

USO DE BLOCKCHAIN EN LA GESTIÓN CLÍNICA PARA ECOSISTEMAS SANITARIOS RESILIENTES Y CONFIABLES

USING BLOCKCHAIN IN CLINICAL MANAGEMENT FOR RESILIENT AND RELIABLE HEALTHCARE ECOSYSTEMS

Remberto Gonzales Cruz

Universidad San Francisco Xavier

gonzales.remberto@usfx.bo

Recibido: 29 Abril 2025 / Revisado: 20 Agosto 2025 / Aceptado: 1 Septiembre 2025 / Publicado: 23 Septiembre 2025

Resumen

La gestión de historias clínicas plantea desafíos estructurales significativos relacionados con la interoperabilidad, la seguridad y la privacidad de los datos. Estos desafíos se acentuaron durante la pandemia de COVID-19, donde la falta de acceso oportuno y fiable a la información médica afectó directamente la capacidad de respuesta de los sistemas de salud. Este artículo se centra en un análisis teórico del uso de la tecnología blockchain como alternativa para la gestión descentralizada, segura y trazable de los registros clínicos. Se examinan los principios de funcionamiento de esta tecnología, sus componentes arquitectónicos clave, como IPFS, contratos inteligentes e identidad digital. Además, se discute su viabilidad desde una perspectiva jurídica, considerando regulaciones estatales. El estudio propone un marco conceptual que permite evaluar los beneficios potenciales, limitaciones y condiciones necesarias para la implementación de blockchain en sistemas de información sanitaria. A través de una revisión sistemática de literatura y el análisis de casos relevantes, se pretende ofrecer una visión amplia, crítica y fundamentada sobre el impacto transformador de blockchain en la administración de historias clínicas.

Palabras Clave: Blockchain, Ipfs, Seguridad, Trazabilidad, Historia Clínica, Salud

Introducción

La gestión de historias clínicas constituye un desafío estructural en los sistemas de salud, marcado por la falta de interoperabilidad, la escasa protección de la privacidad del paciente y la limitada capacidad de compartir información médica de manera segura entre instituciones. Estos problemas se hicieron especialmente evidentes durante la pandemia de COVID-19, cuando la inaccesibilidad oportuna a los datos clínicos obstaculizó la capacidad de respuesta de los sistemas sanitarios Domingos & Goncalves, (2023) . Esta crisis puso en relieve la necesidad urgente de contar con soluciones tecnológicas que permitan una administración más eficiente, confiable y descentralizada de los registros médicos.

En este contexto, la tecnología Blockchain ha emergido como una alternativa prometedora para transformar la forma en que se gestionan los datos clínicos, al ofrecer propiedades como inmutabilidad, trazabilidad, descentralización y control granular de acceso. No obstante, su adopción en el sector salud requiere un análisis riguroso que contemple tanto los fundamentos técnicos como las implicaciones legales, éticas y organizativas. El presente trabajo tiene como objetivo general analizar desde una perspectiva teórica los principios, ventajas y limitaciones del uso de Blockchain en la gestión de historias clínicas. Específicamente, se propone explorar modelos arquitectónicos descentralizados aplicables a entornos clínicos, evaluar la contribución de tecnologías complementarias como IPFS e identidad digital, y reflexionar sobre los marcos regulatorios asociados a la protección de datos sensibles.

Diversos estudios han abordado el potencial de Blockchain en el ámbito biomédico y sanitario. Vazirani et al., (2019) realizó una revisión sistemática destacando la eficiencia de esta

tecnología para mejorar la interoperabilidad clínica. De manera similar, Albiol-Perarnau & Alarcón Belmonte, (2024) enfatizan su aporte en el fortalecimiento de la seguridad de los datos médicos, mientras que Esposito et al., (2018) destaca su utilidad como solución para la privacidad en entornos de nube sanitaria. En el plano regional, investigaciones como la de Riveros Lancheros et al., (2019) ha demostrado la factibilidad técnica de implementar redes Blockchain en sistemas de salud latinoamericanos, aunque también reconocen barreras regulatorias y culturales que deben ser superadas.

