

A. Análisis de literatura

La tecnología blockchain ha transformado múltiples sectores más allá de las criptomonedas, mejorando procesos y eficiencia en banca, cadena de suministros, salud y telecomunicaciones, entre otros. Se busca entender los proyectos realizados, métodos aplicados y la gestión en su desarrollo.

Park et al. [1], destacan los beneficios de la blockchain en la gestión de registros de salud por su seguridad y capacidad de descentralización, aunque su implementación enfrenta desafíos legales, técnicos y sociales.

Indumathi et al. [2] proponen una arquitectura basada en blockchain, IoMT y almacenamiento en la nube para mejorar la gestión de datos médicos, destacando la importancia del blockchain para el futuro de la atención médica.

Tanwar et al. [3], examinan las ventajas del blockchain en registros médicos electrónicos, resaltando mejoras en seguridad, eficiencia y la posibilidad de interoperabilidad entre bases de datos de salud.

Poongodi et al. [4] resaltan la combinación de blockchain e IoT para mejorar la monitorización de la salud de los pacientes, apuntando a beneficios como eficiencia y precisión diagnóstica.

Xu et al. [5] enfatizan la importancia del blockchain en la autenticación de identidades en hogares inteligentes, destacando el papel de los Smart Contracts de Ethereum y la

integración de la computación en la niebla para la seguridad.

La tecnología blockchain, según Reegu et al. [6], proporciona un sistema seguro y descentralizado para almacenar y compartir datos en entornos de atención médica, asegurando la confidencialidad. sugieren un marco que combina blockchain con HIPAA para mejorar la seguridad y privacidad en el cuidado de la salud, aunque enfrenta desafíos de escalabilidad y regulación.

Jennath et al. [7] introducen un entorno de intercambio seguro de datos médicos utilizando blockchain e inteligencia artificial, permitiendo a los pacientes controlar el acceso a su información, aunque asumen limitaciones tecnológicas en hospitales.

III. Identificación de Posibilidades de Integración

Se realiza una revisión documental para la identificación de posibilidades de integración.

A. Análisis de las Posibilidades de Integración

1. Revisión de Sistemas Actuales de EHR en instituciones de salud: En la última década, se ha desencadenado a nivel global la incorporación de nuevas tecnologías para la gestión cotidiana de los EHR. La Organización Mundial de la Salud (OMS) ha reconocido los registros médicos como activos que demandan innovación y cuyo intercambio trasciende su utilidad primaria. Estos registros han emergido con el potencial de impactar significativamente en la calidad de vida a nivel mundial [8].

Debido al vasto volumen diario de datos, el procesamiento, análisis y almacenamiento eficaz a nivel local se vuelve casi imposible. Por ello, muchos proveedores de atención médica optan por trasladar sus datos al ámbito público. Sin embargo, la falta de interoperabilidad en la información médica representa una amenaza, dificultando los análisis y tratamientos, ya que los datos están dispersos en lugares como hospitales, farmacias y clínicas. Se destaca la necesidad de una infraestructura más integrada para permitir la interoperabilidad y el intercambio seguro de información médica entre diversos dominios de atención [9].

En Turquía, se ha evaluado la adopción de Historias Clínicas Electrónicas (EHR) a nivel nacional para mejorar la calidad de los servicios de salud. Entre 2014 y 2017, EE. UU. experimentó un aumento en hospitales con funciones integrales de EHR (25,5% al 39,1%) y una disminución en funciones básicas (58,9% al 41,4%). En Turquía, durante el mismo período, el 63,1% de los hospitales tenía funciones básicas y el 36% funciones integrales. Estudios comparativos destacan un significativo aumento en la adopción de EHR en China, del 18,6% al 85,3% de 2017 a 2018, y en EE. UU., del 9,4% al 96% de 2008 a 2017 [10].

2. Limitaciones y desafíos en la gestión de registros médicos: Las limitaciones en la gestión de registros médicos electrónicos (EHR) se centran en su impacto negativo en la atención personalizada y la interacción médico-paciente. La dinámica médico-computadora-paciente ha reemplazado la atención cara a cara, afectando el razonamiento clínico y perdiendo la narrativa humana. Informes indican que, en promedio, personal médico dedica alrededor del 50% de su tiempo laboral interactuando con la pantalla del EHR en lugar de atender directamente a los pacientes. La introducción de información en la computadora, con múltiples clics del ratón, representa una carga significativa, consumiendo más del 40% de un turno típico de 10 horas y generando más ruido que información clínica relevante. Esto impacta negativamente la eficiencia y calidad de la atención médica [11].

La concentración de información en un solo servidor presenta la amenaza del Punto Único de Fallo (SPoF), comprometiendo la certeza sobre la disponibilidad de datos. Este desafío en la gestión de registros médicos electrónicos sugiere que la interrupción o fallo del servidor podría llevar a la inaccesibilidad total de información crítica. Este riesgo plantea dudas sobre la continuidad y accesibilidad de datos cruciales, resaltando la necesidad de enfoques más resilientes y distribuidos en el diseño de sistemas de gestión de EHR [12].

Continuando con las limitaciones de los EHR, según el metaanálisis realizado por Windari et al. [13], otros desafíos como los altos costos de implementación, especialmente en áreas rurales, preocupaciones sobre la seguridad de los datos ante ciberataques, resistencia de usuarios y falta de experiencia informática en profesionales de la salud. Se proponen soluciones como un liderazgo efectivo, un ambiente positivo, y una educación y capacitación integral.

Peterson et al. [14] , definen la interoperabilidad de los registros sanitarios, destacando desafíos en la estructura y semántica. La complejidad y heterogeneidad de los datos sanitarios dificultan la implementación de estándares propuestos, tanto por la falta de consenso como por la alineación con diversos estándares. La semántica requiere un consenso en esquemas de codificación para garantizar un intercambio efectivo de datos sanitarios. La limitación principal radica en la dificultad para establecer un estándar autorizado y alcanzar consenso en la codificación semántica.

3. Casos de implementación exitosa de blockchain: Hai et al. [15], proponen el marco BVFLEMR, que integra blockchain y aprendizaje federado para mejorar la seguridad y ofrecer recomendaciones de tratamientos personalizados en la gestión de EHR. Utilizan Hyperledger Fabric para el almacenamiento en blockchain, abordando desafíos de privacidad en la descentralización de datos de salud. El marco consta de dos partes esenciales: almacenamiento seguro en blockchain y recopilación de datos mediante aprendizaje federado para procesamiento distribuido sin compartir datos crudos. Proporciona una solución integral para mejorar la eficiencia y privacidad en la gestión de datos de salud y la recomendación de tratamientos personalizados, fundamentado en una implementación de tecnología blockchain.

Tuler De Oliveira et al. [16] propone SmartAcces, como una solución para el intercambio seguro de información médica entre organizaciones. Abordando desafíos cruciales como políticas de acceso compartido, adaptabilidad dinámica en el control de acceso y la transparencia en el manejo de datos. SmartAccess utiliza contratos inteligentes que imitan la granularidad del modelo de control de acceso basado en atributos (ABAC). En la red blockchain, los responsables del

tratamiento definen políticas de acceso en consenso, respaldadas por atributos validados, proporcionando una respuesta integral para aplicaciones en el ámbito de la atención médica, respaldada por pruebas de concepto y una evaluación exhaustiva de seguridad.

B. Mejoras potenciales en el sistema actual de salud.

1. Áreas de la salud donde la blockchain aborda problemas existentes: Blockchain presenta una variedad extensa de aplicaciones y utilidades en el ámbito de la salud. Al posibilitar la transferencia segura de información médica de pacientes, supervisar la cadena de suministro de medicamentos y facilitar la transmisión segura de los historiales médicos, convirtiéndose en una herramienta valiosa para los investigadores en el campo de la atención médica, permitiéndoles explorar códigos genéticos. Debido a su capacidad para respaldar análisis innovadores, las empresas del sector de la salud pueden observar cambios en sus datos en tiempo real, otorgándoles la capacidad de tomar decisiones rápidas sin intervención humana [17].

En el área de la salud el Blockchain tiene grandes posibilidades de aplicación en la gestión de la cadena de suministro de medicamentos y a partir de ahí se destaca que esta tecnología tiene el potencial de revitalizar eficazmente sectores industriales, abarcando áreas como el transporte marítimo, la fabricación, la automoción, la aviación, las finanzas, la energía, la atención sanitaria, la agricultura y la alimentación, el comercio electrónico, entre otros [18].

En la gestión de información sanitaria específicamente se encuentran importantes aplicaciones y que son de suma importancia en los procesos de gestión de información en el sector salud, estas incluyen aplicaciones en el seguimiento de recetas de opioides, información sobre el cáncer controlada por el paciente, telemedicina, atención de telesalud, identificación de pacientes, reclamaciones de seguros y registros médicos de los pacientes [19].

2. Evaluación de Beneficios Potenciales: En general, blockchain puede proporcionar un sistema de información seguro y aumentar la motivación de los pacientes para compartir registros médicos. Según Sadeghib R et al [19], blockchain puede mejorar significativamente la eficiencia y seguridad en el intercambio de registros médicos, lo que beneficia tanto a los pacientes como a los proveedores de atención médica. Además, destacan que blockchain permite a los médicos realizar un seguimiento de los registros sanitarios de los pacientes en segundos, lo que mejora la precisión y la disponibilidad de los registros sanitarios. También se menciona que el sector sanitario puede ahorrar alrededor de 100.000 millones de dólares empleando la tecnología blockchain en los sistemas de información sanitaria.

Las cadenas de bloques ofrecen cinco beneficios clave en comparación con los sistemas tradicionales de gestión de bases de datos de atención médica. Proporcionando una gestión descentralizada, para la colaboración entre las partes interesadas sin intermediario. En segundo lugar, proporcionan pistas de auditoría inmutables, útiles para bases de datos inalterables, como informes de reclamaciones de seguros. En tercer lugar, permiten la procedencia de los datos, como el consentimiento del paciente en ensayos clínicos aumentado la reutilización de datos verificados. En cuarto lugar, garantizan la solidez y disponibilidad de los datos, para la preservación y disponibilidad continua de registros médicos electrónicos de pacientes. Por último, mejoran la seguridad y privacidad de los datos al cifrarlos en blockchain y permitir el descifrado solo con la clave privada del paciente [20].

C. Soluciones Propuestas con Blockchain.

1. Modelos de Integración blockchain en los procesos de EHR: El proyecto EdgeMediChain, propuesto por Akkaoui et al. [21] , es una innovadora plataforma descentralizada para el intercambio de datos médicos basada en tecnología blockchain y tecnologías de borde. Su objetivo es mejorar la seguridad, privacidad y eficiencia en el compartir datos de salud entre pacientes, profesionales de la salud, investigadores y aseguradoras, mediante un marco de trabajo de cuatro capas que permite el control de acceso y la autonomía de decisiones a través de contratos inteligentes. Este enfoque asegura una mayor escalabilidad, fiabilidad y trazabilidad, demostrando ser una solución eficaz para la compartición segura de información de salud.

La infraestructura MediBlocks, diseñada por Babu et al. [22], utiliza la tecnología blockchain para asegurar la transmisión segura de registros médicos electrónicos (EHR), incorporando un sistema de validación de transacciones mediante consenso y almacenamiento de datos en un formato seguro fuera de la cadena. A través de un Proveedor de Servicios de Membresía (MSP) y la Autoridad Certificadora (CA), garantiza la autorización y verificación de usuarios, utilizando Hyperledger Fabric para mantener la integridad de la información médica. MediBlocks se destaca por permitir el intercambio seguro y eficiente de EHR, mejorando la atención médica y protegiendo la privacidad y autenticidad de los registros.

Reegu et al. [6] presentan BCIF-EHR, un marco interoperable basado en blockchain para mejorar la colaboración entre entidades sanitarias, asegurando la privacidad y seguridad de los registros médicos electrónicos a través de una infraestructura que facilita el intercambio e integración de datos de salud. Este sistema pone énfasis en el control del paciente sobre sus registros, utilizando tecnología blockchain y técnicas avanzadas para lograr interoperabilidad entre los estándares HL7 y FHIR, abordando el desafío de los registros médicos duplicados con herramientas específicas para su detección y gestion.

2. Consideraciones éticas y legales: En 2019, se reportó un aumento significativo en las violaciones de datos en el sector salud, triplicando el número de registros afectados a más de 41 millones, en comparación con años anteriores. Este incremento, exacerbado por el trabajo remoto durante la pandemia, resultó en la venta de datos en línea y chantajes a pacientes, con un destacado ataque cibernético comprometiendo 21 millones de registros. Este panorama subraya la vulnerabilidad de los sistemas de registros médicos electrónicos ante incidentes de seguridad [23].

La implementación de blockchain en la gestión de información de salud requiere una estrecha colaboración con reguladores y proveedores de atención médica para cumplir con

regulaciones rigurosas, asegurando la protección de la privacidad y seguridad de los datos médicos. Es fundamental ajustarse a las normativas existentes para garantizar una implementación segura y conforme a la ley [19].

La adopción de blockchain en registros médicos introduce complejidades éticas y legales, desde asegurar la precisión y evitar sesgos en algoritmos, hasta cumplir con obligaciones legales. Estas consideraciones exigen una gestión cuidadosa para beneficiar plenamente de la tecnología sin comprometer aspectos éticos o legales [18].

Integrar EHR en blockchain podría requerir cambios profundos en los sistemas actuales y una inversión significativa en infraestructura y formación para los profesionales de la salud, subrayando la necesidad de un compromiso sustancial para superar estos desafíos [6].