Así, este trabajo se inscribe en una línea de investigación que no solo busca introducir tecnologías emergentes en los sistemas de información clínica, sino también fomentar un ecosistema de salud más transparente, seguro y centrado en el paciente.

Metodología

Este estudio adopta un diseño teórico-descriptivo, el cual integra una revisión sistemática de la literatura científica, un análisis conceptual y técnico de arquitecturas, la sistematización de casos piloto documentados y una revisión jurídica y de políticas públicas. El propósito central es combinar evidencia publicada (artículos, revisiones y estudios de caso), desarrollos técnicos y documentos normativos para construir un marco analítico sólido sobre la aplicabilidad de tecnologías blockchain y de sus componentes asociados como IPFS, contratos inteligentes e identidad digital en la gestión de historias clínicas.

La metodología se organiza en los siguientes ejes:

- **Revisión sistemática de literatura científica:** Se identificaron, consultaron y sintetizaron estudios que evalúan o describen aplicaciones,

arquitecturas, experiencias piloto y análisis legales relacionados con blockchain en el ámbito sanitario. Las búsquedas se realizaron en revistas indexadas como *Journal of Medical Internet Research*, *IEEE Access* y *Health Informatics Journal*. Esta revisión incluyó estudios de caso, revisiones sistemáticas y artículos teóricos Albiol-Perarnau & Alarcón Belmonte, (2024); Bermúdez Ocampo et al., (2023); Vazirani et al., (2019). Asimismo, se complementó con búsquedas en repositorios académicos como Google Scholar y en documentos institucionales, entre ellos los de AGETIC, con el fin de minimizar sesgos de publicación. Si bien este trabajo no constituye estrictamente una revisión sistemática, se aplicaron criterios de inclusión y exclusión: se incorporaron aquellos estudios con aplicación en salud o análisis técnicos de blockchain con implicaciones sanitarias, además de revisiones y casos con datos empíricos; se excluyeron opiniones sin evidencia técnica y trabajos no vinculados al sector salud.

- **Análisis conceptual y técnico:** Se desarrolló una revisión de arquitecturas propuestas y un análisis crítico de sus componentes (Layer 1 y Layer 2, IPFS, bases de datos cifradas, modelos de identidad KYC y smart contracts). Para ello se empleó una metodología de ingeniería de software orientada a descomponer las soluciones en capas y describir los flujos de datos, identificando fortalezas y limitaciones de cada propuesta.
- **Sistematización de casos documentados:** Se recopiló experiencias internacionales de uso de blockchain en salud con documentación técnica suficiente (arquitectura, métricas y lecciones aprendidas), priorizando la diversidad geográfica en Europa y América Latina, como las analizadas por Riveros Lancheros et al., (2019). El objetivo fue

identificar buenas prácticas, errores recurrentes y recomendaciones aplicables a futuros procesos de adopción.

- **Revisión legal:** Se incluyeron cuerpos normativos y documentos de política relevantes en materia de protección de datos y salud Agetic, (2024; Dulce Villarreal et al., (2023). Los criterios de selección contemplaron la jurisdicción aplicable, la vigencia de la norma, su alcance respecto al tratamiento de datos sensibles y su pertinencia para tecnologías descentralizadas.
- **Triangulación interdisciplinaria y validación:** Finalmente, se consideró la incorporación de perspectivas de actores clave (profesionales de la salud, administradores, auditores legales y pacientes) mediante charlas semiestructuradas, con el propósito de contrastar los hallazgos teóricos y técnicos con la realidad operativa y las expectativas regulatorias.

Fundamentos Tecnológicos

Los fundamentos tecnológicos de la implementación de blockchain en la gestión de historias clínicas se articulan sobre un conjunto de componentes que permiten garantizar la seguridad, disponibilidad y descentralización de los datos en salud. A continuación, se detallan los principales elementos tecnológicos y sus funciones dentro de este ecosistema:

- **Blockchain Layer 2:** Estas soluciones permiten ampliar la escalabilidad de la blockchain principal mediante canales paralelos o de segunda capa que procesan transacciones fuera de la cadena principal, reduciendo tiempos de validación y costos operativos. Su implementación resulta esencial para soportar grandes volúmenes de

datos clínicos en tiempo real Esposito et al., (2018).