Además, es crítico abordar cuestiones organizativas y éticas en contextos de bajos ingresos, donde la capacitación y el apoyo técnico son fundamentales para implementar efectivamente soluciones basadas en blockchain [24].

En conclusión, la transición hacia blockchain en el sector salud implica consideraciones complejas que van más allá de la tecnología, incluyendo el cumplimiento regulatorio, la privacidad, la confidencialidad, el consentimiento informado, la transparencia, la responsabilidad ética, la capacitación adecuada, el desarrollo ético de algoritmos para evitar sesgos, la auditoría periódica de la integridad de los datos, el gobierno de datos y la actualización continua de tecnologías y regulaciones.

IV. Planteamiento de integración y análisis de beneficios

A) Identificación de Requisitos y Casos de Uso:

Akkaoui et al. [21] proponen EdgeMediChain, un modelo que garantiza la gestión eficiente de los Registros Médicos Electrónicos (EMR) entre proveedores de atención médica. Este modelo incorpora dispositivos IoT médicos para adquirir datos en tiempo real, permitiendo su registro y compartición para análisis y seguimiento por parte de profesionales de la salud. Gracias a una autenticación robusta y control de acceso, se reduce el riesgo de ataques cibernéticos, preservando la privacidad de los pacientes y posibilitando la recopilación e intercambio de datos para fines investigativos.

Dentro del marco de EdgeMediChain, especifica el uso de Go-Ethereum (Geth) y Solidity para los contratos inteligentes, y detalla un testbed con máquinas virtuales ejecutando Ubuntu. Esto permite simular tanto un blockchain global con Proof of Work (PoW), como pools de minería en el borde con Proof of Authority (PoA), adaptándose a las necesidades de latencia y seguridad. Las interacciones con la plataforma blockchain se realizan mediante Node.js y web3.js, asegurando la fluidez en las transacciones[21].

Por otro lado, Babu et al. [22] presentan MediBlocks, un sistema que permite a los pacientes gestionar sus EHR de manera segura a través de una Interfaz de Usuario (UI). Este modelo garantiza la reserva de citas, la generación de registros de salud y el acceso controlado a datos por parte de laboratorios y farmacias. La implementación de capas de transporte y cifrado aseguran la privacidad de los registros, mientras que la distribución de datos mejora la redundancia y resistencia ante fallos.

Egala et al. [25] en Fortified-Chain, aseguran la integridad de los datos del paciente provenientes de dispositivos de IoMT, mediante la computación híbrida y medidas de anonimato. Este modelo establece requisitos técnicos específicos para la autenticación de dispositivos IoMT, control de acceso y anonimato del paciente, utilizando criptografía y técnicas de acceso selectivo.

Bera et al. [26] proponen un modelo que integra Blockchain, IA y IoMT para el monitoreo de pacientes durante la pandemia de COVID-19. La implementación se realiza con dispositivos inteligentes portátiles, fog servers y un blockchain privado, asegurando la privacidad y la integridad de los datos mediante cifrado y algoritmos de IA.

Hai et al. [15] presentan BVFLEMR, un modelo que combina blockchain con aprendizaje federado para recomendaciones médicas personalizadas. Este modelo se enfoca en la seguridad y privacidad de los datos, utilizando Hyperledger Fabric y modelos de aprendizaje automático para garantizar la protección de la información sensible del paciente.

Finalmente, Cernian et al. [27] proponen PatientDataChain, un modelo que integra registros médicos electrónicos en un sistema descentralizado mediante tecnología blockchain. Este modelo permite la interoperabilidad entre proveedores de servicios de salud y otorga control de datos a los pacientes, con la capacidad de fusionar datos de diversas fuentes sin alterar sistemas EHR existentes.

B) Análisis de Mejoras y Cuantificación de Beneficios:

1. Identificación de métricas claves

Las métricas de rendimiento en un sistema de registros médicos electrónicos son fundamentales para evaluar su operatividad. Estas incluyen la latencia, el throughput, el uso de recursos computacionales y la escalabilidad, proporcionando una comprensión completa del desempeño del blockchain y guiando las estrategias de mejora continua.

La sostenibilidad del sistema se ve reflejada en métricas como el consumo de gas y de energía. El gas controla el esfuerzo computacional en la red, mientras que el consumo de energía es crucial para la escalabilidad y la responsabilidad ambiental. Estas métricas son vitales para garantizar un uso eficiente de los recursos y prevenir abusos [28].

La gestión de identidades y el control de acceso son esenciales para regular la interacción de los usuarios con los datos. Medir aspectos como tiempos de respuesta y tasas de accesos no autorizados bloqueados contribuye a mejorar la seguridad y la eficiencia del sistema [29].

La interoperabilidad entre sistemas de información es facilitada por métricas como la compatibilidad con estándares internacionales, garantizando el intercambio seguro y eficiente de datos entre instituciones y países [30].

Las métricas relacionadas con el usuario, como la satisfacción y la facilidad de uso, son cruciales para entender su experiencia con el sistema. La transparencia y la precisión en los registros médicos son fundamentales para generar confianza y cumplir con regulaciones legales [31].

El impacto clínico de la implementación del blockchain se mide a través de métricas que evalúan mejoras en la toma de decisiones clínicas y en la atención al paciente, permitiendo

tomar decisiones informadas sobre el rendimiento del sistema [32].

Para evaluar la viabilidad financiera y económica del sistema, se consideran métricas como los costos de implementación, despliegue y mantenimiento, así como el retorno de la inversión. Estos aspectos ofrecen una visión integral de los aspectos financieros involucrados en el sistema [33].

La seguridad y privacidad del sistema se garantizan mediante métricas que evalúan la integridad de los registros, el cumplimiento regulatorio, la detección y mitigación de brechas de seguridad, entre otros. Estas métricas fortalecen la confianza en el entorno blockchain y aseguran el manejo ético de los datos médicos [34].

C) Explicación de Técnicas para la Gestión de Datos en la Integración

1. Análisis de requisitos de Datos

Es fundamental comprender los requisitos y la gestión de datos en un sistema basado en blockchain, comenzando por la identificación y protección de datos sensibles, como la información personal de salud (PHI) sujeta a regulaciones como HIPAA en los Estados Unidos. La PHI abarca diversos tipos de datos, desde registros médicos electrónicos hasta información de facturación, y su protección es crucial para evitar repercusiones legales y daños a la privacidad de los individuos.

Para proteger estos datos, se emplean técnicas como el cifrado y la anonimización, siendo la k-anonimización una herramienta valiosa para preservar la privacidad de los pacientes. Sin embargo, factores como los datos cuasi-identificadores pueden representar riesgos para la privacidad y requieren estrategias adicionales de protección [35].

La gestión de acceso y control de datos es otro requisito esencial, definiendo quiénes tendrán acceso a qué datos en diferentes situaciones, incluyendo pacientes, proveedores de salud e investigadores. El consentimiento del paciente y la propiedad de los datos son fundamentales, y la blockchain ofrece soluciones para gestionar el consentimiento de manera transparente a través de contratos inteligentes [7].