- **IPFS (InterPlanetary File System):** Se trata de un sistema de archivos distribuido que permite almacenar documentos médicos como radiografías, resonancias, y otros tipos de imágenes, con una estructura inmutable y verificable. Los archivos se referencian mediante hashes criptográficos, asegurando la integridad y disponibilidad de los datos sin depender de un servidor centralizado.
- **Bases de datos cifradas:** Complementan la estructura descentralizada permitiendo que información altamente sensible (como datos personales del paciente), se almacenen de forma cifrada. Este cifrado garantiza la confidencialidad, y el acceso controlado mediante llaves privadas y sistemas de autenticación robustos.
- **Identidad digital con protocolos KYC (Know Your Customer):** Asegura que cada

usuario en el sistema (paciente, médico, administrador) esté correctamente autenticado y vinculado a una identidad digital única, reforzando los mecanismos de trazabilidad y gobernanza del sistema Kuo et al., (2017).

- **Interfaces de usuario (web y móvil):** Aplicaciones que permiten al paciente y a los profesionales consultar, visualizar y administrar datos clínicos bajo una interfaz amigable y segura, facilitando la interacción con el sistema sin requerimientos técnicos avanzados.
- **Contratos inteligentes (Smart Contracts):** Programas autoejecutables alojados en la blockchain que permiten automatizar procesos como el otorgamiento de permisos de acceso, la validación de recetas, o la verificación de identidad entre instituciones. Estos contratos actúan como intermediarios digitales incorruptibles, asegurando el cumplimiento de reglas preestablecidas sin intervención humana.

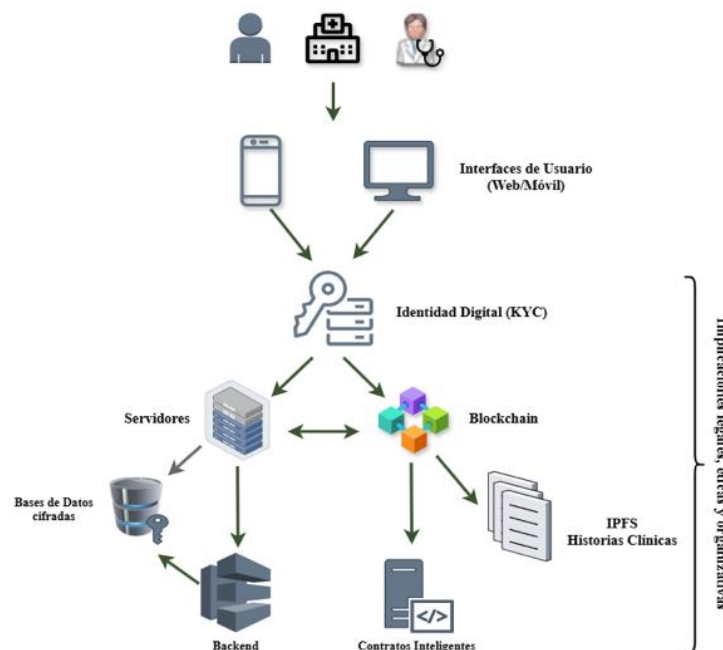


Figura 1. Arquitectura tecnológica

Resultados

- **Identificación clara de beneficios de Blockchain en la gestión de historias clínicas:** El documento evidencia que Blockchain puede resolver problemáticas persistentes como la fragmentación de la información médica, la falta de interoperabilidad entre instituciones y la limitada participación del paciente. Entre los beneficios más destacados están la trazabilidad, inmutabilidad de los registros, descentralización del control de datos y fortalecimiento de la privacidad.
- **Marco conceptual sólido para la aplicación de Blockchain en salud:** El trabajo proporciona un marco conceptual que describe los componentes tecnológicos clave (Blockchain, IPFS, contratos inteligentes e identidad digital) y cómo estos se integran en un sistema clínico. Este resultado es valioso como referencia para futuras investigaciones, ya que sintetiza la información técnica y legal en un esquema coherente que puede servir como base para modelos funcionales o simulaciones.
- **Análisis detallado de componentes técnicos aplicables al entorno clínico:** El estudio describe con precisión los elementos técnicos que harían viable un sistema descentralizado de historias clínicas: IPFS para almacenamiento seguro, contratos inteligentes para automatización de reglas, bases cifradas para protección de datos sensibles, e identidad digital con KYC para autenticación confiable.
- **Sistematización de experiencias internacionales y casos piloto:** El artículo recopila y analiza diversos casos documentados de implementación de Blockchain en salud, tanto en Europa como América Latina. Esta revisión permite