La interoperabilidad entre sistemas y organizaciones es necesaria para facilitar el intercambio seguro y eficiente de datos, utilizando estándares como HL7 y FHIR. El análisis de datos, incluyendo algoritmos de machine learning y procesamiento de lenguaje natural, puede mejorar la interoperabilidad al mapear datos entre diferentes formatos y estándares [36].

Cumplir con requisitos regulatorios locales e internacionales, como HIPAA en los Estados Unidos y GDPR en Europa, es esencial para garantizar el cumplimiento legal y ético en la gestión de datos de salud. Estos requisitos regulan la seguridad y privacidad de la información, asegurando que los sistemas cumplan con los más altos estándares de protección de datos [37].

2. Modelado de datos

En la fase de modelado de datos para sistemas basados en blockchain, se prioriza la accesibilidad, seguridad e integridad de la información. La elección del tipo de base de datos es crucial, considerando la flexibilidad necesaria para la diversidad de datos de salud. Las bases de datos NoSQL y en la nube ofrecen alternativas superiores para manejar datos complejos y no estructurados, mientras que sistemas como IPFS mejoran la accesibilidad y persistencia de los datos en un entorno descentralizado [38] y [12].

La normalización y desnormalización de datos se evalúan en función de la integridad y el rendimiento. Se aplican técnicas estadísticas para estandarizar mediciones y evitar redundancias que comprometan la precisión del tratamiento médico. El hashing se utiliza para proteger la confidencialidad y reducir la carga de la red, almacenando solo hashes en la blockchain y manteniendo los datos detallados de forma segura fuera de la cadena [39].

Las regulaciones como el GDPR en Europa establecen requisitos específicos para la eliminación de datos personales, lo que requiere enfoques cuidadosos, como el uso de contratos inteligentes para la gestión de acceso y técnicas de encriptación para garantizar la privacidad incluso después de la eliminación de la clave de encriptación [40] y [41].

Los contratos inteligentes son fundamentales para gestionar datos médicos de manera segura y precisa, utilizando plataformas como Ethereum o Hyperledger Fabric [42]. La implementación de identificadores únicos, como UUID o DID, facilita el rastreo y acceso a los registros médicos sin comprometer la privacidad, promoviendo la interoperabilidad y el control autónomo sobre las identidades digitales [43].

Integrar estos conceptos en un sistema de registros médicos electrónicos basado en blockchain garantiza seguridad, eficiencia y adaptabilidad, cumpliendo con las regulaciones de salud y promoviendo la escalabilidad para satisfacer las necesidades clínicas y administrativas en evolución.

3. Criptografía para Seguridad de Datos

La criptografía desempeña un papel esencial en la seguridad de los datos en la tecnología blockchain, dividiéndose en criptografía simétrica y asimétrica. La simétrica utiliza claves privadas y públicas, mientras que la asimétrica emplea un único protocolo HTTPS, siendo más económica [44]. La criptografía de curva elíptica ofrece ventajas sobre el RSA, como claves más cortas y mayor eficiencia. Por otro lado, la encriptación basada en atributos (ABE) permite el acceso a datos basado en criterios definidos, siendo útil en escenarios dinámicos [45].

La criptografía basada en hash utiliza funciones deterministas para crear un resumen digital del mensaje, resistente a la pre-imagen y colisiones. Aunque requiere claves de un solo uso, su resistencia a la computación cuántica lo hace relevante en la era post-cuántica [46]. RSA y AES son algoritmos ampliamente utilizados, con RSA basado en factorización de números primos y AES conocido por su seguridad y eficiencia [47] y [48].

4. Estandarización de datos

La estandarización de datos en salud, mediante estándares como HL7 y FHIR, facilita la interoperabilidad entre sistemas. HL7, aunque flexible, puede dificultar la interoperabilidad, mientras que FHIR estructura la información en recursos, permitiendo una integración más simple. El mapeo de datos es crucial para garantizar la coherencia entre sistemas, implicando una transformación exhaustiva de formatos y reglas claras para la transformación. En el contexto de blockchain, la inmutabilidad de los registros y la descentralización plantean desafíos adicionales en la estandarización de datos [49] y [50].

D) Recomendaciones para Implementaciones Futuras

1) Análisis de Tendencias Tecnológicas

Es crucial explorar los desarrollos recientes de la tecnología blockchain en el sector de la salud, especialmente los protocolos innovadores que prometen una gestión más eficaz, segura y rápida de los registros médicos electrónicos (EHR). Ejemplos como EdgeMediChain y MediBlocks demuestran cómo la implementación de contratos inteligentes y políticas de control de acceso restringido puede garantizar una compartición segura de datos de salud entre múltiples partes. La criptografía de curva elíptica (ECC) ofrece una capa adicional de seguridad al cifrar y descifrar datos, generando claves más desafiantes de descifrar, lo que la convierte en la próxima generación en criptografía de clave pública [21] y [22].

La integración de blockchain con tecnologías emergentes como la inteligencia artificial (IA) y el Internet de las Cosas Médicas (IoMT) es fundamental para revolucionar la atención médica. Investigaciones como las de Indumathi et al. [2] y Jennath et al. [7] proponen arquitecturas integrales que aprovechan estas sinergias para mejorar la administración de datos y ofrecer atención médica personalizada y eficiente. Además, la adopción de estándares de interoperabilidad como HL7 y FHIR es esencial para facilitar un intercambio efectivo de información de salud entre sistemas de EHR diferentes, garantizando un flujo de datos coherente y accesible.

Es importante no solo evaluar las tecnologías y modelos existentes, sino también anticipar futuras innovaciones en el campo de la salud digital. Esto incluye el seguimiento de avances en criptografía, como la criptografía cuántica, y el análisis del impacto de las regulaciones actuales y futuras en el desarrollo de nuevas tecnologías y protocolos. Estos factores son fundamentales para una adopción exitosa de avances e innovaciones tecnológicas en la gestión de EHR con blockchain, asegurando prácticas seguras, eficientes y centradas en el paciente en el ámbito de la salud digital.

E) Planteamiento de la Integración de Blockchain y Cloud Computing

1. Diagrama de interacción:

La integración de Blockchain y la Computación en la Nube en la gestión de registros médicos electrónicos (EHR) es esencial para fortalecer la protección de datos, facilitar la interacción entre sistemas y optimizar el procesamiento de información sanitaria. Identificar las operaciones clave en la administración de EHR, como la recolección de información de salud, la conservación segura de datos y el acceso y compartición de expedientes médicos, es fundamental para comprender cómo estas tecnologías pueden beneficiar la gestión de registros médicos.