identificar patrones, buenas prácticas y errores comunes, lo que proporciona una base empírica útil para planificadores, tomadores de decisiones o investigadores que deseen replicar o adaptar estos modelos a sus propios contextos.

- **Fortalecimiento del enfoque interdisciplinario en salud digital:** El documento integra los campos de ingeniería informática, derecho, ética médica y gestión sanitaria, demostrando que el desarrollo de soluciones en salud digital requiere equipos interdisciplinarios. Este enfoque promueve una visión integral donde la tecnología no es un fin en sí mismo, sino una herramienta al servicio de procesos humanos y clínicos.

Discusión

¿Puede Blockchain garantizar plenamente la privacidad de los datos médicos en entornos descentralizados?

La privacidad en Blockchain se basa en mecanismos criptográficos que permiten la inmutabilidad y la verificación sin necesidad de intermediarios. Sin embargo, en el contexto médico, la privacidad va más allá de la integridad de los datos: implica control de acceso, anonimato y confidencialidad. Aunque el almacenamiento descentralizado en IPFS con hashes criptográficos y bases de datos cifradas fortalece la protección, el simple hecho de registrar cualquier información en una cadena inmutable (incluso metadatos) puede representar un riesgo si no se gestiona adecuadamente.

Un desafío clave es la implementación de sistemas de permisos granulares que permitan al paciente decidir quién accede a qué parte de su información, por cuánto tiempo y con qué fines. Además, el uso de identidad digital y autenticación robusta (como el protocolo KYC)

plantea dilemas sobre cómo balancear trazabilidad con anonimato. En este sentido, la privacidad en Blockchain no es automática ni absoluta: depende del diseño cuidadoso de la arquitectura, de políticas de gobernanza y de regulaciones adecuadas.

Viabilidad de la interoperabilidad entre sistemas de salud públicos y privados mediante Blockchain

Uno de los grandes obstáculos de la gestión clínica actual es la fragmentación de los datos entre instituciones. Blockchain puede ofrecer un modelo compartido para registrar información médica que distintos actores (hospitales, aseguradoras, clínicas, farmacias), puedan consultar de forma segura y estandarizada. No obstante, esta interoperabilidad no depende exclusivamente de la tecnología, sino de acuerdos entre actores y de voluntad política.

El desafío reside en integrar la Blockchain con sistemas legados (por ejemplo, historias clínicas almacenadas en software local sin conexión a la red), y en adaptar los formatos a modelos como HL7 FHIR (Fast Healthcare Interoperability Resources - Recursos rápidos de interoperabilidad en el sector sanitario). Además, se deben resolver cuestiones como el control sobre los nodos, la sincronización de datos y la compatibilidad de políticas de acceso. Aun si la infraestructura Blockchain es común, su interoperabilidad solo será real si hay un consenso regulatorio, técnico y operativo.

Desafíos regulatorios y éticos en la implementación de Blockchain en salud

La descentralización que propone Blockchain entra en tensión con marcos regulatorios tradicionales, basados en modelos centralizados de responsabilidad y supervisión. En muchos países, las leyes de protección de datos personales

(como el GDPR en Europa o el anteproyecto AGETIC en Bolivia) imponen criterios de localización, control, derecho al olvido y consentimiento explícito, que no siempre encajan con las propiedades de inmutabilidad y replicación de Blockchain.