En cuanto a los procesos administrativos, se incluye el registro de pacientes, el agendamiento de citas, la facturación y procesamiento de pagos, así como la gestión de consentimientos. Los procesos clínicos abarcan el acceso a historiales médicos, la gestión de prescripciones médicas, el procesamiento de órdenes médicas y el monitoreo de la salud del paciente. Además, se consideran los procesos de soporte técnico y seguridad, como la interoperabilidad y compartición de datos, y la generación de reportes de salud y análisis de datos.

Se identifican los actores involucrados en el sistema de EHR, como pacientes, profesionales de la salud, administradores de EHR, proveedores de tecnología Blockchain, proveedores de servicios de Cloud Computing, reguladores de salud y desarrolladores de software. Cada actor tiene responsabilidades específicas y desempeña roles clave en la gestión de registros médicos electrónicos.

El mapeo de interacciones entre los actores y el sistema EHR permite comprender cómo interactúan entre sí y con el sistema, considerando los roles y responsabilidades definidos. Esto incluye el intercambio de datos, la solicitud de servicios y cualquier otra forma de colaboración, tanto directa como indirecta. Estas interacciones proporcionan información crucial para establecer un flujo de datos y de trabajo efectivo en el sistema de EHR.

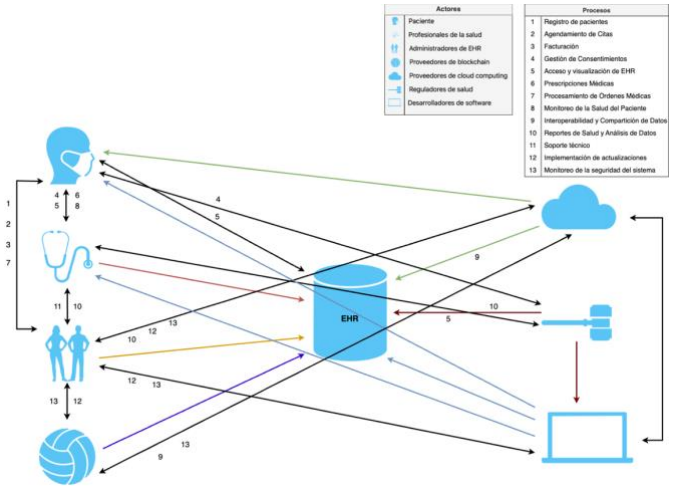

Fig. 1. Representación gráfica de interacciones.

La integración de la criptografía de curva elíptica (ECC) con tecnologías de blockchain y cloud computing representa un avance significativo en la protección de datos en los registros electrónicos de salud (EHR). La ECC facilita el cifrado eficiente y seguro de datos, asegurando la protección de información sensible en el sector salud y cumpliendo con regulaciones como HIPAA. Además, la implementación de contratos inteligentes basados en ECC agiliza la gestión de consentimientos y autorizaciones de acceso, mejorando la eficiencia operativa y garantizando la seguridad de los datos.

La gestión de identidades y accesos se refuerza mediante la adopción de Multi-Factor Authentication (MFA) y Role-Based Access Control (RBAC), junto con el uso de Decentralized Identifiers (DID) y k-anonimización para garantizar la privacidad de los datos. Estas medidas proporcionan un marco sólido para abordar los desafíos contemporáneos en la gestión de información de salud, asegurando la confidencialidad y seguridad de los datos en todo momento.

La combinación de cloud computing y blockchain, utilizando el modelo Blockchain-as-a-Service (BaaS) con Tolerancia a Fallos Bizantinos (BFT), ofrece una solución óptima para la gestión segura y eficiente de EHR. Este enfoque garantiza la

escalabilidad y flexibilidad de la nube, junto con la robustez y transparencia del blockchain. Además, la arquitectura BFT puede configurarse de manera rentable, lo que la hace ideal para aplicaciones en cloud computing, reduciendo costos y complejidad operativa para las instituciones de salud.

Para implementar una solución de EHR que integre blockchain y cloud computing, se recomienda una sinergia entre Amazon Web Services (AWS) y Hyperledger Fabric. AWS ofrece una infraestructura escalable y segura, mientras que Hyperledger Fabric destaca por su enfoque en la privacidad y confidencialidad de las transacciones, junto con su rendimiento y flexibilidad en el mecanismo de consenso. Esta combinación proporciona una solución integral que cumple con los requisitos de seguridad y privacidad, promoviendo un sistema de EHR más seguro, eficiente y conforme a las regulaciones.

El flujo de datos en el sistema de EHR implica la generación, cifrado, transmisión segura, almacenamiento en la nube, registro en blockchain y gestión de accesos y compartición de datos. Cada etapa se lleva a cabo con cuidado y se verifica mediante puntos de control clave para garantizar la integridad, seguridad y disponibilidad de los datos en todo momento. Además, se implementan estrategias de replicación de datos y recuperación ante desastres en AWS para garantizar la disponibilidad continua de la información crítica del paciente.

2. *Modelado de la Integración de Blockchain y Cloud Computing*

La arquitectura del sistema se organiza en capas para facilitar la comprensión de su funcionamiento. Primero, se inicia con la obtención del permiso para acceder al EHR, donde el usuario solicita acceso a través de un proceso de autenticación inicial, seguido de verificaciones de identidad y Control de Acceso Basado en Roles (RBAC). Luego, el API Gateway otorga un token de acceso que permite al usuario interactuar con los recursos protegidos del sistema.

Los componentes principales de la arquitectura incluyen las Aplicaciones de Usuarios Finales, el API Gateway, contratos inteligentes en Hyperledger Fabric, almacenamiento en la Nube (AWS S3) y la plataforma blockchain (Hyperledger Fabric). Estos elementos se conectan entre sí, permitiendo la interacción bidireccional entre la interfaz de usuario y el procesamiento lógico, así como la comunicación con la nube y la infraestructura blockchain.

Las conexiones entre los componentes implican solicitudes y respuestas entre la interfaz de usuario y el procesamiento lógico, así como el almacenamiento y recuperación de datos en la nube. La interacción con la infraestructura blockchain implica consultas para validar permisos y garantizar la integridad de los datos almacenados, lo que justifica flechas de doble sentido en algunas conexiones.

Es importante destacar que la conexión entre Hyperledger Fabric y AWS S3 es indirecta, ya que se centra en vincular información inmutable almacenada en la blockchain con datos cifrados en la nube. Esto se logra mediante la grabación de hashes criptográficos en la blockchain, lo que permite la validación de la integridad de los datos almacenados en la nube sin la necesidad de transferir datos directamente entre los sistemas. Este enfoque garantiza la seguridad y la transparencia en el manejo de datos sensibles en el sector de la salud, cumpliendo con regulaciones como HIPAA.