Además, se abren debates éticos sobre quién decide qué datos se registran, cómo se audita el uso de la tecnología y qué pasa si hay errores o falsificaciones en los registros. La gobernanza ética de un sistema distribuido requiere nuevas figuras normativas: custodios digitales, auditores algorítmicos, o mecanismos de arbitraje que sustituyan al “administrador central” clásico. Por tanto, el marco legal debe evolucionar paralelamente a la tecnología para evitar brechas de responsabilidad.

Implicaciones sociales y culturales del control del paciente sobre su historia clínica

Uno de los mayores aportes de Blockchain es devolver al paciente el control sobre sus datos. Sin embargo, este empoderamiento también supone una carga: administrar claves privadas, entender mecanismos de permisos y asumir decisiones sobre su información médica. En contextos con baja alfabetización digital, este modelo puede generar exclusión o errores involuntarios con consecuencias clínicas graves.

Culturalmente, además, muchos sistemas de salud están estructurados sobre la autoridad del médico o la institución como guardianes de la información. Cambiar hacia una lógica de “autogestión del dato” implica revisar el rol del paciente, el modelo de consentimiento informado, y la corresponsabilidad en el manejo del historial clínico. Este cambio no es solo técnico, sino educativo y cultural.

Impacto económico de adoptar Blockchain en sistemas de salud

Aunque Blockchain promete reducir costos operativos a largo plazo (al eliminar intermediarios y reducir errores), su implementación inicial puede ser costosa y compleja. Requiere inversión en infraestructura, capacitación, rediseño de procesos y adaptación legal. Además, existen dudas sobre si los sistemas actuales de salud pública -muchos de ellos subfinanciados- están en condiciones de asumir esta transición tecnológica.

Un análisis costo-beneficio debe incluir factores indirectos: prevención de fraudes, disminución de repeticiones de exámenes, mejora en el seguimiento de tratamientos, entre otros. Por otro lado, sin una estrategia clara de sostenibilidad, Blockchain puede quedar relegada a pilotos sin impacto real.

Capacidad de escalabilidad y respuesta en tiempo real en contextos de emergencia sanitaria

Durante emergencias como pandemias o desastres naturales, los sistemas de salud requieren agilidad, interoperabilidad y fiabilidad. Blockchain puede ofrecer trazabilidad y control de acceso instantáneo, pero su escalabilidad ha sido históricamente un problema, especialmente en Blockchains públicas. Las soluciones de Layer 2 y cadenas privadas pueden mitigar esto, pero añaden complejidad al diseño.

Se deben prever cuellos de botella, congestión de red y mecanismos de recuperación ante fallos. Un sistema de salud basado en Blockchain solo será útil en emergencias si ha sido diseñado y probado previamente en contextos de alta demanda.

Riesgos técnicos y de gobernanza

La exposición de metadatos, la custodia de claves, los posibles ataques a los contratos inteligentes y la complejidad de las soluciones de segunda capa (L2) representan riesgos latentes en la implantación de blockchain en salud. Para mitigarlos, es necesario definir con precisión qué datos y metadatos deben ser realmente públicos, evitando exponer información sensible de manera innecesaria.

Otro aspecto crítico es la custodia de las claves utilizadas para firmar certificados. Para reducir vulnerabilidades, se recomienda implementar estructuras de multi-firma, en las cuales no solo un par de claves sea responsable de la validación, sino un conjunto de ellas. Esto refuerza el control y disminuye el riesgo de manipulación o pérdida de acceso.

En cuanto a los contratos inteligentes, su despliegue público permite que sean revisados por cualquier persona, lo cual aporta transparencia, pero también aumenta el riesgo de ataques. Por ello, antes de ser implementados deben ser sometidos a auditorías exhaustivas y detalladas, con el objetivo de identificar y corregir posibles vulnerabilidades.

Más allá de los aspectos técnicos, también existen riesgos de gobernanza, regulatorios y socioculturales. La colisión entre el derecho al olvido o la localización de datos frente a la inmutabilidad y replicación puede generar incumplimientos legales. Asimismo, la ausencia de un “administrador central” claro complica la asignación de responsabilidades, mientras que los modelos de identidad y consentimiento pueden entrar en tensión al intentar equilibrar anonimato y trazabilidad.