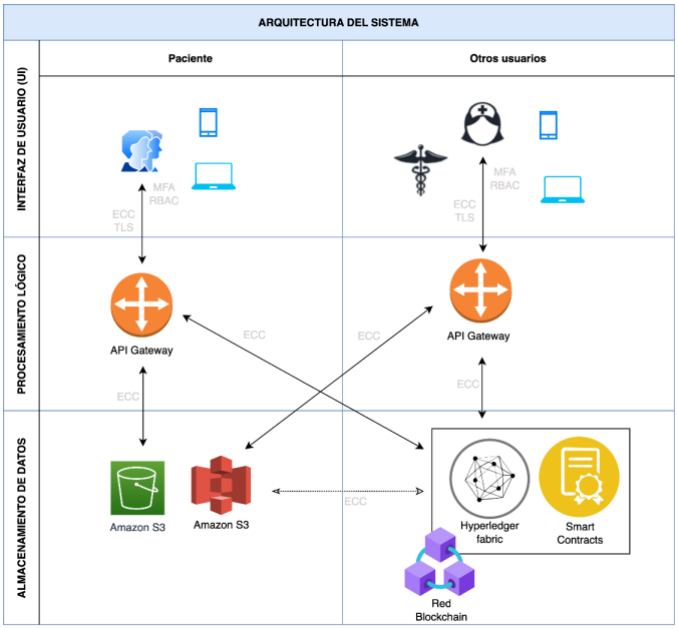

Fig. 2. Arquitectura del sistema.

La gestión de identidades se fortalece mediante la adopción de identificadores descentralizados (DIDs), permitiendo a los usuarios controlar sus credenciales digitales de forma autónoma. Estos DIDs, implementados en la blockchain de Hyperledger Fabric, ofrecen una solución resistente a la centralización y a fallos únicos, esenciales para proteger la identidad digital en el ámbito de la salud. Además, se implementan soluciones de autenticación multifactor (MFA) y control de acceso basado en roles (RBAC) para garantizar la integridad y seguridad del sistema, en conformidad con regulaciones como HIPAA.

La interoperabilidad de datos se logra mediante la adopción de estándares reconocidos como HL7 FHIR, facilitando el intercambio eficiente de datos y la comunicación entre sistemas. Con la implementación de APIs específicas, se asegura la compatibilidad y comunicación efectiva entre la infraestructura de blockchain y los servicios en la nube, garantizando acceso completo y seguro a la información médica para los proveedores de atención médica.

Los smart contracts desempeñan un papel crucial en la automatización de procesos, gestión de consentimientos, integración y compartición segura de datos, y registro de actividades. Estos contratos mejoran la seguridad y eficiencia del sistema, permitiendo una gestión transparente y automatizada de los registros médicos, con un enfoque en la protección de la privacidad del paciente y el cumplimiento normativo.

Para el monitoreo y auditoría del sistema, se emplean herramientas como Amazon CloudWatch, AWS CloudTrail y el Explorador de Blockchain de Hyperledger Fabric. Estas herramientas proporcionan visibilidad completa del sistema,

generando alertas automáticas frente a actividades inusuales y permitiendo una intervención temprana ante amenazas. Además, se establecen intervalos regulares para auditorías sistemáticas, complementadas por revisiones periódicas de políticas de auditoría y seguridad para mantener el sistema actualizado y alineado con las regulaciones vigentes. Este enfoque demuestra un compromiso con la integridad, seguridad y cumplimiento de la gestión de EHR, a través de una integración efectiva de tecnologías de blockchain y cloud computing.

F. Análisis de la Gestión del Riesgo

Es crucial evaluar y gestionar los riesgos al integrar tecnologías de blockchain y computación en la nube en la gestión de registros electrónicos de salud, para proteger la seguridad, privacidad e integridad de los datos sensibles y asegurar el cumplimiento normativo mediante un enfoque proactivo.

1. *Identificación de riesgos potenciales y Evaluación de impacto:*

En el contexto de la gestión de registros electrónicos de salud (EHR) mediante tecnologías de blockchain y computación en la nube, diversos riesgos y vulnerabilidades emergen, incluyendo errores de configuración que pueden exponer datos sensibles, comprometiendo la privacidad y la conformidad con regulaciones como HIPAA. Vulnerabilidades en el software, debido a actualizaciones insuficientes o defectos de diseño, pueden permitir accesos o alteraciones no autorizadas, afectando la integridad y disponibilidad de los EHR. La gestión inadecuada de claves criptográficas, errores de usuarios y fallas de interoperabilidad entre sistemas de EHR resaltan la importancia de una gestión de riesgos meticulosa para garantizar la continuidad y calidad del cuidado del paciente. Asimismo, el incumplimiento normativo, las brechas de seguridad en la transmisión de datos y las fallas de infraestructura en la nube subrayan la necesidad de estrategias de seguridad robustas. Para abordar estos desafíos, se recomienda la implementación de prácticas como la actualización constante del software, políticas estrictas de gestión de claves, educación de usuarios sobre prácticas seguras, un marco de cumplimiento normativo sólido, auditorías de seguridad regulares y un plan de respuesta efectivo ante incidentes, todo ello orientado a minimizar los riesgos y proteger la integridad y confidencialidad de los datos de salud en un entorno tecnológicamente avanzado y regulado.

V. Conclusiones

La revisión bibliográfica sobre la aplicación de la tecnología Blockchain en la gestión de registros médicos electrónicos (EHR) ha demostrado su potencial para abordar desafíos críticos como la seguridad, la privacidad y la interoperabilidad. Este estudio ha establecido un marco teórico sólido, resaltando la importancia de Blockchain en la automatización y manejo eficiente de historiales clínicos, y ha identificado oportunidades significativas para su integración en los sistemas de salud actuales, prometiendo mejoras en la eficiencia operativa y la seguridad de los datos de los pacientes.

La fusión de Blockchain con la computación en la nube en el contexto de los EHR introduce un nuevo paradigma en el almacenamiento, acceso y compartición de datos de salud, marcando un hito en la seguridad, transparencia e inmutabilidad de los registros. Este enfoque promete una gestión de datos más segura y eficiente pero requiere una planificación y gestión de riesgos meticulosas para abordar los desafíos técnicos y de seguridad que surgen, particularmente en la configuración de la infraestructura en la nube y la gestión de claves criptográficas, subrayando la necesidad de habilidades especializadas en seguridad informática y políticas robustas de gestión de claves.

Por otro lado, la interoperabilidad entre diferentes sistemas de EHR y su integración efectiva con Blockchain es crucial para un ecosistema de salud integrado, destacando la importancia de adoptar estándares abiertos y protocolos que faciliten el intercambio seguro de información médica. Además, se reconoce la importancia de otorgar a los pacientes un mayor control sobre su información de salud, empoderándolos a través del acceso seguro y la gestión del consentimiento, lo que representa un avance hacia la atención centrada en el paciente y subraya el impacto positivo de Blockchain en la satisfacción del paciente y la optimización de los procesos operativos en el sector salud.