Conclusiones

El análisis teórico realizado permite inferir que blockchain representa una tecnología con alto potencial para mejorar la gestión de datos médicos en sistemas de salud. Su capacidad para garantizar inmutabilidad, trazabilidad y control de acceso es ampliamente reconocida, especialmente en contextos donde la confianza en los sistemas actuales es baja. No obstante, su adopción requiere considerar aspectos regulatorios, culturales y tecnológicos que condicionan su éxito.

Referencias Bibliográficas

- Agetic. (2024, octubre). *Anteproyecto: Ley de Protección de Datos Personales*. <https://www.agetic.gov.bo/wp-content/uploads/2024/10/Manual-de-Proteccion-de-Datos-2-firmado.pdf>
- Albiol-Perarnau, M., & Alarcón Belmonte, I. (2024a). Blockchain en salud: Transformando la seguridad y la gestión de datos clínicos. *Atención Primaria*, 56(5), 102848. <https://doi.org/10.1016/j.aprim.2023.102848>
- Albiol-Perarnau, M., & Alarcón Belmonte, I. (2024b). Blockchain en salud: Transformando la seguridad y la gestión de datos clínicos. *Atención Primaria*, 56(5), 102848. <https://doi.org/10.1016/j.aprim.2023.102848>
- Bermúdez Ocampo, J. S., Salazar Marulanda, N. L., & Vélez Rueda, L. (2023). Blockchain y salud: Una herramienta versátil y segura. *Ciencia, Tecnología e Innovación en Salud*, 6, 52–60. <https://doi.org/10.23850/25393871.5617>
- Domingos, I. M., & Goncalves, R. M. (2023a). Gobernanza Blockchain: Tecnología disruptiva para el control de la corrupción en la salud públicaa (Blockchain governance: disruptive technology for controlling corruption in public health). *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4592779>
- Domingos, I. M., & Goncalves, R. M. (2023b). Gobernanza Blockchain: Tecnología disruptiva para el control de la corrupción en la salud públicaa (Blockchain governance: disruptive technology for controlling corruption in public health). *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4592779>
- Dulce Villarreal, E. R., Betancourt Romo, J. H., Solarte Solarte, F. N. J., & Rosero Galíndez, C. M. (2023). BLOCKCHAIN: UNA MIRADA DESDE LA PROTECCIÓN DE DATOS SENSIBLES EN EL SECTOR SALUD. *REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA)*, 2(38), 69–78. <https://doi.org/10.24054/rcta.v2i38.1279>
- Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018a). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, 5(1), 31–37. <https://doi.org/10.1109/MCC.2018.011791712>
- Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018b). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, 5(1), 31–37. <https://doi.org/10.1109/MCC.2018.011791712>
- Galván Torres, D. R. (2021). *Prototipo de una aplicación descentralizada de apoyo a los procedimientos de gestión de inventarios de la Universidad Distrital usando Blockchain e IPFS*. <http://hdl.handle.net/11349/29176> La - Spanish
- Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger

technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 1211–1220. <https://doi.org/10.1093/jamia/ocx068>

Riveros Lancheros, D. F., Martínez Zarama, G., González Arteta, J. D., & Cabrera Venegas, N. E. (2019a). *Diseño e implementación de tecnologías Blockchain para el sector salud en Colombia* [Universidad de los Andes]. <https://hdl.handle.net/1992/45108>

Riveros Lancheros, D. F., Martínez Zarama, G., González Arteta, J. D., & Cabrera Venegas, N. E. (2019b). *Diseño e implementación de tecnologías Blockchain para el sector salud en Colombia* [Universidad de los Andes]. <http://hdl.handle.net/1992/45108>

Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019a). Implementing Blockchains for Efficient Health Care: Systematic Review. *Journal of Medical Internet Research*, 21(2), e12439. <https://doi.org/10.2196/12439>

Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019b). Implementing Blockchains for Efficient Health Care: Systematic Review. *Journal of Medical Internet Research*, 21(2), e12439. <https://doi.org/10.2196/12439>