Finalmente, la integración exitosa de Blockchain y cloud computing en la gestión de EHR, desde la perspectiva de la ingeniería industrial, sugiere un cambio paradigmático en la gestión de la salud, enfatizando la importancia de una colaboración multidisciplinaria para navegar las complejidades de adaptar estas tecnologías a los sistemas de salud. Esto incluye una atención rigurosa al cumplimiento de regulaciones, la seguridad de los datos, y la gestión de la interoperabilidad y el cumplimiento normativo, lo que demuestra que, con un enfoque proactivo y cuidadoso, Blockchain puede revolucionar el sector de la salud, mejorando la seguridad de los datos y la eficiencia en la prestación de servicios.

VI. Recomendaciones

Para robustecer la gestión de registros electrónicos de salud (EHR), es clave optimizar la infraestructura de computación en la nube y promover la interoperabilidad entre sistemas de EHR y plataformas blockchain, estandarizando protocolos para asegurar la integridad y confidencialidad de los datos médicos. La capacitación continua en seguridad y uso efectivo de las tecnologías basadas en blockchain es vital para usuarios y profesionales, garantizando así la protección óptima de la información de salud.

Las auditorías de seguridad y pruebas de penetración son esenciales para detectar y mitigar vulnerabilidades mediante un enfoque multicapa que incluye cifrado y autenticación multifactor, reforzando la defensa contra ataques cibernéticos. Es crucial mantener actualizadas las políticas de conformidad y seguridad, alineadas con regulaciones vigentes, para la protección de datos en tránsito y almacenados. Estas prácticas prometen mejorar la eficiencia y seguridad en la gestión de EHR, aumentando la confianza de los pacientes en la seguridad de su información de salud.

REFERENCES

[1] Y. R. Park, E. Lee, W. Na, S. Park, Y. Lee, y J. H. Lee, «Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility», *J Med Internet Res*, vol. 21, n.º 2, feb. 2019, doi: 10.2196/12533.

[2] J. Indumathi *et al.*, «Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6HCS)», *IEEE Access*, vol. 8, pp. 216856-216872, 2020, doi: 10.1109/ACCESS.2020.3040240.

[3] S. Tanwar, K. Parekh, y R. Evans, «Blockchain-based electronic healthcare record system for healthcare 4.0 applications», *Journal of Information Security and Applications*, vol. 50, feb. 2020, doi: 10.1016/j.jisa.2019.102407.

[4] T. Poongodi, R. Sujatha, M. Kiruthika, y P. Suresh, «Chapter 9 - IoT-based health care data analytical paradigm using blockchain technology», en *Cognitive Data Models for Sustainable Environment*, S. Bhattacharyya, N. K. Mondal, K. Mondal, J. P. Singh, y K. B. Prakash, Eds., Academic Press, 2022, pp. 203-230. doi: https://doi.org/10.1016/B978-0-12-824038-0.00001-8.

[5] X. Xu, Y. Guo, y Y. Guo, «Fog-enabled private blockchain-based identity authentication scheme for smart home», *Comput Commun*, vol. 205, pp. 58-68, may 2023, doi: 10.1016/j.comcom.2023.04.005.

[6] F. A. Reegu *et al.*, «Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System», *Sustainability (Switzerland)*, vol. 15, n.º 8, abr. 2023, doi: 10.3390/su15086337.

[7] H. S. Jennath, V. S. Anoop, y S. Asharaf, «Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Artificial Intelligence», *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6, n.º 3, p. 15, 2020, doi: 10.9781/ijimai.2020.07.002.

[8] E. Y. Daraghmi, Y. A. Daraghmi, y 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.

[9] F. Jamil, S. Ahmad, N. Iqbal, y D. H. Kim, «Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals», *Sensors (Switzerland)*, vol. 20, n.º 8, abr. 2020, doi: 10.3390/s20082195.

[10] İ. Köse *et al.*, «Basic electronic health record (EHR) adoption in **Türkiye is nearly complete but challenges persist», *BMC Health Serv Res*, vol. 23, n.º 1, dic. 2023, doi: 10.1186/s12913-023-09859-w.

[11] S. Honavar, «Electronic medical records - The good, the bad and the ugly», *Indian Journal of Ophthalmology*, vol. 68, n.º 3. Wolters Kluwer Medknow Publications, pp. 417-418, 1 de marzo de 2020. doi: 10.4103/ijo.IJO_278_20.

[12] B. S. Egala, A. K. Pradhan, S. Gupta, K. S. Sahoo, M. Bilal, y K. S. Kwak, «CoviBlock: A Secure Blockchain-Based Smart Healthcare Assisting System», *Sustainability (Switzerland)*, vol. 14, n.º 24, dic. 2022, doi: 10.3390/su142416844.

[13] A. Windari, E. Susanto, y I. Q. Fadhilah, «Hospital administrative services with electronic medical records: A meta-analysis», *Journal of Public Health and Development*, vol. 21, n.º 3. Mahidol University - ASEAN Institute for Health Development, pp. 333-348, 1 de septiembre de 2023. doi: 10.55131/jphd/2023/210325.

[14] K. Peterson, R. Deeduvanu, P. Kanjamala, y K. Boles, «A Blockchain-Based Approach to Health Information Exchange Networks».

[15] T. Hai, J. Zhou, S. R. Srividhya, S. K. Jain, P. Young, y S. Agrawal, «BVFLEMR: an integrated federated learning and blockchain technology for cloud-based medical records recommendation system», *Journal of Cloud Computing*, vol. 11, n.º 1, dic. 2022, doi: 10.1186/s13677-022-00294-6.

[16] M. Tuler De Oliveira *et al.*, «SmartAccess: Attribute-Based Access Control System for Medical Records based on Smart Contracts», vol. 4, pp. 1-20, 2022, doi: 10.1109/ACCESS.2017.DOI.

[17] A. F. Abbas, N. A. Qureshi, N. Khan, R. Chandio, y J. Ali, «The Blockchain Technologies in Healthcare: Prospects, Obstacles, and Future Recommendations; Lessons Learned from Digitalization», *International journal of online and biomedical engineering*, vol. 18, n.º 9, pp. 144-159, 2022, doi: 10.3991/ijoe.v18i09.32253.

[18] P. Sabbagh *et al.*, «Evaluation and classification risks of implementing blockchain in the drug supply chain with a new hybrid sorting method», *Sustainability (Switzerland)*, vol. 13, n.º 20, oct. 2021, doi: 10.3390/su132011466.

[19] J. K. Sadeghib R, V. R. Prybutok, y B. Sauser, «Theoretical and practical applications of blockchain in healthcare information management», *Information and Management*, vol. 59, n.º 6, sep. 2022, doi: 10.1016/j.im.2022.103649.

[20] D. V. Dimitrov, «Blockchain applications for healthcare data management», *Healthc Inform Res*, vol. 25, n.º 1, pp. 51-56, 2019, doi: 10.4258/hir.2019.25.1.51.

[21] R. Akkaoui, X. Hei, y W. Cheng, «EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange», *IEEE Access*, vol. 8, pp. 113467-113486, 2020, doi: 10.1109/ACCESS.2020.3003575.

[22] E. S. Babu, B. V. R. N. Yadav, A. K. Nikhath, S. R. Nayak, y W. Alnumay, «MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns», *Cluster Comput*, vol. 26, n.º 4, pp. 2217-2244, ago. 2023, doi: 10.1007/s10586-022-03652-w.

[23] H. Landi, «Number of patient records breached nearly triples in 2019».

[24] K. T. Akhter Md Hasib *et al.*, «Electronic Health Record Monitoring System and Data Security Using Blockchain Technology», *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/2366632.

[25] B. S. Egala, A. K. Pradhan, V. Badarla, y 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, n.º 14, pp. 11717-11731, jul. 2021, doi: 10.1109/JIOT.2021.3058946.

[26] B. Bera, A. Mitra, A. K. Das, D. Puthal, y Y. H. Park, «Private Blockchain-Based AI-Envisioned Home Monitoring Framework in IoMT-Enabled COVID-19 Environment», *IEEE Consumer Electronics Magazine*, vol. 12, n.º 3, pp. 62-71, may 2023, doi: 10.1109/MCE.2021.3137104.

[27] A. Cernian, B. Tiganoaia, I. S. Sacala, A. Pavel, y A. Iftemi, «Patientdatachain: A blockchain-based approach to integrate personal health records», *Sensors (Switzerland)*, vol. 20, n.º 22, pp. 1-24, nov. 2020, doi: 10.3390/s20226538.

[28] F. G. Monleón, «El blockchain al servicio de la sostenibilidad», ESIC. https://www.esic.edu/rethink/tecnologia/el-blockchain-al-servicio-de-la-sostenibilidad

[29] A. Zwitter, O. J. Gstrein, y E. Yap, «Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual», Frontiers In Blockchain, vol. 3, may 2020, doi: 10.3389/fbloc.2020.00026.

[30] J. M. G. Montón, «Interoperabilidad de los sistemas de salud», ehCOS, 25 de mayo de 2021. https://www.ehcos.com/interoperabilidad-los-sistemas-salud/

[31] M. Tutty, L. E. Carlasare, S. Lloyd, y C. A. Sinsky, «The complex case of EHRs: examining the factors impacting the EHR user experience», Journal Of The American Medical Informatics Association, vol. 26, n.o 7, pp. 673-677, abr. 2019, doi: 10.1093/jamia/ocz021.

[32] R. M. A. Rodríguez, I. G. Alfaro, R. B. Toledo, y J. D. C. Rodríguez, «Historia clínica y receta electrónica: riesgos y beneficios detectados desde su implantación. Diseño, despliegue y usos seguros», Atención Primaria, vol. 53, p. 102220, dic. 2021, doi: 10.1016/j.aprim.2021.102220.

[33] D. Thompson et al, "reducing clinical costs with an EHR," Healthcare Financial Management, vol. 64, (10), pp. 106-8, 110, 112 passim, 2010. Available: https://www.proquest.com/trade-journals/reducing-clinical-costs-with-ehr/docview/811379490/se-2.

[34] F. A. Reegu et al., «Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System», Sustainability, vol. 15, n.o 8, p. 6337, abr. 2023, doi: 10.3390/su15086337.

[35] G. K. Wabo, F. Praßer, K. Gierend, F. Siegel, y T. Ganslandt, «Data Quality– and Utility-Compliant Anonymization of Common Data Model–Harmonized Electronic Health Record Data: Protocol for a Scoping Review», JMIR Research Protocols, vol. 12, p. e46471, ago. 2023, doi: 10.2196/46471.

[36] Y. C. Quiel, A. Saavedra, y V. Villarreal, «Estándares de codificación e interoperabilidad en Salud: evaluación del proyecto AmIHEALTH», 2019. https://www.redalyc.org/journal/3776/377665579007/html/
[37] T. F. Alves, F. A. Almeida, F. A. Almeida, F. S. V. Tourinho, y S. R. De Andrade, «Regulation and Use of Health Information Systems in Brazil and Abroad», CIN: Computers, Informatics, Nursing, vol. 40, n.o 6, pp. 373-381, nov. 2021, doi: 10.1097/cin.0000000000000828.
[38] J. montemagno, «Uso de bases de datos NoSQL como una infraestructura de persistencia - .NET», Microsoft Learn, 10 de mayo de 2023. https://learn.microsoft.com/es-es/dotnet/architecture/microservices/microservice-ddd-cqrs-patterns/nosql-database-persistence-infrastructure
[39] Sql, «Normalización y desnormalización en Bases de Datos SQL | Programar SQL», Programar en SQL, 4 de agosto de 2023. https://www.programarsql.com/normalizacion-y-desnormalizacion-en-bases-de-datos-sql/
[40] N. Vollmer, «Artículo 17 UE Reglamento general de protección de datos. Privacy/Privazy according to plan.», Nicholas Vollmer, 4 de abril de 2023. https://www.privacy-regulation.eu/es/17.htm
[41] E. Πολίτου, F. Casino, E. Alepis, y C. Patsakis, «Blockchain Mutability: Challenges and Proposed Solutions», IEEE Transactions On Emerging Topics In Computing, vol. 9, n.o 4, pp. 1972-1986, oct. 2021, doi: 10.1109/tetc.2019.2949510.
[42] A. Khatoon, «A Blockchain-Based Smart Contract System for Healthcare Management», Electronics, vol. 9, n.o 1, p. 94, ene. 2020, doi: 10.3390/electronics9010094.
[43] A. Zwitter, O. J. Gstrein, y E. Yap, «Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual», Frontiers In Blockchain, vol. 3, may 2020, doi: 10.3389/fbloc.2020.00026.
[44] I. Montenegro, «Encriptación Simétrica y Asimétrica: Conoce sus diferencias», GB Advisors, 27 de julio de 2021. https://www.gb-advisors.com/es/encriptacion-simetrica-y-asimetrica-conoce-sus-diferencias/
[45] Vishwesh J, Dr. S. M. Sundaram «CP-ABE Protocol for Iot with Cloud», IJERT, abr. 2018, doi: 10.17577/IJERTCONV5IS22035.
[46] D. T. Bac y B. Khit, «An overview of quantum resistance digital signatures based on hash functions», Vinh University Journal Of Science, vol. 52, n.o 3A, pp. 40-54, sep. 2023, doi: 10.56824/vujs.2023a046.
[47] E. Milanov «The RSA algorithm», 2009. https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf
[48] Ciberseg, «¿Qué es el cifrado AES y cómo funciona?», Ciberseguridad, 9 de marzo de 2022. https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-aes/
[49] J. Lopez «Conectar - ProQuest». https://www.proquest.com/dissertations-theses/mapeamentos-de-hl7-v2-x-para-fhir/docview/2917303306/se-2?accountid=29068
[50] Heather Landi ;«Amazon, Google, Microsoft and IBM renew pledge to - ProQuest». https://www.proquest.com/trade-journals/amazon-google-microsoft-ibm-renew-pledge-support/docview/2266661042/se-2